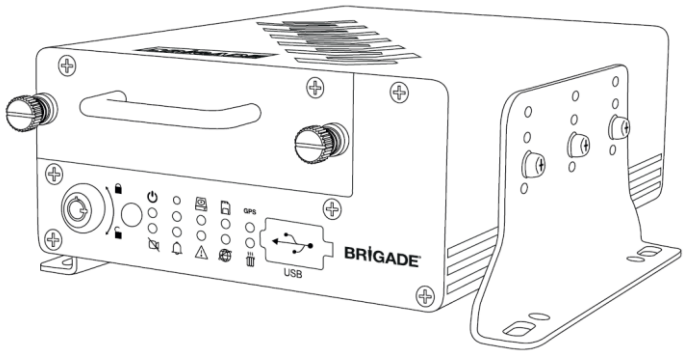
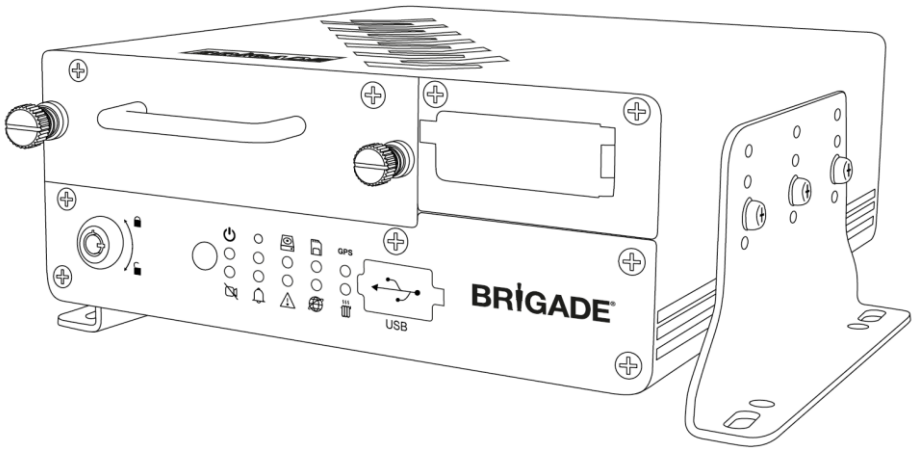
Mobile Digital Recorder

MDR-504GW-500
MDR-504G-500
MDR-504W-500



MDR-508GW-1000
MDR-508G-1000
MDR-508W-1000



MDR 500 Series Network Connectivity Software and Infrastructure Manual
(For Operators and Information Technology Professionals)

Please refer to www.brigade-electronics.com for most up-to-date data on all products

Table of Contents

1 Introduction to MDR 500 Series Technology

Brigade's MDR-508xx-1000 and MDR-504xx-500 are advanced Mobile Digital Recorders (MDRs) designed to record and playback 8 or 4 channels. The system uses Analog High Definition (AHD), Phase Alternating Line (PAL) or National Television System Committee (NTSC) television systems. The resolution can be CIF, WCIF, HD1, WHD1, D1, WD1 or AHD (HD/720p or FULL HD/1080p). Information related to recording parameters, alarms and trigger status can be recorded along with speed, location and G-Force data. In addition, data related to the unit itself such as voltage and temperature are recorded and plotted graphically in MDR Software (MDR-Dashboard 5.0 and MDR-Player 5.0). This information is called metadata.

Recordings can be searched, viewed and downloaded (clipped and saved locally) using MDR-Dashboard 5.0 software. This allows you to access all the vehicle's travel information, including route tracking. Recordings can be easily downloaded in three different ways: as a simple audio/video AVI file playable by consumer media players; as native proprietary format clips or as a password protected .exe file with an embedded MDR-Player 5.0.

The main storage unit is a large capacity Hard Disk Drive (HDD). The secondary storage is an internal SD (Secure Digital) card for sub-stream, HDD mirror (simultaneous) or alarm recording. The SD card stores video data and frame information only in chosen image resolution and frame rate. This is useful in extreme scenarios where the primary storage media reaches its limitations (e.g. a HDD write error during a collision).

Mobile network and Wi-Fi settings found in this manual relate to wireless products as described below. These features can be attained by upgrading the MDR 500 Series units. 8 channel models allow you to modularly upgrade. These units can be upgraded by various expansion modules. 4 channel units do not have a modular design to allow for mobile network/Wi-Fi upgrades.

To complete firmware upgrades, configuration imports/exports and video downloads, a USB bus-powered hub (minimum 2 ports) is required.

It is imperative that Brigade MDRs are fitted and commissioned by competent and trained technicians. The installers are responsible for the correct setup of the overall system and must adhere to relevant regulations and legislation.

Table 1: Description of MDR 500 Series Models:

#	MODEL	NUMBER OF CHANNELS	HDD CAPACITY	SD CAPACITY	GPS	MOB. NET	WI-FI
(1)	MDR-504GW-500	4	500GB	32GB	✓	✓	✓
(2)	MDR-504G-500	4	500GB	32GB	✓	✓	
(3)	MDR-504W-500	4	500GB	32GB	✓		✓
(4)	MDR-504-500	4	500GB	32GB	✓		
(5)	MDR-508GW-1000	8	1TB	64GB	✓	✓	✓
(6)	MDR-508G-1000	8	1TB	64GB	✓	✓	
(7)	MDR-508W-1000	8	1TB	64GB	✓		✓
(8)	MDR-508-1000	8	1TB	64GB	✓		

Table 2: Software for MDR 500 Series Products:

WINDOWS PC SOFTWARE	MOBILE PHONE APPS
(1) MDR-Dashboard 5.0	(1) MDR 5.0 (Android)
(2) MDR-Player 5.0	(2) MDR 5.0 (iOS)
(3) MDR Server 5.0	

Warning: Prior to attempting this system setup, please ensure the MDR 500 Series Installation & Operation Guide is thoroughly read and understood. Brigade will not be responsible for any failures due to incorrect installation or operation.
Ensure your anti-virus software has exclusions in place to allow the MDR software package to function properly.

1.1 Product Features

Table 3: Differences between MDR-504xx-500 and MDR-508xx-1000.

MDR-504XX-500	MDR-508XX-1000
500GB (2TB maximum) 2.5" HDD with anti-vibration mounting	1TB (2TB maximum) 2.5" HDD with anti-vibration mounting
Industrial grade 32GB (256GB maximum) internal SD card for mirror, sub-stream and alarm recording	Industrial grade 64GB (256GB maximum) internal SD card for mirror, sub-stream and alarm recording
Simultaneous 4 channel recording up to FULL HD @25fps (PAL) / @30fps (NTSC) each	Simultaneous 8 channel recording up to HD @25fps (PAL) / @30fps (NTSC) each or 8 channels at FULL HD @12fps (PAL) / @15fps (NTSC)
4x Select video connectors typical to camera inputs with audio	8x Select video connectors typical to camera inputs with audio
Weight: 2.2Kg	Weight: 2.75Kg

Table 4: Features of MDR 500 Series

MDR 500 SERIES	
Internal anti-vibration mount for the HDD and embedded super-capacitor for finalisation of recording after unexpected power interruption (up to 10 seconds). Individual channel configurations for recording resolution, frame rate and quality, display split 1/4/9 channels and monitor margin adjustment	Pre-alarm recording 1-60 minutes and Post-alarm recording 0-1800 seconds. (0 to 30 minutes), Normal, Alarm or Timer recording modes and flip vertical each channel, this will change live view (monitor) and recorded data
Start-up time to recording is approximately 50 seconds (recommend drivers to wait 3 minutes for recording to begin). 10 LEDs for diagnostic troubleshooting and flip doors for easy SIM/SD card access	Video quality selectable at 8 different quality levels for recording, video/audio compression H.264/ADPCM and operation log files for troubleshooting and anti-tampering feature – using digital code
Operating temperature: -40˚C to +70˚C. 12V Output max 1A load and 8.5-36V Power Input and I/O: 8x trigger input (trigger voltage 9V which can be set to trigger at low/high); 2x trigger output (12V max. 200mA)	Alarm recordings configurable for trigger, speed, G-Force, video loss, motion detection, blind detection, panic button, geo-fencing and SD card/HDD errors
USB-A (2.0) interface on the Docking Station (DS) for downloads, upgrades and configurations onto a USB flash drive (flash memory only, maximum 16GB) and USB-B (3.0) interface on the Mobile Caddy Unit (MCU) for displaying video recordings on a Windows™ operating system using MDR-Dashboard 5.0	Low voltage protection with configurable shut-down delay minimum restart voltage, ethernet 10/100 RJ45 port for configuration, live view, playback and video download. Mouse for configuration and recording/event search and Shut-down delay configurable from 0 seconds to 24 hours
Built-in G-Sensor and Built-in Audible Buzzer and GPS for location monitoring and tracking with external antenna and 2x EIA/TIA 485 (RS485) for optional External G-Sensor and Remote Status & Interface Panel	MCUs (Mobile Caddy Units) can be swapped between 4 and 8 channel units. Requires formatting before use.

2 MDR Server Requirements and Installation

MDR Server 5.0 is required software that runs on the Windows Server. This software enables an MDR unit to connect to the Windows Server. MDR Server controls the assignment of ports and its functionalities.

Note: This software runs on a **yearly license**. When nearing the expiration date, please visit Brigade's website (www.brigade-electronics.com) to download new license files. These files need to be copied onto the Windows Server running MDR Server 5.0. Copy these files to the following path **C:\Program Files (x86)\MDR Server\TransmitServer**.

2.1 MDR Server Requirements

To use mobile network and Wi-Fi connectivity features, networking expertise are required for implementation. The mobile network server is accessed by the MDR externally through a public IP (Internet Protocol) address. The Wi-Fi server is accessed by the MDR using a Wi-Fi network. This setup requires all devices (Server, Client and MDR) to be connected to a shared network. Client refers to MDR-Dashboard 5.0 or MDR 5.0 mobile apps. It is better for customers to use both network connectivity options to achieve different goals, live camera capabilities of mobile networks and the low data cost of downloading video data over Wi-Fi.

Warning: If you have two separate MDR Server 5.0 software installations, video and metadata stored on each server is NOT linked.

Table 5: The minimum requirements below for MDR Server 5.0 with **1-10 MDR units**

COMPONENT	MINIMUM REQUIREMENTS
CPU (Central Processing Unit)	Dual Core - 1 GHz (x86 CPU) or 1.4 GHz (x64 CPU)
RAM (Random Access Memory)	8GB
Requested HDD space for software installation	10 GB required, 40 GB or more recommended (depending on the number of MDRs connected at one instant and the features used). Each MDR requires an additional 250MB of storage
Video	Super VGA or higher video card and monitor
Operating System	Windows Server 2012 R2 Standard 32\64bit
Framework	Microsoft .Net Framework v3.5 SP1 or above version must be installed on both server and client**
Wireless Adaptor	Wireless Access Point 802.11 b/g/n

**Client refers MDR-Dashboard 5.0 software

Table 6: The Recommended requirements below for MDR Server 5.0 with **>10 MDR units <100**

COMPONENT	RECOMMENDED REQUIREMENTS
CPU (Central Processing Unit)	Quad-Core Xeon 5504*2 or greater
RAM (Random Access Memory)	12GB
Requested HDD space for software installation	10 GB required, 150 GB or more recommended (depending on the number of MDRs connected at one instant and the feature used)
Video	Super VGA or higher video card and monitor
Operating System	Windows Server 2012 R2 Standard 32\64bit
Framework	Microsoft .Net Framework v3.5 SP1 or above version must be installed on both server and client**
Wireless Adaptor	Wireless Access Point 802.11 b/g/n

**Client refers MDR-Dashboard 5.0 software

Warning: The limitations to view several MDR video data feeds at one instant would be dependent on network speed, mobile network coverage, Windows Server's HDD (Hard Drive Disk) and RAM (Random Access Memory) capacity.

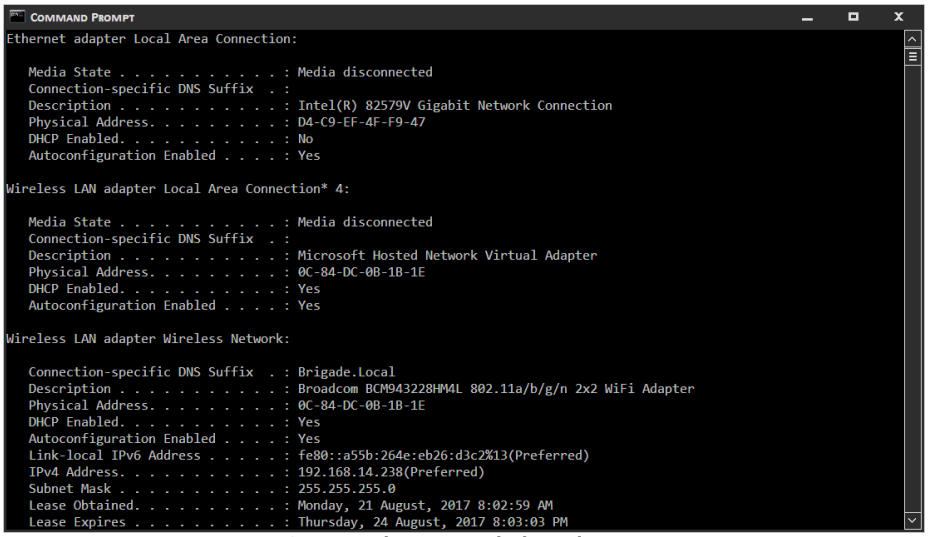
2.2 MDR Server Installation

Establish the IP address and MAC address of the Windows Server.

- IP address of Wi-Fi Server
- IP address of Mobile Network Server

Wi-Fi: Connect the router to the Wi-Fi Windows Server with an ethernet cable or Wi-Fi network.

Mobile Network: Contact the IT department to setup port forwarding on to the Windows Server as shown in below:



Command Prompt Window Figure 1

Table 7: Port Forwards List

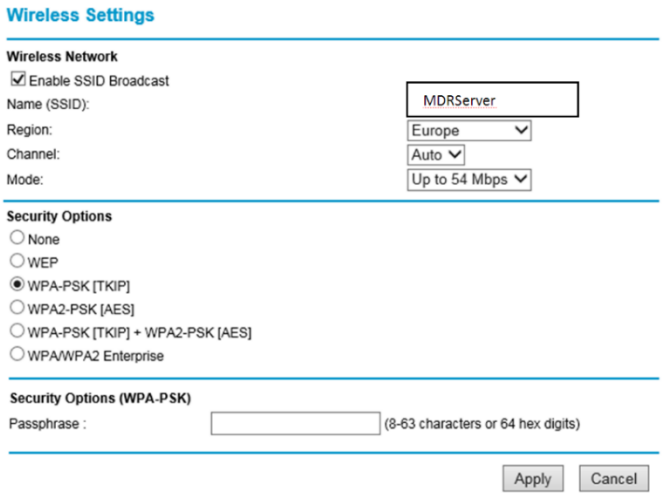
#	PORT NAME	PORT NUMBER	PORT FUNCTION (CLIENT REFERS TO MDR-DASHBOARD 5.0 / MDR 5.0 APP)	USED BY
(1)	Device Access to Server	5556	Message Server	Device
(2)	Balance Server	7264	Balance the load for clustering servers - (for future clustering of servers) – specify this port when logging in – creates initial connection	Client
(3)	Running Port	10086	For internal communication and background services	Internal
(4)	Operation Server Web	12003	Port used for internal communication	Internal
(5)	Client instruction service	12020	Client message service - data connection	Client
(6)	Black box Data Query	12040	For Metadata	Internal
(7)	HTTP Data Port	12041	Port used for internal communication	Internal
(8)	Data Port	12042	MDR Server Feature	Internal
(9)	Video playback service	12045	For video playback from Server to the Clients	Client
(10)	Proxy Server (Remote Setting) Client Data	12050	For the remote config (within MDR-Dashboard 5.0) feature – from Server to Client	Client
(11)	Proxy Server (Remote Setting) Device Data	12051	For the remote config (within MDR-Dashboard 5.0) feature – from MDR to Server	Device
(12)	Web Service	12055	For browser access	Client
(13)	One key alarm media service	12065	Support one key alarm service	Device
(14)	MDR4 Streaming Media Server	12091	MDR 400 Series Products – Live view data transmission	MDR 400 Firmware
(15)	MDR5 Streaming Media Server	12092	MDR 500 Series Products – Live view data transmission	MDR 500 Firmware
(16)	Transmit Server	17891	For MDR Server to connect to Clients - to transfer Live video	Client

Wi-Fi: An example of a router page is shown in *Wireless Router Settings Figure 2*. The router login page is accessed using the factory settings. You may find the router IP, username and password underneath the router, alternatively contact the manufacturer. Once logged into the router, setup the wireless network. MDR units are compatible with **WPA**, **WPA2** or **WEP** encryption.

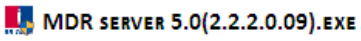
Wi-Fi: *Wireless Router Settings Figure 2* shows an example of a wireless network created. The **SSID** (Service Set Identifier) is **MDRServer** and **WPA-PSK** security has been used. When entering the SSID into the MDR unit, this is case sensitive. It is advised to create SSIDs without spaces to avoid any typing errors on the MDR.

Wi-Fi: When using an access point no port forwarding is required on a basic network. If you want to access the Wi-Fi server remotely you will need to port forward to the Wi-Fi MDR Server from your firewall (a static public IP address is required).

Mobile Network: The Windows Server should have a static public IP address. The IP address is 192.168.14.193 (in this example). This can be permanently assigned using the server's MAC address.
It is recommended to use a newly-built or clean Windows Server.



Wireless Router Settings Figure 2



MDR Server Icon Figure 3

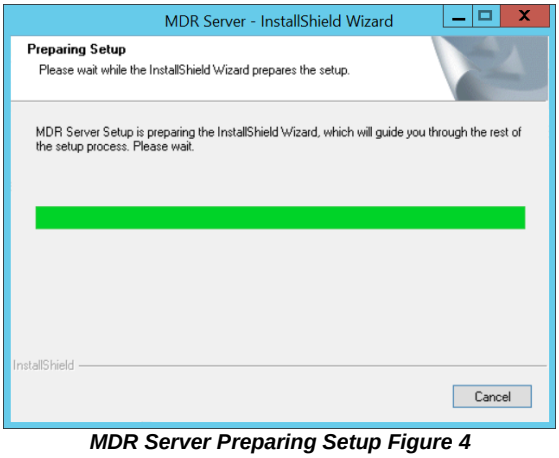
Warning: If this device is used to host other software that uses SQL, we do not recommend installing MDR Server 5.0 on the same Windows Server.

Before starting the MDR Server installation, ensure Microsoft .Net Framework v3.5 SP1 or above is installed on your Windows Server.

Right-click the installation file found in *MDR Server Icon Figure 3* and **RUN AS ADMINISTRATOR**. You may be prompted to back up any data if they have previously installed MDR Server software on this Windows Server.

Warning: The backup feature can only backup user and vehicle information. This cannot backup video data, metadata and evidence data.

Give the software a few minutes to prepare the setup. As shown in *MDR Server Preparing Setup Figure 4*.

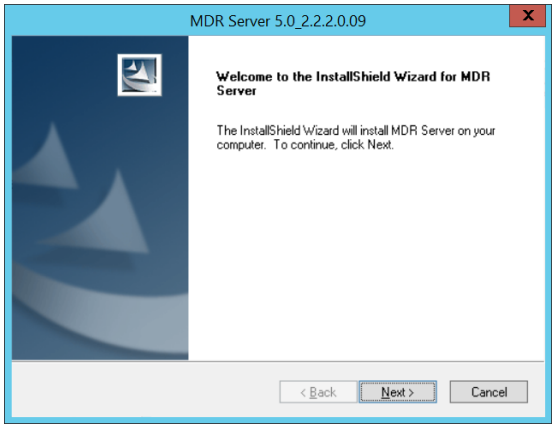


MDR Server Preparing Setup Figure 4

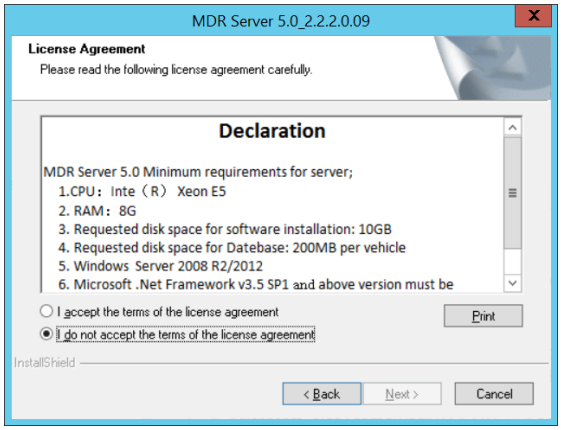
The installation window as shown in *MDR Server Installation Figure 5* will be displayed. Click **NEXT** to begin the installation.

You can configure the destination location which is shown in *MDR Server Location Figure 7*. Although, this is not recommended.

Warning: It is NOT recommended to change the default location.



MDR Server Installation Figure 5



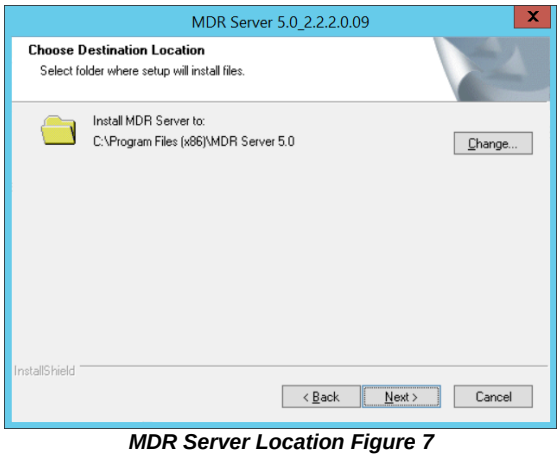
MDR Server Declaration Figure 6

The next step is to select the MDR Server features. *MDR Server Feature Setup Figure 8* shows the services that are available. Please ensure that **ALL** services are ticked to be installed.

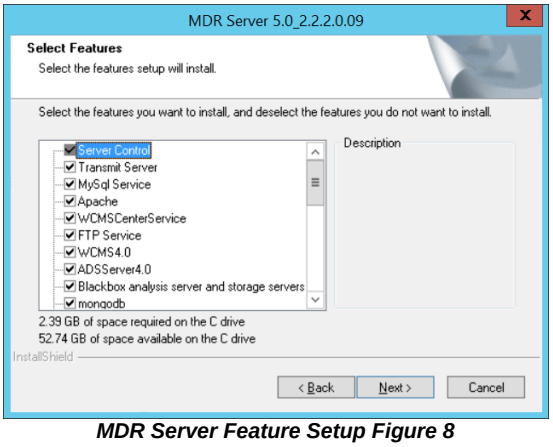
Click **INSTALL** to start the installation. Close other software during this process.

See *MDR Wi-Fi Server Port Configuration Figure 11*. The default **MESSAGE** and **VIDEO** ports should not be changed. If you are already using these ports on your network, you will have to change the ports within your other applications.

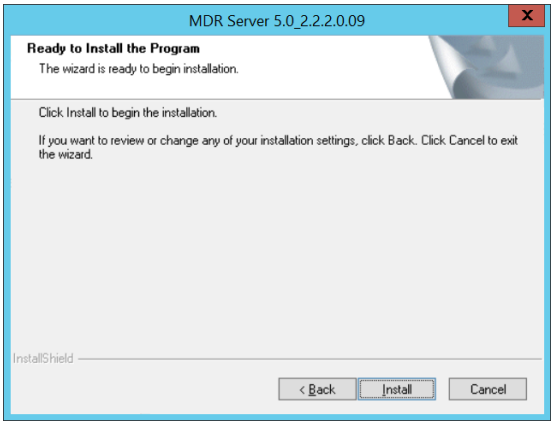
- IP: 192.168.14.193 (IP address of the network adaptor of the Windows Server).
- IP: 12.345.6.78 (Public IP address of the Firewall)



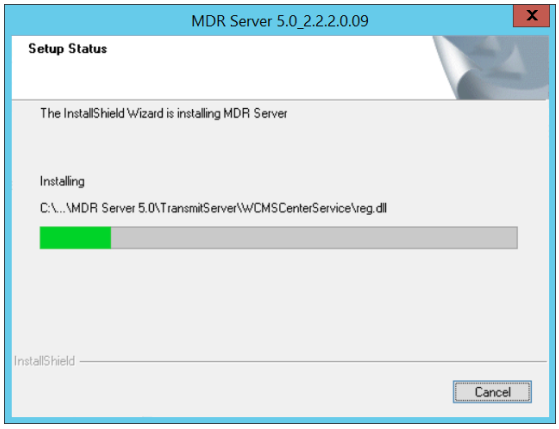
MDR Server Location Figure 7



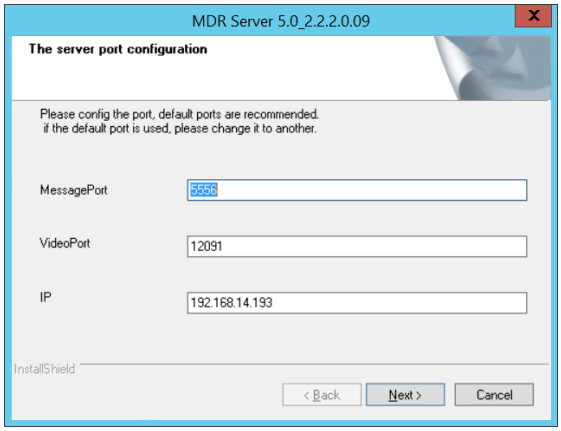
MDR Server Feature Setup Figure 8



MDR Server Installation Figure 9



MDR Server Setup Status Figure 10



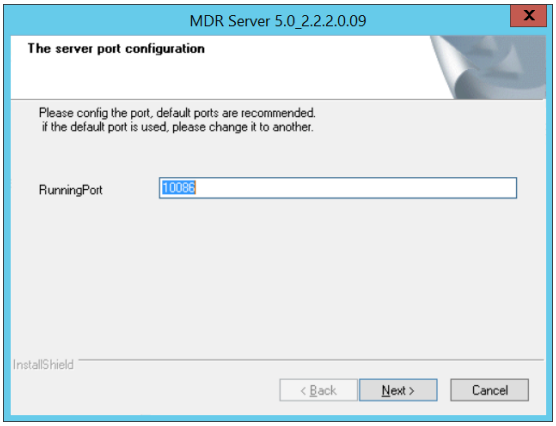
MDR Wi-Fi Server Port Configuration Figure 11

The setup status is displayed on screen. See *MDR Server Setup Status Figure 10*. You will see various services being installed, this period is dependent on your server configuration. In general, allow approximately 15 minutes for your MDR Server installation.

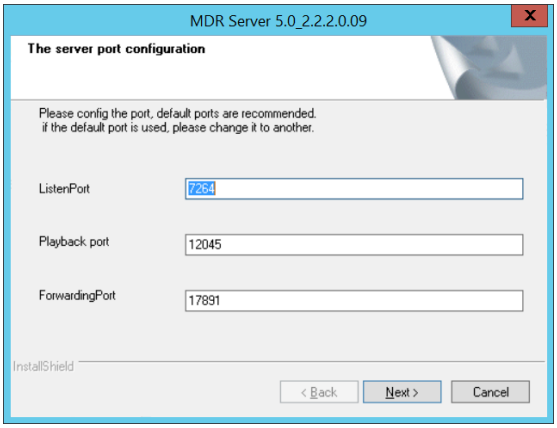
The port configuration shown in *Running Port Configuration Figure 12* to *Data and Blackbox Port Configuration Figure 15* is automatically populated by the software.

Do not change the default ports. If you have already used these ports on your network, please assign different ports in your other software.

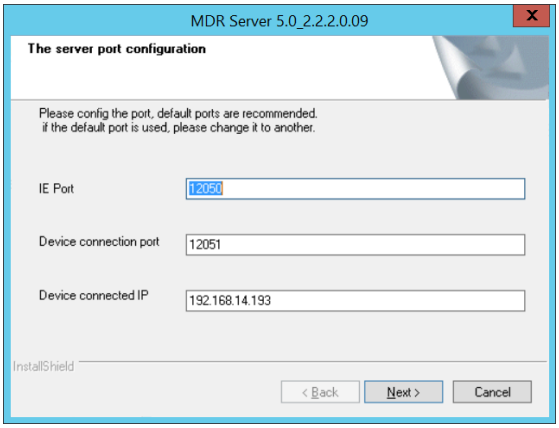
Warning: Any changed ports MUST be noted as this is used to configure the MDR unit.



Running Port Configuration Figure 12



Listen, Playback and Forwarding Port Configuration Figure 13



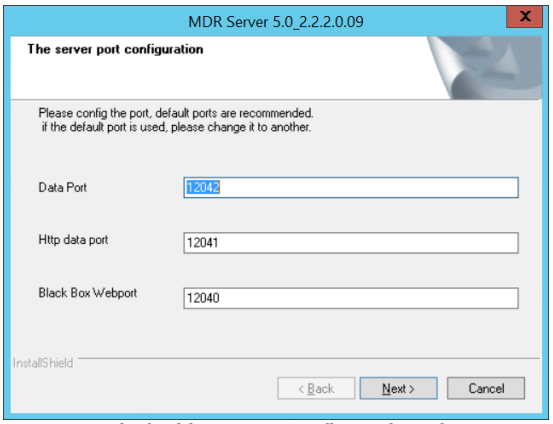
IE and Device Port Configuration Figure 14

Warning: DEVICE CONNECTED IP (*IE and Device Port Configuration Figure 14*) **MUST be a STATIC PUBLIC IP address of the Mobile Network Server (Firewall in some cases).**

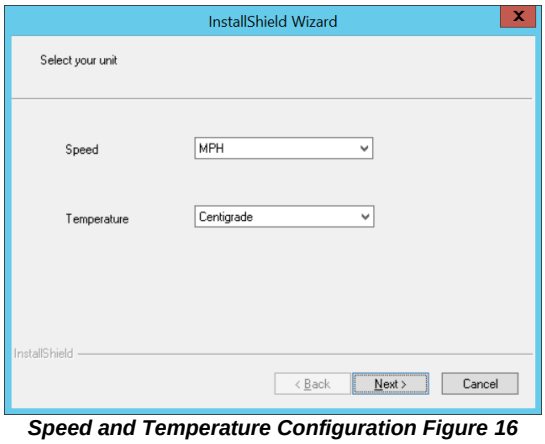
You can now configure the **SPEED** and **TEMPERATURE** units. See *Speed and Temperature Configuration Figure 16*.The options are miles per hour or kilometres per hour. Temperature can either be set to degrees Celsius or Fahrenheit.

Web Port Configuration Figure 17 shows the settings used for the **WEB PORT**.

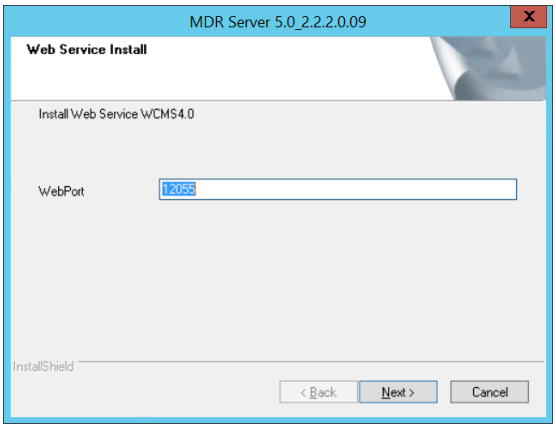
Do not change the default web port. If you have already used this port on your network, please assign a different port in your other software.



Data and Blackbox Port Configuration Figure 15



Speed and Temperature Configuration Figure 16



Web Port Configuration Figure 17

Certificate import is used for the mobile apps' push notifications. A push notification is a message that pops up on a mobile device. App publishers can send them at any time; you don't have to be in the app or using their devices to receive them.

See *MDR Server Local Machine Figure 18*. By default, Current User is chosen. Change this to **Local Machine.**

Do not change the path specified in *MDR Server Certificate File Name Figure 19*. This is an auto-populated path. Ensure the path is "**MDR Server 5.0\TransmitServer\PushService\aps_production.p12**".

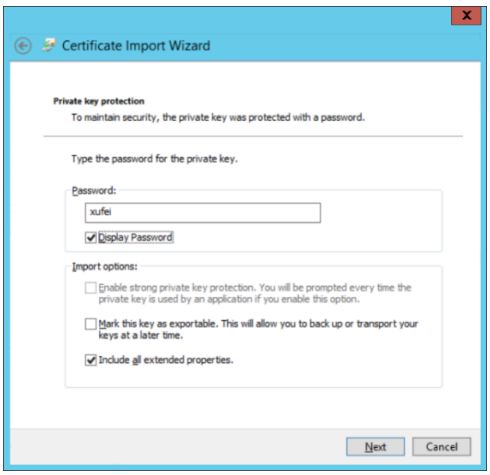
Type the password into the field shown in *MDR Server Certificate Password Figure 20*. The password is "**xufei**".

Tick "include all extended properties". See *MDR Server Certificate Password Figure 20*.

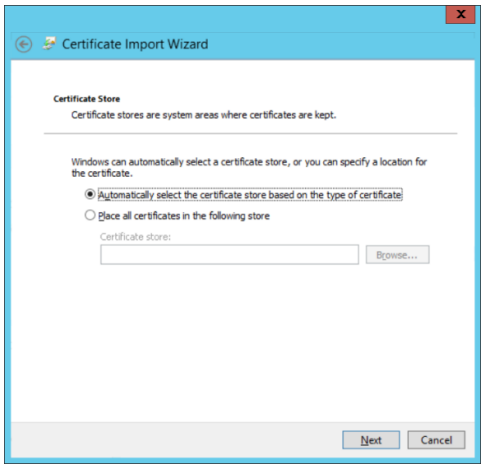
Tick "Automatically select the certificate store based on the type of certificate". See *MDR Server Certificate Store Figure 21*.

MDR Server Local Machine Figure 18

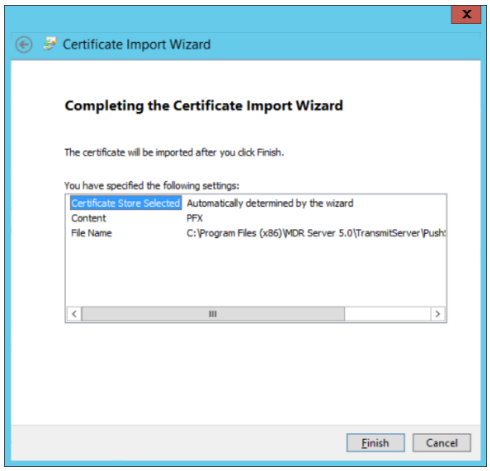
MDR Server Certificate File Name Figure 19



MDR Server Certificate Password Figure 20

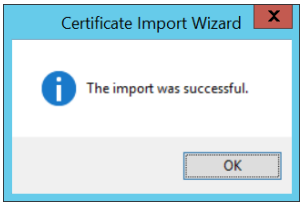


MDR Server Certificate Store Figure 21

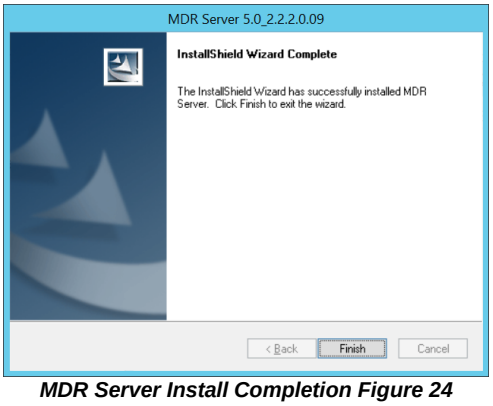


MDR Server Completing Certificate Import Figure 22

Click **FINISH** to complete the final step of the installation. See *MDR Server Install Completion Figure 24*.



MDR Server Certificate Successful Import Figure 23



MDR Server Install Completion Figure 24

2.3 MDR Server Configuration

After installing MDR Server, go to the **MDR SERVER** folder as shown in *MDR Server Menu Figure 25*.

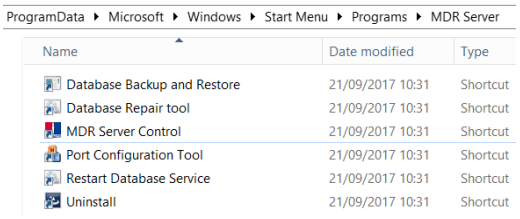
To access the MDR Server Control window, you can click on **MDR Server Control** or right-click the MDR Server icon. As shown in *Displaying MDR Server Control Figure 26*.

Now, click the **OPEN/HIDE WINDOW** option as shown in *Accessing MDR Server Control Window Figure 27*.

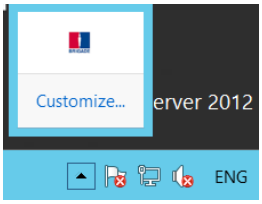
If the software is not open, ensure it is **RUN AS ADMINISTRATOR** as shown in *MDR Server Control Menu Figure 31*.

Use the following steps to ensure MDR Server always runs as administrator.

- Right-click MDR Server (*MDR Server Right click menu Figure 28*) then click **Properties**.
- Go to the **Compatibility** tab, under **Privilege Level**, tick **Run this program as administrator**. See *Privilege Level Figure 29*.
- Click **Apply** to ensure all changes are saved.

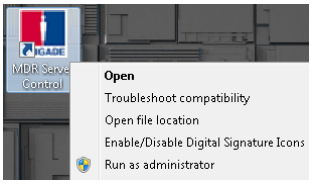


MDR Server Menu Figure 25

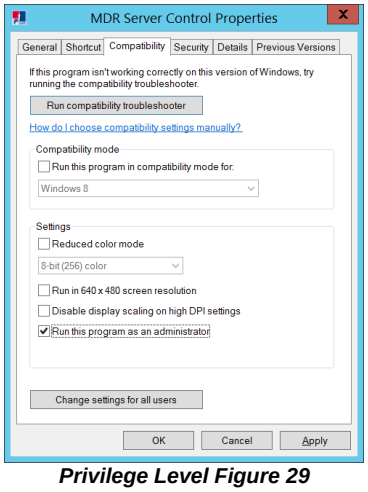


Displaying MDR Server Control Figure 26

Accessing MDR Server Control Window Figure 27



MDR Server Right click menu Figure 28

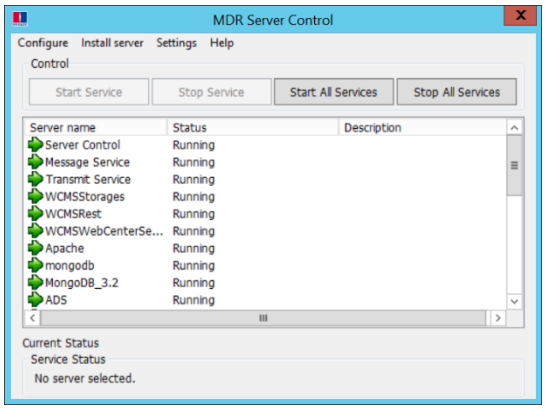


Privilege Level Figure 29

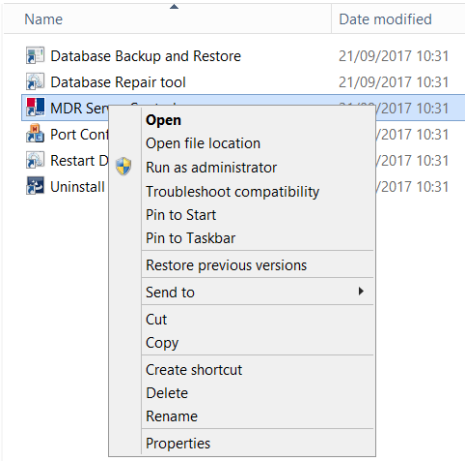
Once the window opens as shown in *MDR Server Control Window Figure 30*, click **CONFIGURE** then **CONFIGURE MESSAGE SERVER.**

The window shown in *MDR Server Message Server Configuration Figure 32* will be displayed. The following configuration is used:

- Server IP: 127.0.0.1 (loopback IP address of server)
- Server Port: 5556



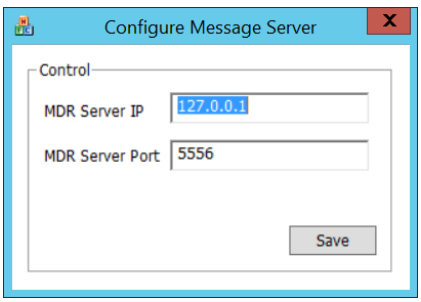
MDR Server Control Window Figure 30



MDR Server Control Menu Figure 31

Note: If not all MDR Server services are running (*MDR Server Control Window Figure 30*). There are a few steps to attempt to fix this issue:

- Exit the MDR Server control window and run the application as administrator. See *MDR Server Control Menu Figure 31*.
- Ensure that the MDR Server installation is not expired – check Brigade website for the latest license files.
- Install the latest Microsoft .NET Framework (3.5 is the minimum).
- Check the MDR Server IP in *MDR Server Message Server Configuration Figure 32*. Click **SAVE** on the configuration of the Message Server window.
- Restart the Windows Server.
- If none of the above steps work, reinstall the software.



MDR Server Message Server Configuration Figure 32

A brief description of each MDR Server Control service is shown in the table below.

(1) Server Control: manages all services. It can restart automatically everyday (setting).	(2) Message Service: creates TCP connection from server to MDR. Manages client software login states and registers MDR states. Transports commands from server to MDR and writes GPS/alarm data into mongodb using MDR5 protocol.
(3) Transmit Service: forwards media data from MDR to client software using transmit port.	(4) WCMSStorages: storing GPS and alarm data into MYSQL database (MDR 400).
(5) WCMSRest: querying GPS and alarm data from MYSQL database.	(6) WCMSTransmitors: sends GPS data to GPS client software (obsolete).
(7) WCMSWebCenterService: supports MDR-Dashboard 5.0 remote firmware batch upgrades.	(8) Mongodb: Mongo Database service, for storing GPS, alarm data and metadata from MDR 500 (MYSQL used for MDR 400).
(9) ADS: Auto Download System is used to avoid too many MDR-Dashboard 5.0 connections to one Windows Server.	(10) ClientBalance: If there are more than 1 MDR Server 5.0 installations on different servers, it keeps MDR Server 5.0 in balance by assigning which clients connect to which server
(11) n9m_proxy: Works as a proxy server to set MDR parameters remotely.	(12) ARMSStorageSever: Stores metadata (from auto download function) into mongodb.
(13) ARMSRestServer: Analyses metadata file path (from auto downloads) in MYSQL database.	(14) ServiceSTPlay: For MDR-Dashboard 5.0 remote playback server data.
(15) AlarmService: For alarm service program, used internally.	(16) ClientAccessService: For sending MDR online/offline messages to clients. For MDR-Dashboard 5.0 to receive MDR online/offline messages. For transporting orders from MDR-Dashboard 5.0 to MDR.
(17) Redis Service: Buffers MDR online/offline information for mobile app queries.	(18) PushService: For pushing alarms to mobile apps.
(19) OnlineServer: Manages MDR online/offline messages and updates clients with this information.	(20) EvidenceService: For managing evidence data (video, snapshots) upload to Windows Server and remotely access with MDR-Dashboard 5.0.
(21) CmdServer: commands sent to MDR Server 5.0.	(22) WCMSRunningService: For supporting MDR-Dashboard 5.0 remote firmware batch upgrades. Adds vehicles automatically to MDR-Dashboard 5.0.
(23) CenterManageService: For updating center data to related MDR-Dashboard 5.0.	(24) ServiceSTMgr: For server management, used internally.
(25) ServiceSTWorker: For server management, used internally.	(26) ServiceSTconfigure: For server management, used internally
(27) .FTPServer: Works as FTP server for saving data (video, snapshots, firmware etc.).	

Double-click on **MESSAGE SERVICE** as shown in *MDR Server Control Window Figure 30*. This will open another window which shows the current state of the network. See *MDR Server Message Logs View Figure 34*.

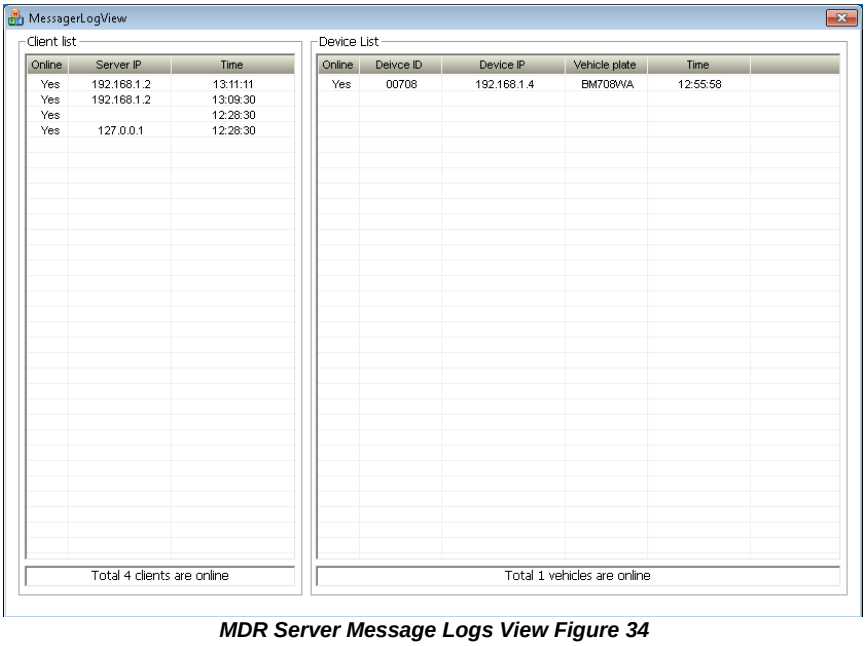
In *MDR Server Message Logs View Figure 34*, the IP addresses of the connected clients are shown in the left column. This includes the server loopback address. If an MDR has been configured correctly it will appear online in the right column.

Note: IP addresses are assigned dynamically by the mobile network. In addition, the MDR toggles the mobile network periodically if no activity is detected.

MDR Server 5.0 has a prompt message that will appear on the Windows Server to inform the system administrator that the MDR Server is nearing its expiration date. See *MDR Server Expiry Prompt Figure 33*.

The system administrator will need to download a new 1-year license file from Brigade's website (Product Support area). Copy this file to the following path **C:\Program Files (x86)\MDR Server\TransmitServer**. It will overwrite the existing license file.

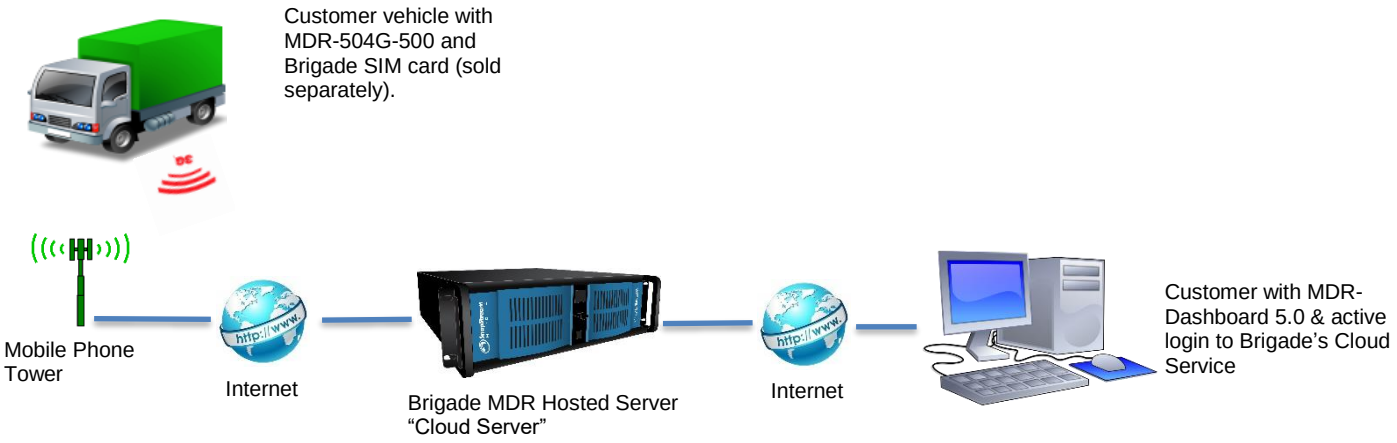
MDR Server Expiry Prompt Figure 33



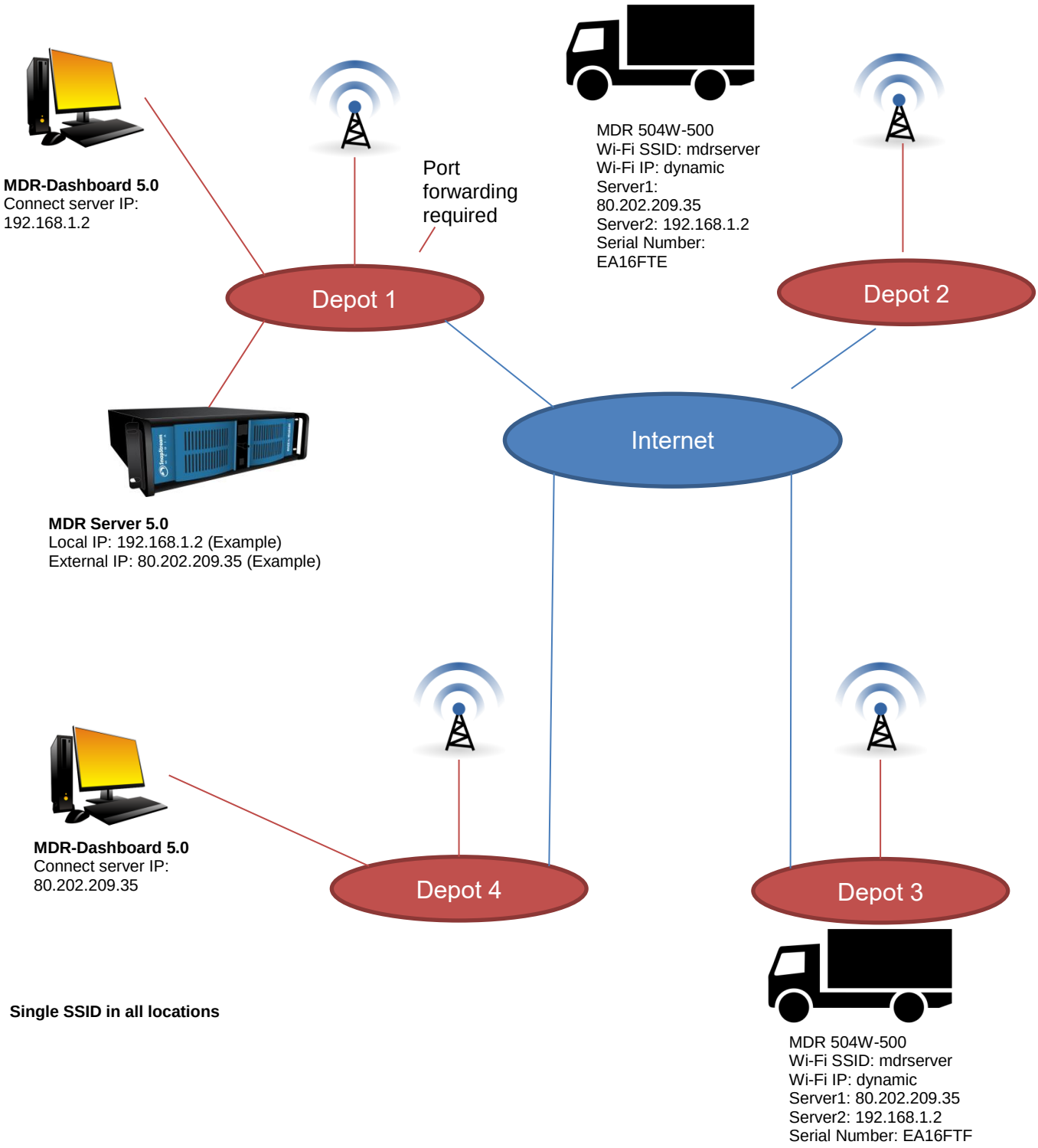
MDR Server Message Logs View Figure 34

2.4 Hardware Communication Options

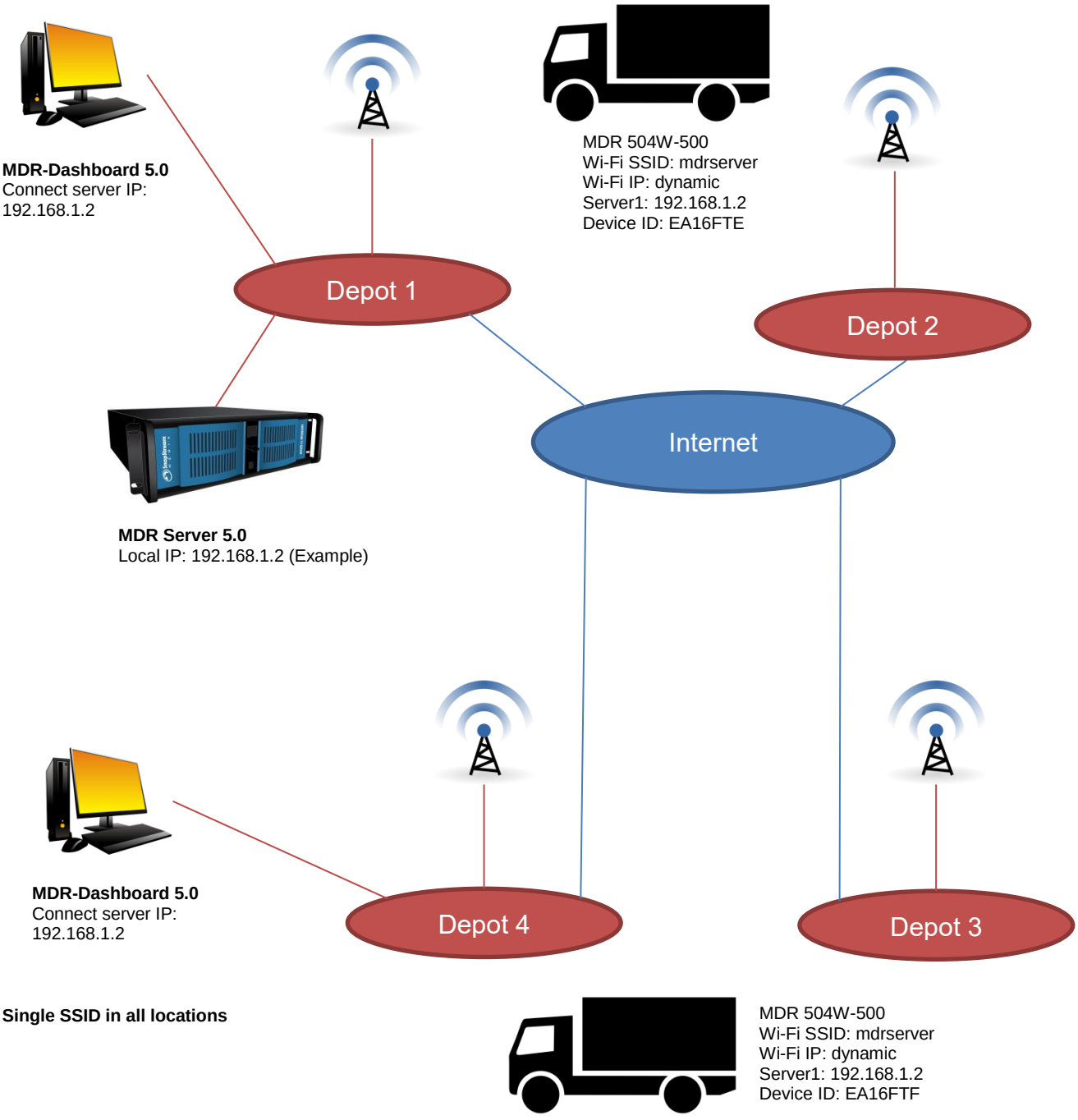
Each MDR will need its own mobile network enabled sim card. You login to MDR-Dashboard 5.0 to view live video, track vehicles in real-time and download video/metadata when required.



Option 1 - Hosted Mobile Network Figure 35



Option 2 – Wi-Fi only, multi depot, without VPN Figure 36



Option 3 - Wi-Fi only, multi depot, with VPN Figure 37

3 MDR-Dashboard 5.0 Requirements & Installation

MDR-Dashboard 5.0 software is used for advanced local playback, analysis, downloading, GPS tracking, vehicle information and events/log display. When an MDR is out of network range, features that are network dependent will no longer function. MDR-Dashboard 5.0 has the following features:

- Real-time Preview
- Multi Vehicle Monitoring
- Playback of MDR Server and Online MDR data
- Playback of Local Files data (network independent)
- Clipping and Downloading Data (network independent)
- Evidence Management
- Auto Download Scheduling
- Basic Data Management (network independent)
- Alarm Center

Table 9: Differences between MDR-Dashboard 5.0 and MDR-Player 5.0

MDR-DASHBOARD 5.0	**MDR-PLAYER 5.0**
Installation Required	Executable
Full Featured	Compact – limited features
View and Download Recordings	View Recordings
Sources – MDR Server, HDD/SD, Online MDR and Local Files	Sources – Standard and Export Downloads

For more information on MDR-Player 5.0 please refer to MDR 500 Series Installation&Operation Guide.

3.1 MDR-Dashboard 5.0 Requirements

Table 10: Minimum requirements for MDR-Dashboard 5.0

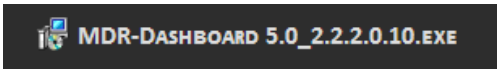
COMPONENT	**MINIMUM REQUIREMENTS**
CPU (Central Processing Unit)	INTEL i3-3220 and above 1 GHz (x86 CPU) or 1.4 GHz (x64 CPU)
RAM (Random Access Memory)	4GB
Requested HDD space for software installation	367 MB
Video	Intel® HD Graphics 4000 or equivalent
Operating System	Windows™ 7, 8 or 10
Web browser	Internet Explorer 10
Software	Flash Player (up-to-date)
Resolution	1280x760

Table 11: Recommended requirements for MDR-Dashboard 5.0

COMPONENT	**RECOMMENDED REQUIREMENTS**
CPU (Central Processing Unit)	INTEL i5 and above 1.9 GHz (x64 CPU) Dual core
RAM (Random Access Memory)	8GB
Requested HDD space for software installation	367 MB
Video	Intel® HD Graphics 5000 or equivalent
Operating System	Windows™ 7, 8 or 10
Web browser	Internet Explorer 10
Software	Flash Player (up-to-date)
Resolution	1680 x 1050

3.2 MDR-Dashboard 5.0 Installation

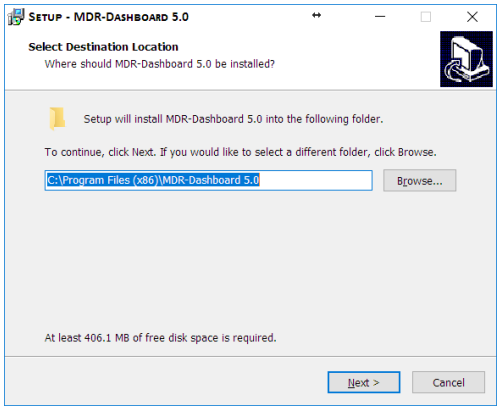
Install MDR-Dashboard 5.0 on the client PC. (Administrator rights are required). Double-click the installation file shown in *MDR-Dashboard Icon Figure 38*.



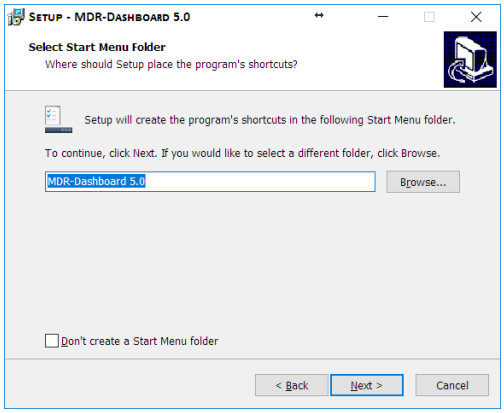
MDR-Dashboard Icon Figure 38

There may be a security warning pop-up which may be ignored. Click **RUN**. The setup wizard window will then be displayed. Click **NEXT** to begin the installation. See *MDR-Dashboard Setup Figure 39*.

You can configure the destination location (if there is not enough free disk space) which is shown in *MDR-Dashboard Location Figure 40*. **It is NOT recommended to change the default location**.

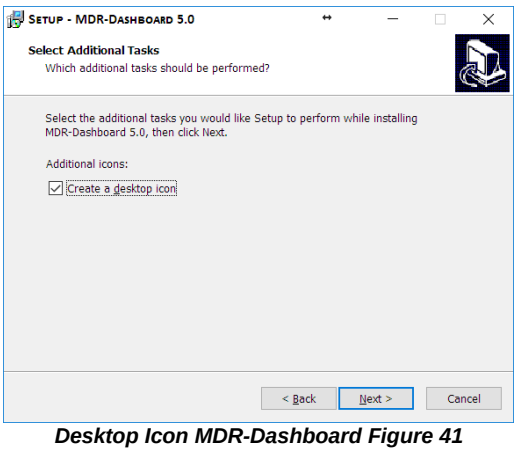


MDR-Dashboard Setup Figure 39



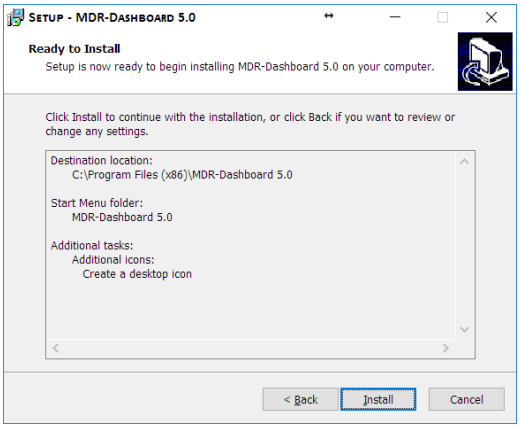
MDR-Dashboard Location Figure 40

Referring to *Desktop Icon MDR-Dashboard Figure 41*, you can choose if a desktop icon is created.



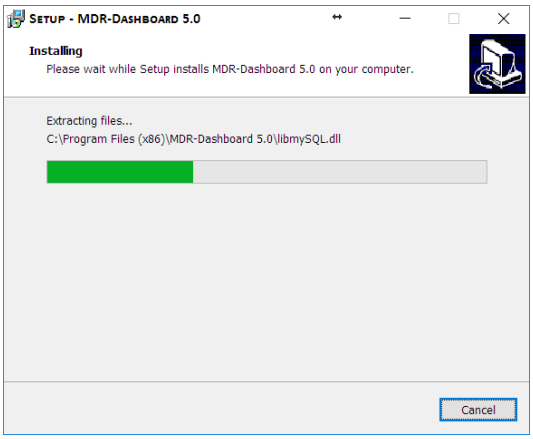
Desktop Icon MDR-Dashboard Figure 41

You are prompted to click **INSTALL** to begin the installation. This is indicated in *Install MDR-Dashboard Figure 42*.



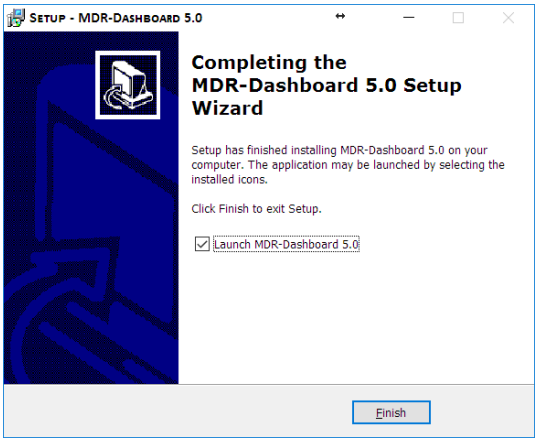
Install MDR-Dashboard Figure 42

The progress of the installation is indicated in *MDR-Dashboard Installation Figure 43*.



MDR-Dashboard Installation Figure 43

MDR-Dashboard Launch Step Figure 44 depicts the final step; you may choose to launch the software. Tick the box and click **FINISH**.



MDR-Dashboard Launch Step Figure 44

4 Wi-Fi Configuration

4.1 MDR Unit Configuration (Wi-Fi)

4.1.1 Mobile Digital Recorder Requirements

The setup described in this installation guide requires a Wi-Fi enabled MDR.

- Wi-Fi antenna (included)
- GPS antenna (included)

Prior to any configuration, restore the MDR factory settings by following, **LOGIN → SETUP → MAINTENANCE → RESET → RESTORE**.

Browse to this Wi-Fi network page using **SETUP → BASIC SETUP → NETWORK → Wi-Fi.**

Enable should be set to On. Once enabled, the settings below will become active, this will turn on the Wi-Fi module. See *MDR Wi-Fi Settings Figure 45*.

SSID is the service set identifier. It is used to identify a wireless LAN and is usually unique to an area. This is where you will enter the name of the wireless network that the MDR will connect to.

Encryption refers to protocols used to protect your network. MDR supports WEP and WPA/WPA2. We suggest using WPA2, as it is the newer encryption form and thus the most secure. This is case-sensitive.

Password is the wireless network password, this should be entered carefully as it is case-sensitive.

MDR Wi-Fi Settings Figure 45

Browse to this Wi-Fi network page using **SETUP → BASIC SETUP → NETWORK → Wi-Fi→PAGE DOWN.**

Static IP is used to turn DHCP off or on. Once enabled, the settings found below will become active. Only use static IP if you are experiencing an unstable connection, this is not recommended for fleets of vehicles.

IP Address refers to the internet protocol address of the wireless module. This address is used to join the wireless network.

Subnet Mask is used to identify the network address of an IP address. By default, this is 255.255.255.000.

Gateway helps route network traffic and is the IP address of the network gateway.

MDR Wi-Fi Settings 2 Figure 46

Browse to this Wi-Fi module page using **SYS INFO → MODULES → NETWORK → Wi-Fi.**

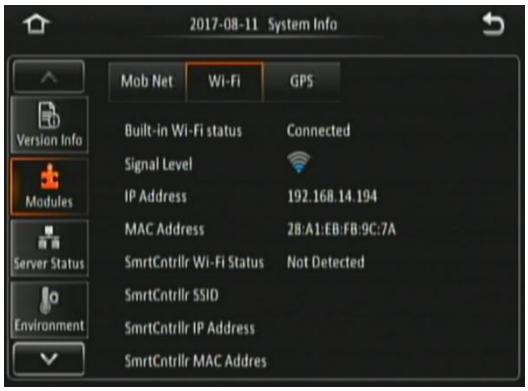
Built-in Wi-Fi status indicates the status of the Wi-Fi network connection. The different states are DETECTED, NOT DETECTED, CONNECTING, CONNECTED, CONNECTION FAILED and OBTAINING IP ADDRESS (DHCP). Once it has successfully connected to a Wi-Fi network then the status will change to CONNECTED.

Signal Level will display the power level of the signal in a visual form  . The more blue bars you see, the better the signal level is.

IP Address refers to the IP address obtained by the wireless module.

MAC Address refers to media access control address which is a unique identifier. This is assigned to network interfaces for communications at the data link layer of a network segment. This consists of 6 groups of 2 hexadecimal digits.

Smart Controller (SmrtCntrllr) settings are currently unused.



Sys Info Wi-Fi Module Figure 47

Browse to this Server page using **SETUP → BASIC SETUP → NETWORK → SERVER.**

Center Server refers to the Windows Server. A maximum of 6 center servers can be saved. An MDR can connect to a maximum of 2 servers using the same protocol type.

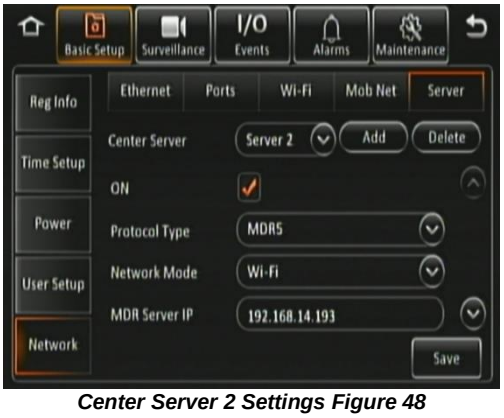
Add is used to add another center server, a new blank center server page is displayed with a new server number.

Delete removes the currently displayed center server.

ON enables the current center server. MDR will attempt to connect to this server.

Protocol Type refers to the protocol used by the MDR unit to send its data (video and metadata) to the MDR Server. By default, this is set to MDR5. Maintenance is not currently used.

Network Mode refers to the network communication module used to communicate with the MDR Server. The options are Ethernet, Mobile Network and Wi-Fi. This indicates the MDR will connect to the server using its Wi-Fi module.



Center Server 2 Settings Figure 48

Browse to this Server page using **SETUP → BASIC SETUP → NETWORK → SERVER→PAGE DOWN.**

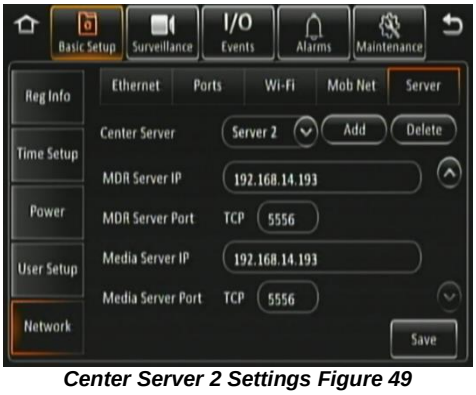
MDR Server IP is the public IP address of the firewall which forwards any traffic to the Windows Server, or IP address of the Windows Server hosting the MDR Wi-Fi Server. Example: 192.168.14.193 is the IP address of the Windows Server hosting the MDR Wi-Fi Server.

MDR Server Port is used for device access to server. By default, this is 5556.

Media Server IP should be the same as MDR Server IP.

Media Server Port should be the same as MDR Server Port. By default, this is 5556.

Save all the changes and exit the menu on the MDR. The MDR will then connect to the MDR Wi-Fi Server.



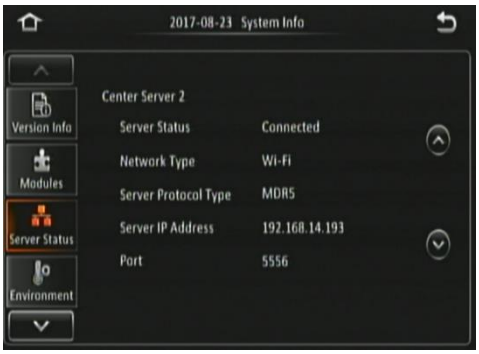
Center Server 2 Settings Figure 49

Center Server refers to the MDR Windows Server. It will read CONNECTED or UNCONNECTED.

Network Type indicates the MDR will connect to the server using its Wi-Fi module.

Server Protocol Type by default, this is set to MDR5. Maintenance is not currently used.

Port refers to MDR Server port. By default, this is 5556.



Wi-Fi Server Status Figure 50

4.2 MDR-Dashboard 5.0 Configuration (Wi-Fi)

This is the PC software that is installed on the client PC. Multiple MDR-Dashboard clients may connect to a single MDR server. The limitation will be on the Windows Server's ability and bandwidth. This is because there is only one connection from the server to each MDR unit. The MDR-Dashboard 5.0 can display up to 500 online vehicles, any further vehicles are replaced by "**".

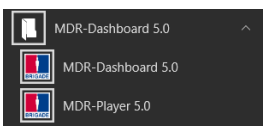
- Connect the client PC to the MDR Server Wi-Fi network.
- The client PC can also be connected to the domain with an Ethernet cable if you require network/internet access. Alternatively, the router may be configured to have internet access.

4.2.1 Logging into Server Mode (Wi-Fi)

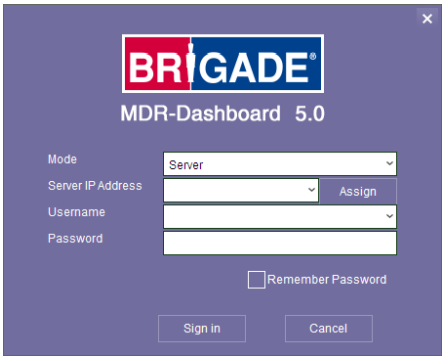
This operation is performed on the client PC. Go to **START → ALL PROGRAMS**, click on the MDR-Dashboard icon and run it as administrator as shown in *MDR-Dashboard Start Menu Figure 51*.

You are then presented with the MDR-Dashboard Login Screen. See *MDR-Dashboard Wi-Fi Login Figure 52*. Using the dropdown menu, you must choose the **SERVER** option.

You may type the server IP directly into *MDR-Dashboard Wi-Fi Login Figure 52* or follow the steps below.



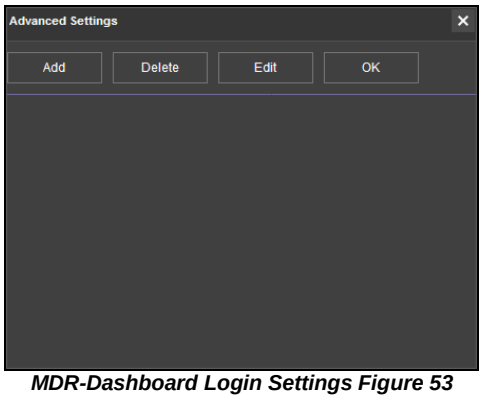
MDR-Dashboard Start Menu Figure 51



MDR-Dashboard Wi-Fi Login Figure 52

Click on **ASSIGN** which will bring up the window shown in *MDR-Dashboard Login Settings Figure 53*. This allows user to save several server names and their associated IP addresses.

Click on **ADD** which will display *Adding a Server Figure 54*. The **SERVER NAME** can contain up to 21 alphanumerical characters. **SERVER IP** should contain numerical values and be in xxx.xxx.xxx.xxx format.



MDR-Dashboard Login Settings Figure 53

Adding Wi-Fi Server Figure 55 indicates how the server has been named Wi-Fi Server and the IP has been entered as 192.168.1.14.

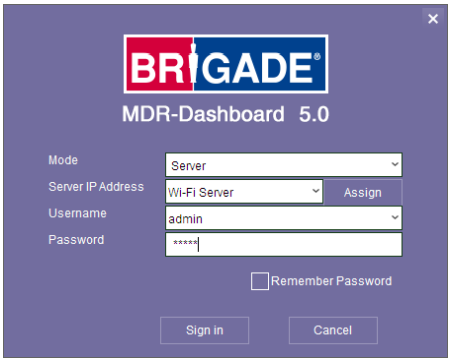
Once the details have been entered, click **OK** and the following window shown in *Wi-Fi Server Saved Figure 56* will be displayed.

If the incorrect **USER**, **PASSWORD** or **SERVER IP** is entered a "login failed" screen will be displayed.

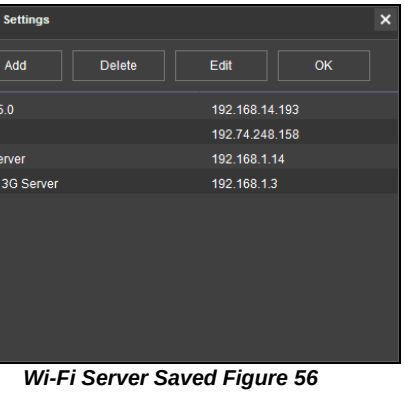
The **USER** by default is **admin** and the **PASSWORD** by default is **admin**. You may tick the **SAVE PASSWORD** if desired. Brigade recommends changing this password as sensitive data may be accessed within MDR-Dashboard.

Choose **WI-FI SERVER** and click **OK**. You will then be presented with *Wi-Fi Login Information Figure 57*.

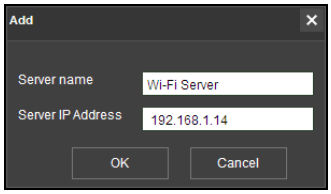
Click **OK** to login. A loading screen will be displayed like *Wi-Fi Loading Screen Figure 58*.



Wi-Fi Login Information Figure 57



Adding a Server Figure 54



Adding Wi-Fi Server Figure 55

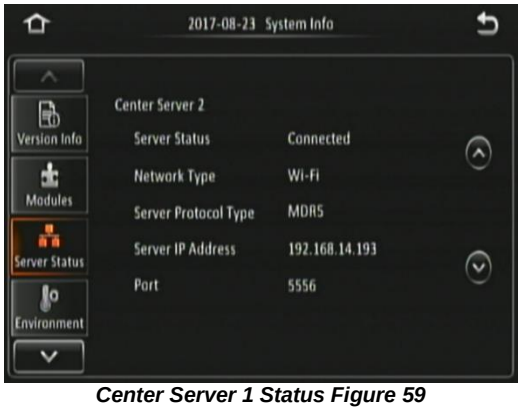
Wi-Fi Server Saved Figure 56

Wi-Fi Loading Screen Figure 58

4.2.2 Connecting an MDR to MDR-Dashboard 5.0 (Wi-Fi)

Center Servers indicate when the MDR unit has connected to a relevant MDR Server.

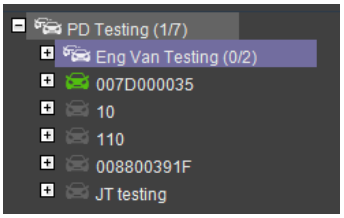
If the Chapter 4.1 MDR Unit procedure has been followed correctly on the MDR, access **SYS INFO → SERVER STATUS** and confirm the Center Server 1 has successfully connected. See *Center Server 1 Status Figure 59*.



Center Server 1 Status Figure 59

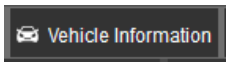
Once the above connection has been made, it may take a few minutes for the MDR unit to appear in MDR-Dashboard 5.0.

If the MDR automatically appeared, it will be found under a group labelled **TODAY'S DATE** and the MDR will be named using its **SERIAL NUM**.

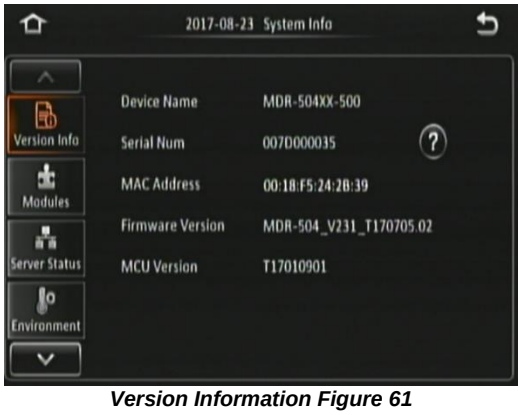


Automatically Found MDR Figure 60

Alternatively, manually connect the MDR to MDR-Dashboard by following the steps below:

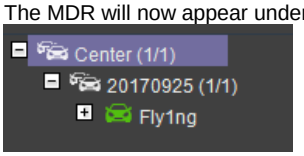
- In MDR-Dashboard 5.0, click **System Management**  found on the top right of the software.
- Browse to 

- Click 

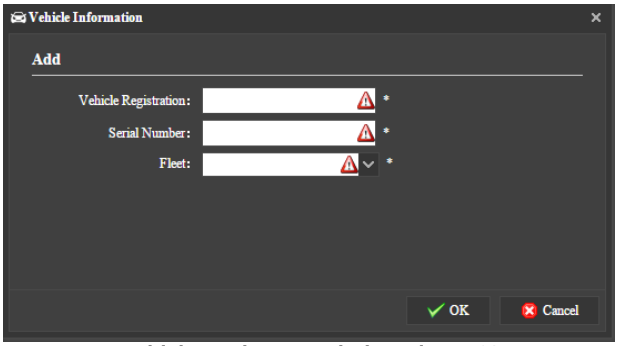


Version Information Figure 61

- Vehicle registration should match the vehicle's actual registration. This is your choice. The maximum is 50 alphanumeric characters.
- Ensure your **SERIAL NUMBER** from the MDR firmware is entered correctly. An example is shown in *Version Information Figure 61*.
- Once completed click **OK**
- The MDR will now appear under the group you assigned it to.



- It will appear online if the MDR is powered on or within its shutdown delay period



Vehicle Equipment Window Figure 62

5 Mobile Network Configuration

5.1 MDR Unit Configuration (Mobile Network)

5.1.1 Mobile Digital Recorder Requirements

The setup described in this installation guide requires a Mobile Network enabled MDR.

- Mobile Network/4G antenna (included)
- GPS antenna (included)
- Standard size SIM Card (not included) - required to connect to a mobile data network.

For the Mobile Network operation of an MDR, a SIM card with a data connection is required. This must be standard size. The SIM data connection must be activated and tested prior to being installed in the MDR.

Prior to any configuration, restore the MDR factory settings by following, **LOGIN → SETUP → MAINTENANCE → RESET → RESTORE**.

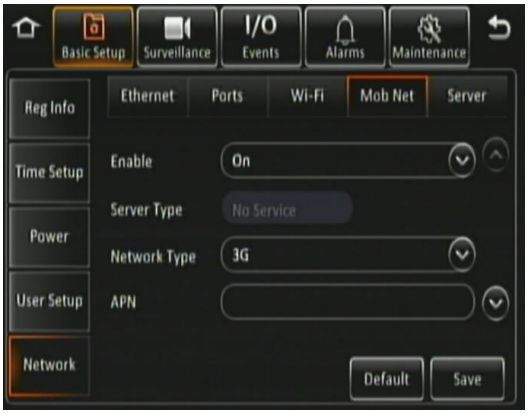
Browse to this Mobile Network page using **SETUP → BASIC SETUP → NETWORK → MOB NET.**

Enable is used to turn the mobile network module off or on. Once enabled, the settings found below will allow you to fill in your details.

Server Type is an auto-populated field, indicates the mobile network connection type.

Network Type refers to the type of mobile network connection that is used by the MDR to connect to the internet. Currently, 4G is the fastest connection speed. Set the network type to **3G** or **4G**. **MIX** can cause connectivity issues in low mobile network coverage areas.

APN refers to Access Point Name. This information is dependent on your mobile carrier network. Obtain APN, username, password, access number and authentication type settings from your SIM card provider.



Mobile Network Settings Page 1 Figure 63

Browse to this Mobile Network page using **SETUP → BASIC SETUP → NETWORK → MOB NET → PAGE DOWN.**

Username obtain from your SIM card provider.

Password obtain from your SIM card provider.

Access Number refers to the dial up phone number needed to connect to the network. By default, this is set to *99#

Certification refers to the authentication mode, can be set to either CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). CHAP should be chosen as this is a more secure authentication protocol. This is chosen by the network operator.

SIM Phone Number is not a required field. You may enter the phone number of the SIM card found inside the MDR for future reference.

Mobile Network Settings Page 2 Figure 64

Browse to this mobile network module page using **SYS INFO → MODULES → NETWORK → MOB NET.**

Connection Type shows the connection used to connect to network operators. The options are: GPRS/EDGE, CDMA, EVDO, WCDMA, TDSCDMA, FDD and TDD.

Module Status shows whether the MDR sees the presence of the mobile network module. This status will either show detected or not detected.

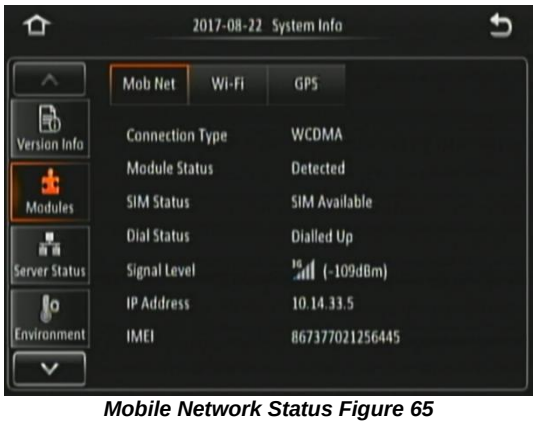
SIM Status shows whether the MDR sees the presence of a SIM card. The statuses are detected, not detected, available, not available and busy.

Dial Status indicates the SIM card's dial status, which can be dialled up, failed dial up and unknown error.

Signal Level will display the power level of the signal, this will be xxdBm format.

IP Address refers to the IP address obtained by the SIM card from the network provider.

IMEI refers to International Mobile Equipment Identity number. This is made up of 15 alphanumeric characters.



Mobile Network Status Figure 65

Browse to this Server page using **SETUP → BASIC SETUP → NETWORK → SERVER.**

Center Server refers to the MDR Windows Server. A maximum of 6 center servers can be saved. An MDR can connect to a maximum of 2 servers using the same protocol type.

Add is used to add another center server, a new blank center server page is displayed with a new server number.

Delete removes the currently displayed center server.

ON enables the current center server. MDR will attempt to connect to this server.

Protocol Type refers to the protocol used by the MDR unit to send its data (video and metadata) to the MDR Server. By default, this is set to MDR5. Maintenance is not currently used.

Network Mode refers to the network communication module used for to communicate with the MDR Server. The options are Ethernet, Mobile Network and Wi-Fi. This is discussed in further detail in *MDR 500 Series Network Connectivity SW&Infrastructure Manual*. This can be found on the Brigade website.

Center Server 1 Settings Page 1 Figure 66

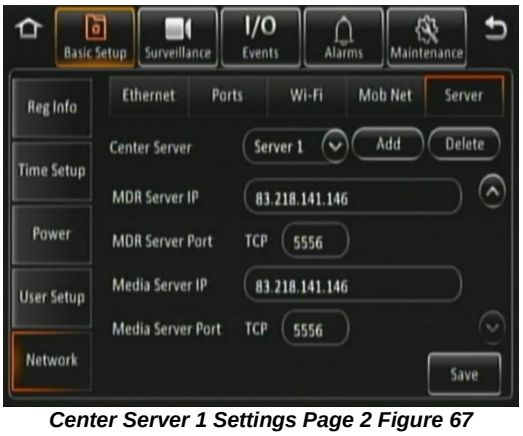
Browse to this Server page using **SETUP → BASIC SETUP → NETWORK → SERVER→ PAGE DOWN.**

MDR Server IP Public IP address of the firewall which forwards any traffic to the Windows Server or IP address of the Windows Server hosting the MDR Wi-Fi Server.

MDR Server Port is used for device access to server. By default, this is 5556.

Media Server IP should be the same as MDR Server IP.

Media Server Port should be the same as MDR Server Port. By default, is 5556.



Center Server 1 Settings Page 2 Figure 67

Center Server # displays the current server configuration details. A maximum of 6 center servers can be stored.

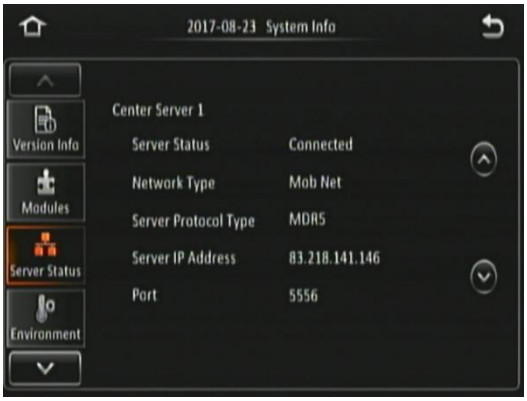
Server Status shows connection state of the chosen server. This can either be connected or unconnected.

Network Type indicates the type of connection interface the center server will use to attempt to communicate with the MDR Server. There are three options: Ethernet, Wi-Fi and Mobile Network.

Server protocol type shows the built-in proprietary communication protocol that will be used between the MDR unit and MDR Server. This can either be MDR5 or maintenance. Ensure that this is set to MDR5.

Server IP Address displays the IP address of the MDR Server. This can either be internal or external IP address.

Port shows the port used for communication between the MDR and MDR server.



Mobile Network Signal Information Window Figure 68

5.2 MDR-Dashboard 5.0 Configuration (Mob. Net.)

5.2.1 Logging into Server Mode (Mob. Net.)

Mode refers to the MDR-Dashboard 5.0 mode you would like to access. Options are **LOCAL** and **SERVER**.

Server IP Address displays the IP address of the MDR Server. This can either be an internal or an external IP address.

Port shows the port used for communication between the MDR and MDR server.

You may type the server IP directly into *Mobile Network MDR-Dashboard Figure 69* save the IP address with names. Follow the steps below:

- Click on **ASSIGN** which will bring up the window shown in *Mobile Network Advanced Settings Figure 70*. This allows you to save several server names and its associated IP addresses.
- Click on **ADD** which will display *Adding Mobile Network Server Figure 71*. The **SERVER NAME** can contain up to 21 alphanumerical characters. **SERVER IP ADDRESS** should contain numerical values and be in xxx.xxx.xxx.xxx format.

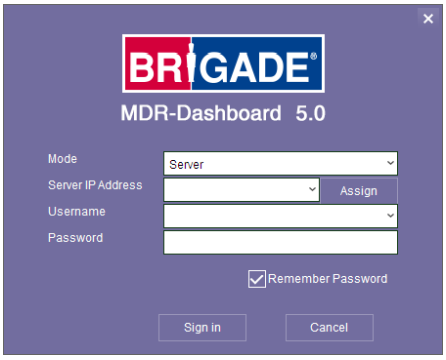
If you are accessing the Mobile Network server externally (outside the firewall) then use the external IP address. *External Mobile Network Server Figure 72* indicates how the server has been named Mobile Network Server External and the IP has been entered as 12.345.6.78.

If you are accessing the Mobile Network server internally (behind the firewall) then use the IP address of the MDR Windows Server. *Internal Mobile Network Server Figure 73* indicates how the server has been named Mobile Network Server Internal and the IP has been entered as 192.168.14.100.

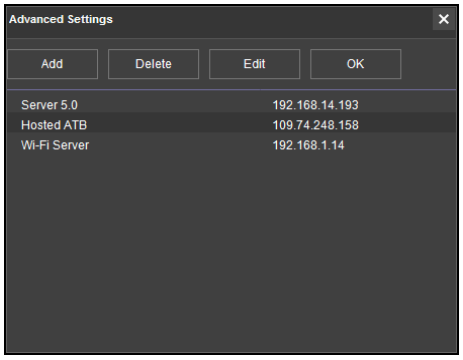
Choose **MOBILE NETWORK SERVER INTERNAL** and click **OK**. You will then be presented with *Mobile Network Login Figure 74*.

If the incorrect **USER**, **PASSWORD** or **SERVER IP** is entered a “login failed” screen will be displayed.

The **USER** by default is **admin** and the **PASSWORD** by default is **admin**. You may tick the **SAVE PASSWORD** if desired.

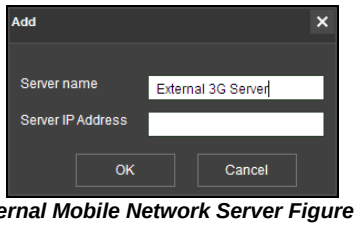


Mobile Network MDR-Dashboard Figure 69

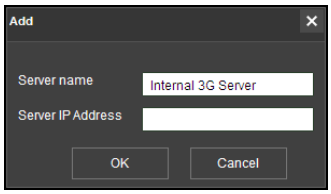


Mobile Network Advanced Settings Figure 70

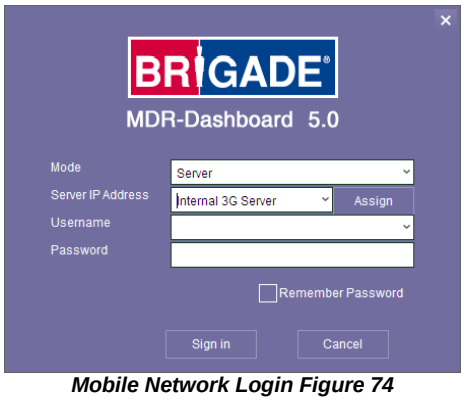
Adding Mobile Network Server Figure 71



External Mobile Network Server Figure 72



Internal Mobile Network Server Figure 73

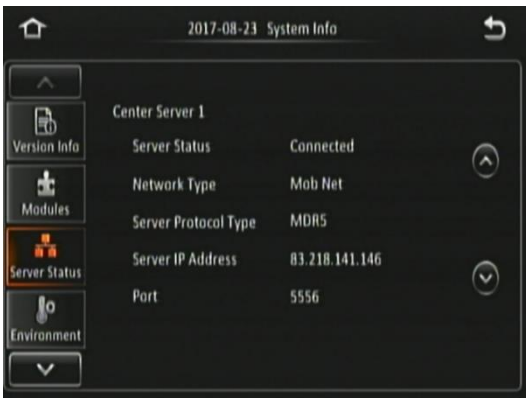


Mobile Network Login Figure 74

5.2.2 Connecting an MDR to MDR-Dashboard 5.0 (Mobile Network)

Center Servers indicate when the MDR unit has connected to a relevant MDR Server.

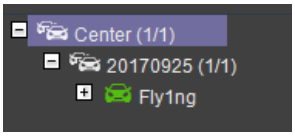
If the Chapter 4.1 MDR Unit procedure has been followed correctly, on the MDR, access **SYS INFO → SERVER STATUS** and confirm the Center Server 1 has successfully connected. See *Center Server 1 Status Figure 59*.



Center Server 1 Status Figure 75

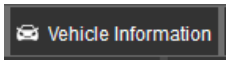
Once the above connection has been made, it may take a few minutes for the MDR unit to appear in MDR-Dashboard 5.0.

If the MDR automatically appeared, it will be found under a group labelled **TODAY'S DATE** and the MDR will be named using its **SERIAL NUM**.



Automatically Found MDR Figure 76

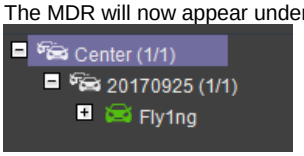
Alternatively, manually connect the MDR to MDR-Dashboard by following the steps below:

- In MDR-Dashboard 5.0, click **System Management**  found on the top right of the software.
- Browse to 

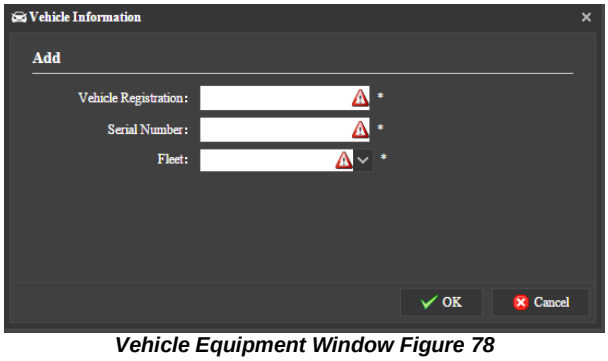
- Click 

Version Information Figure 77

- Vehicle registration should match the vehicle's actual registration. This is your choice. The maximum is 50 alphanumeric characters.
- Ensure your **SERIAL NUMBER** from the MDR firmware is entered correctly. An example is shown in *Version Information Figure 77*.
- Once completed click **OK**
- The MDR will now appear under the group you assigned it to.



- It will appear online if the MDR is powered on or within its shutdown delay period



Vehicle Equipment Window Figure 78

6 MDR-Dashboard 5.0 Operation

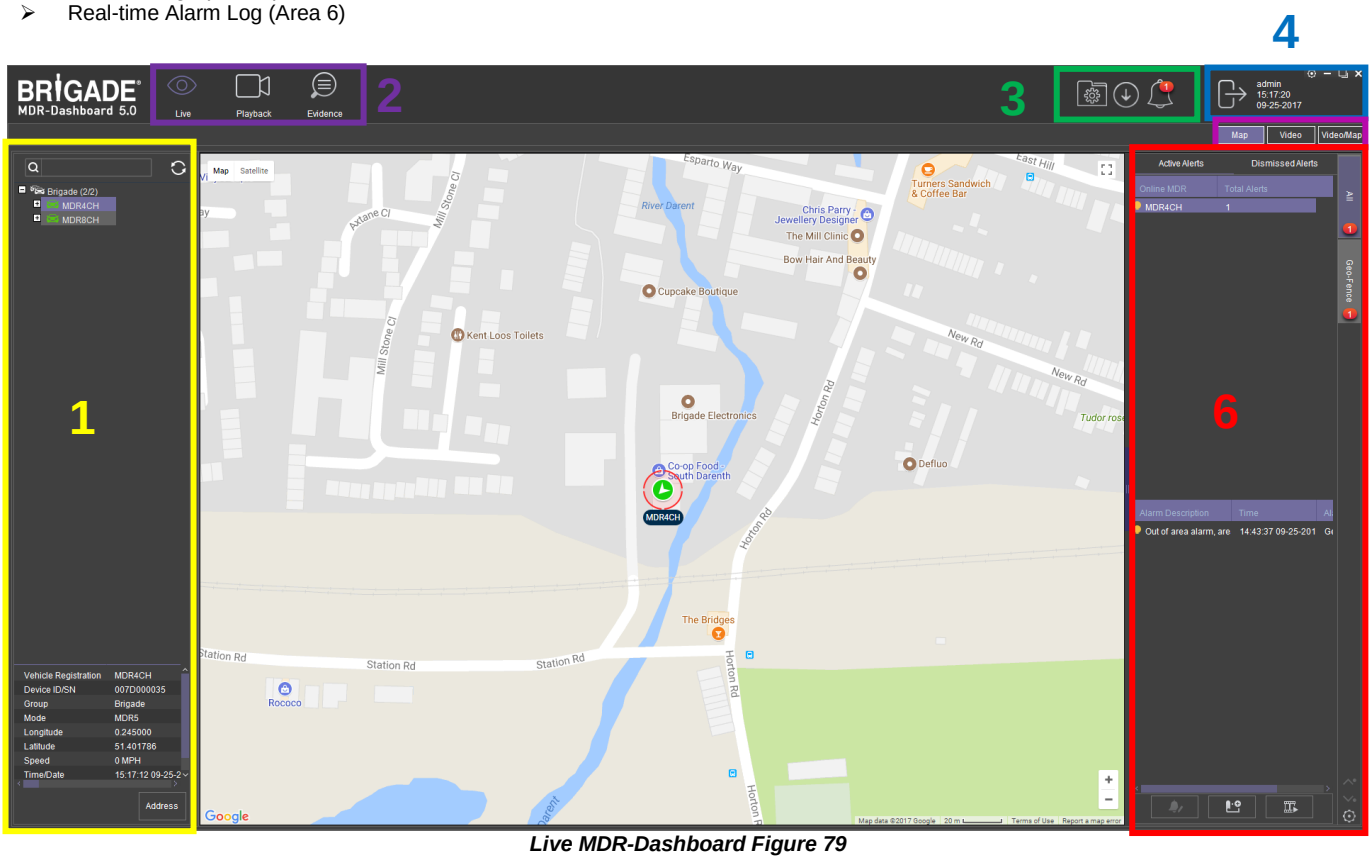
Usage scenarios must be clearly defined to meet and surpass the you' needs. See the table below which displays the different benefits achieved using Mobile Network or Wi-Fi.

Table 12: Mobile Network vs Wi-Fi Benefits

MOBILE NETWORK	WI-FI
Vehicles are away from company site	Vehicles must be in AP (access point) range and in an ON or shutdown delay (post-record) state
Remotely monitor vehicle operation (stream live MDR video).	Download data without physically going to the vehicle(s).
Instant alerts of alarms for immediate action.	Automatic alerts of alarms when vehicle returns within Wi-Fi range.
Instantly download MDR video to store and view alarms.	Automatic download of MDR video to store and view alarms when vehicle returns within Wi-Fi range.
Instantly upload evidence to the secure server.	No mobile network costs (Mobile Network).
Real-time GPS tracking (within mobile network coverage areas only)	Real-time GPS tracking (within wireless network only)

SERVER MODE allows you to access features such as **LIVE**, **PLAYBACK** and **EVIDENCE**. The following sub-chapters will explain these features and typical operation.
You are presented with the following window after logging in, *Live MDR-Dashboard Figure 79*.
MDR-Dashboard 5.0 consists of several key areas such as:

- Vehicle State (Area 1)
- Type of operation (Area 2)
- System Management, Downloads and Alarm Center (Area 3)
- User and System Settings (Area 4)
- View Settings (Area 5)
- Real-time Alarm Log (Area 6)

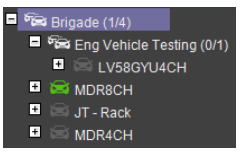


Live MDR-Dashboard Figure 79

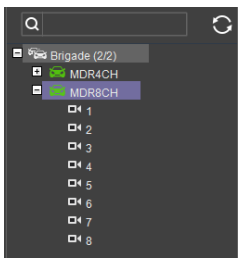
6.1 Vehicle State (Area 1)

This area will list the state (online or offline) of vehicles which have been configured. An example of an offline vehicle is shown in *Offline Vehicle Figure 80*. Camera channels may be expanded  to choose a camera to view.

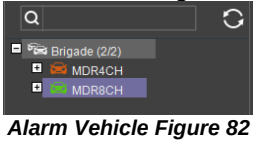
If an MDR is offline, camera channels cannot be accessed. Also, the vehicle icon is greyed out to indicate its offline state. An online vehicle example is shown in *Online Vehicle Figure 81*. The vehicle icon may display as a red icon if it currently in an alarm state. See *Alarm Vehicle Figure 82*.



Offline Vehicle Figure 80



Online Vehicle Figure 81



Alarm Vehicle Figure 82

The fleet **BRIGADE** may be right-clicked to show a sub-menu. See *Fleet Menu Figure 83*. This allows the list of vehicles in that fleet to be **EXPANDED** or **COLLAPSED**.

Use the **REFRESH** button  to update data for online vehicles. See *Fleet Menu Figure 83*.

To view the latest vehicle list please **LOGOUT** and **LOGIN** again. This will help update any changes in the list.

SEARCH is used to find specific vehicles based on the vehicle registration number. See *Fleet Menu Figure 83*. If there is more than one vehicle registration that contains the search data these vehicles will be displayed in list form for the user to choose from.

Quick information of the selected vehicle is shown below the tree structure in Area 1. Quick information consists of Vehicle Number, Device ID, Group, Type, Longitude, Latitude, Speed and Time. An example is shown in *Quick Information Figure 84*.

An advanced vehicle menu shown in *Vehicle Menu Figure 85* can be accessed by right-clicking a vehicle registration. This menu has the following options:

- MDR Settings
- Quality
- GPS Upload Rate
- Get Version
- IO settings
- Geo-Fence
- Remote Format
- Restart

MDR SETTINGS are used to access **ONLINE MDR** units' settings. Once **MDR SETTINGS** is accessed, *Brigade Loading Figure 86* is displayed.

Depending on the speed of the connection to the MDR, the login window is displayed after 1-5 minutes.

If you get the error shown in Online *MDR Settings Error Figure 87*, this means that the password you entered is incorrect.

There are two ways to fix this problem. Method one is to enter the correct firmware password, this is a temporary one-time access fix. Method two is to save the firmware password in the MDR-Dashboard settings menu, which is a permanent fix (unless someone changes the firmware login password on the MDR unit).

Method one:

- Click Confirm
- Enter Username and Password then click Login

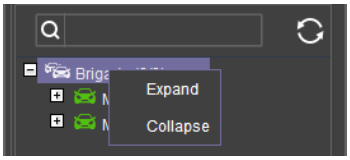
Method two:

- Click X to close the error prompt
- Click System Management
- Click MDR Information
- Click Update
- Enter Username and Password then click OK

See *Vehicle Settings Menu Setup Figure 89*, you can configure MDR settings related to: **Basic Setup**, **Surveillance**, **Events** and **Alarms**. This menu structure follows the MDR firmware.

QUALITY is used to switch between recommended, best frame rate, normal frame rate, normal resolution and best resolution. By default, this is set to Recommended.

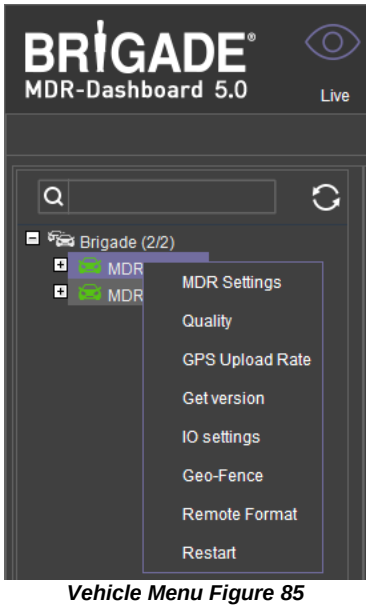
Online MDR GPS Upload Rate Figure 91 is used to configure the interval with which the MDR uploads GPS information to the server. By default, it is 10 seconds.



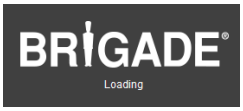
Fleet Menu Figure 83

Vehicle Registration	MDR8CH
Device ID/SN	0088003929
Group	Brigade
Mode	MDR5
Longitude	0.245378
Latitude	51.402358
Speed	0 MPH
Time/Date	15:25:49 09-25-2

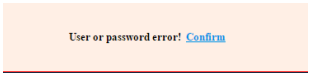
Quick Information Figure 84



Vehicle Menu Figure 85

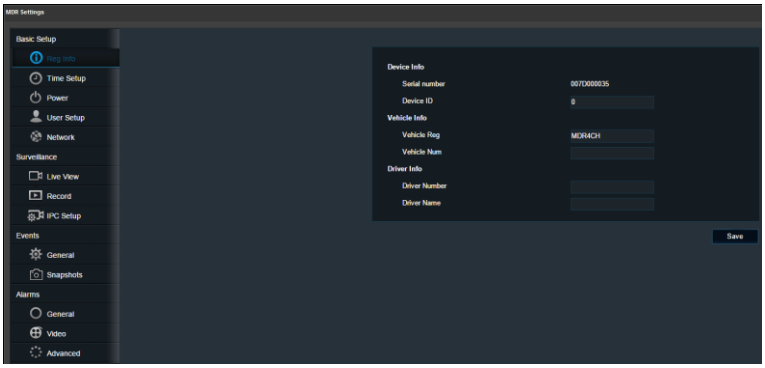


Brigade Loading Figure 86

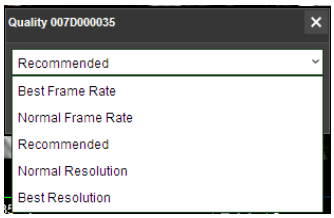


Online MDR Settings Error Figure 87

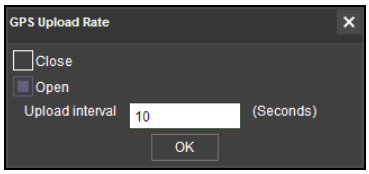
Online MDR Settings Menu Setup Login Figure 88



Vehicle Settings Menu Setup Figure 89



Online MDR Quality Setting Figure 90



Online MDR GPS Upload Rate Figure 91

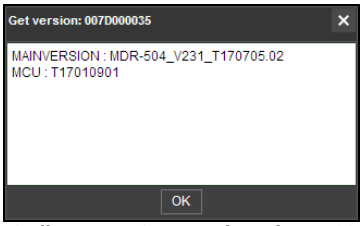
GET VERSION is used to obtain the current firmware and MCU version installed on the MDR. See *Online MDR Get Version Figure 92*.

IO SETTINGS are used to remotely control the alarm outputs found on the IO cable. These outputs can be set to high or low. It can also be set to auto revert to its previous state after a defined period. By default, state is low, auto revert state is off and duration is 30 seconds. See *Online MDR IO Settings Figure 93*.

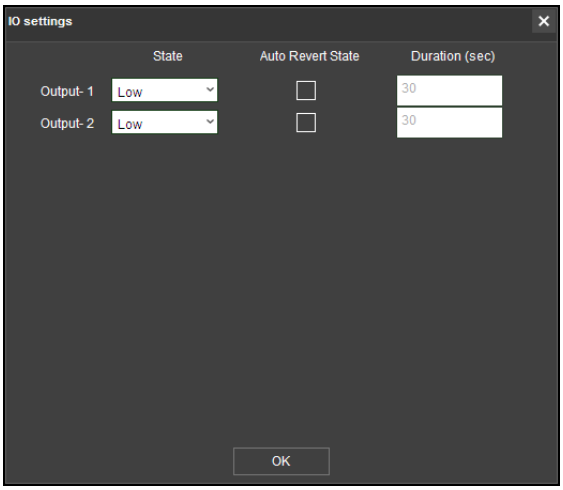
GEO-FENCE is used to add geo-fences. Geo-fences are used to send an alarm if a vehicle leaves or enters a geographical region. This region is setup by the user in MDR-Dashboard 5.0. Fence types are polygon, circle and line. Triggering conditions can be entry, exit and in or out. Geo-fences can be batch issued if this needs to be applied to a fleet of vehicles. See *Online MDR Geo-Fence Figure 94*.

REMOTE FORMAT can be used to remotely format the HDD of an MDR. See *Online MDR Remote Format Figure 95*.

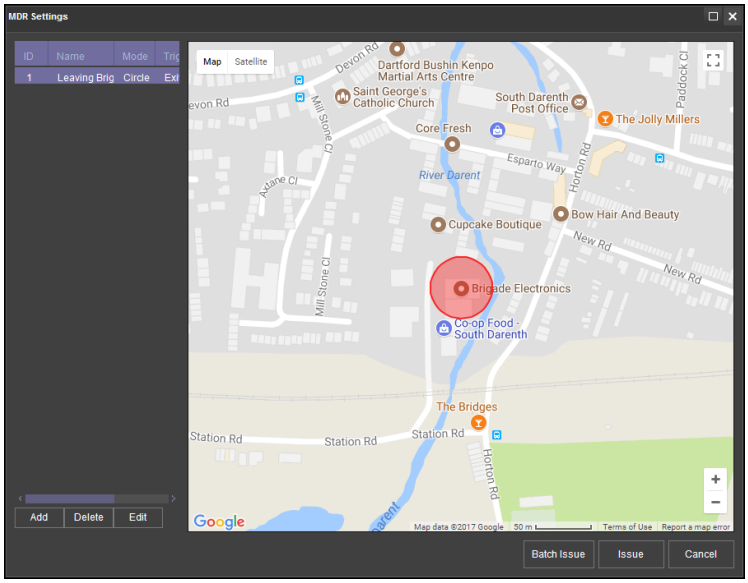
RESTART can be used to remotely restart an MDR. See *Online MDR Restart Figure 96*.



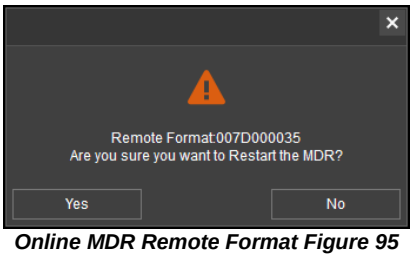
Online MDR Get Version Figure 92



Online MDR IO Settings Figure 93



Online MDR Geo-Fence Figure 94



Online MDR Remote Format Figure 95

Online MDR Restart Figure 96

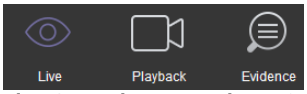
6.2 Type of operation (Area 2)

You can choose between **LIVE**, **PLAYBACK** and **EVIDENCE**. Each option has features which are discussed further in sub-sections 6.2.1, 6.2.2 and 6.2.6.

Note: Local data and server data can be accessed when the MDR-Dashboard 5.0 is in server mode. When the MDR-Dashboard 5.0 is in local mode there is limited functionality. See MDR 500 Series Installation&Operation Guide for details on local mode.

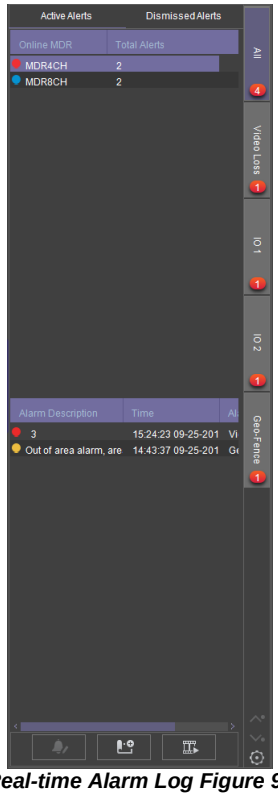
6.2.1 Live View

You access live operation by clicking on the **LIVE** icon. See *Live Operation Type Figure 97*.



Live Operation Type Figure 97

A key feature of live operation is the real-time alarm log that shows currently occurring alarms on an online MDR. See *Real-time Alarm Log Figure 98*.



Real-time Alarm Log Figure 98

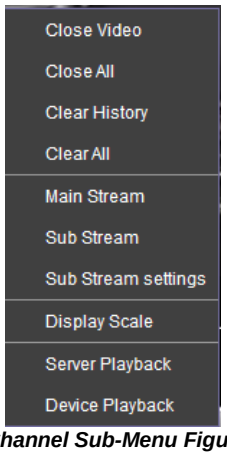
Choose a suitable view - **MAP**, **VIDEO** or **VIDEO/MAP**. See *View Type Figure 99*. The various views are discussed further in *View Settings (Area 5)*.

View Type Figure 99

The *Live Control Bar Figure 100* is displayed when the **VIDEO** view is used. You can mute  , snapshot  , expand current video view to full screen  , scroll between channels  , or change channel view  .

Live Control Bar Figure 100

When you right click a video channel, the sub menu shown in *Live Channel Sub-Menu Figure 101* will be displayed.



Live Channel Sub-Menu Figure 101

OPEN VIDEO is used to display all channel information and live video. See *Live Channel Sub-Menu Figure 101*.

CLOSE VIDEO is used to stop this channel's video displaying but shows the vehicle registration number and channel name. See *Live Channel Sub-Menu Figure 101*. It can be re-opened.

CLOSE ALL is used to stop all video channels displaying but shows the vehicle registration number and channel name.

CLEAR HISTORY is used to remove all data from the channel; this channel can no longer be opened. See *Live Channel Sub-Menu Figure 101*.

CLEAR ALL is used to remove all data from all channels.

MAIN STREAM is used to access a higher quality stream from the MDR. This is based on your HDD recording settings.

SUB-STREAM used to access a lower quality stream from the MDR.

SUB-STREAM SETTINGS control the quality of sub-streams. This is based on your HDD and SD card recording settings.

DISPLAY SCALE controls the aspect ratio of the video channel. The options are original size, 4:3, 16:9 and auto fit. By default, this is 16:9.

SERVER PLAYBACK will automatically playback MDR Server data for the MDR from the start of the current day. If there is no content, a prompt will state "No Video Found".

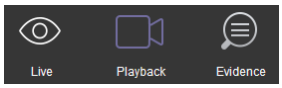
DEVICE PLAYBACK will automatically playback the MDR's HDD content from the start of the current day.

Note:

- A maximum of 64 channels can be viewed at one time.
- To access a cleared channel, double-click the vehicle to refresh all channels.
- Live view may have video stuttering due to a limitation in the available bandwidth.

6.2.2 Playback

You access playback operation by clicking on the **PLAYBACK** icon. See *Playback Operation Figure 102*.



Playback Operation Figure 102

Playback Options Figure 103 will then be presented to you. There are 4 playback options:

- MDR Server
- HDD/SD
- Online MDR
- Local Files

Playback Options Figure 103

Playback Bar Figure 104

In each **PLAYBACK** mode you can download recordings. During playback, click on the clipping icon  , shown in *Playback Bar Figure 104*.

Clipping Toolbar Figure 105

You are then presented with the tool bar shown in *Clipping Toolbar Figure 105*.

The clipping toolbar is used to either Play, Screenshot, Map Screenshot, Evidence Snapshot, Screenshot all channels or screenshot select.

The **PLAY** function is used to play the video during clipping mode.

Once the **SCREENSHOT** button is clicked, a screenshot of the video image is stored locally under C:\You*username*\AppData\Roaming\MDR-Dashboard5.0\config\Photo*screenshot filename*. It is labelled with the vehicle ID, video date and video time. A popup message will show up next to your PC time for 6 seconds. An example is shown in Screenshot pop-up Figure 106.

MAP SCREENSHOT is used to take screenshot of only the current map position being displayed. Once this is clicked, the data will appear in the **SNAPSHOT LIST** as shown in *Snapshot list Figure 107*. Items can easily be deleted from the snapshot list by using the delete (trash can) icon. See *Snapshot list Delete Icon Figure 108*. The delete icon turns green when the mouse hovers over it. See *Snapshot list Active Delete Icon Figure 109*.

EVIDENCE SNAPSHOT is used to take a screenshot of the current video position. Once this is clicked, the data will appear in the Snapshot list as shown in *Snapshot list Figure 107*.

SCREENSHOT ALL CHANNELS is used to screenshot all channels which then appears in the Snapshot list as shown in *Snapshot list Figure 107*.

SCREENSHOT SELECT is used to give you the option to choose from several automatically generated video screenshots based on the current time marker (15:17:08 shown in *Screenshot Select Figure 110*.

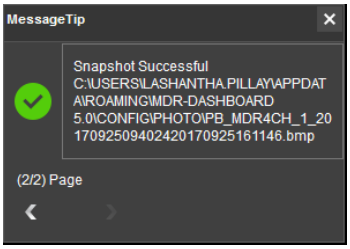
Once a screenshot is chosen, it will appear in the Snapshot list as shown in *Snapshot list Figure 107*.

Once satisfied with the snapshot list, you will then position the clipping markers to the start and end time of the desired clip. Click **OK**. See *Clipping Markers Figure 111*.

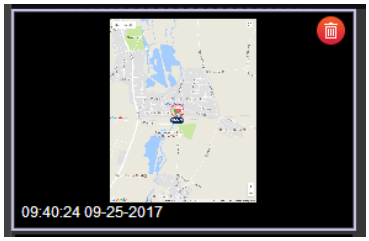
The clip settings window will now be shown. See *Clip Settings Figure 112*. You can manually set the **START TIME** and **END TIME**. Choose from your available channels. There are 3 different ways to clip:

- **STANDARD** - You must set the desired **PATH** before clicking **OK**. These H.264 files are opened manually by MDR-Dashboard 5.0 / MDR-Player 5.0 and are stored locally. Standard downloads can also be uploaded as evidence.
- **EXPORT** – This file must not be larger than 1.5GB. If it is larger, it will not function. You must set the desired **PATH** and **FOLDER** name before clicking **OK**. This option creates an executable (.exe) file including the MDR-Player 5.0 with the embedded video. These files may be password protected. Evidence option is not available. These files are stored locally.
- **AVI** - You must set the desired **PATH** before clicking **OK**. These files can be played by standard media players. Evidence option is not available. These files are stored locally.

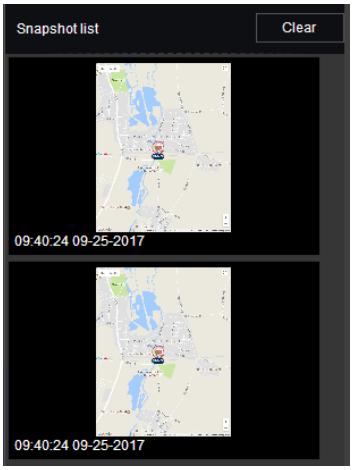
Note: If the **EVIDENCE** feature is used, the downloaded video will be uploaded to the server. The data is found in the Evidence tab. See section 6.2.6 Evidence for more information.



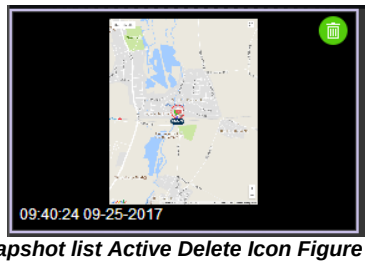
Screenshot pop-up Figure 106



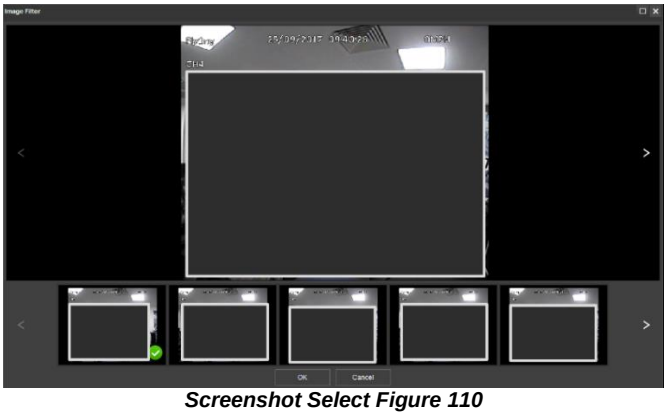
Snapshot list Delete Icon Figure 108



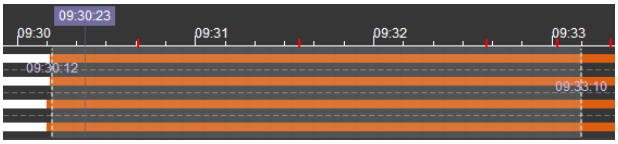
Snapshot list Figure 107



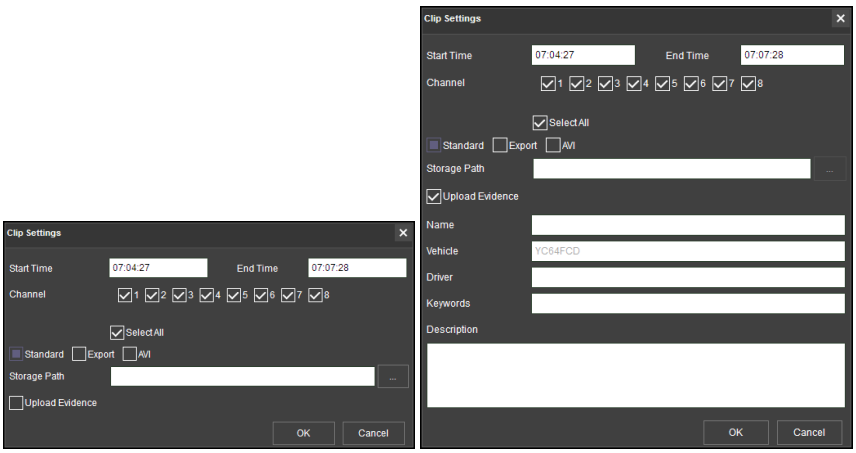
Snapshot list Active Delete Icon Figure 109



Screenshot Select Figure 110



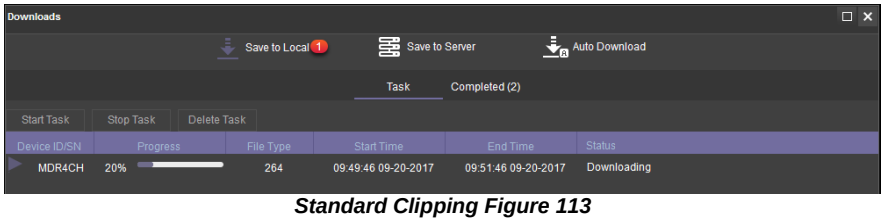
Clipping Markers Figure 111



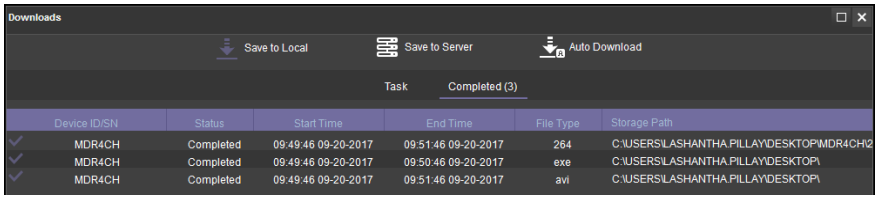
Clip Settings Figure 112

You can check the progress of clippings under **DOWNLOAD** → **TASK** (Area 3). See *Standard Clipping Figure 113*.

Once the task is completed, you can view the status and storage path under **DOWNLOAD → COMPLETED**. See *Completed Clippings Figure 114*.



Standard Clipping Figure 113



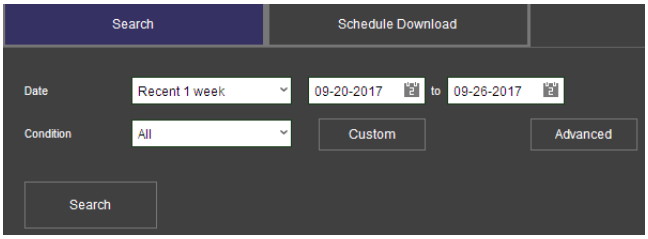
Completed Clippings Figure 114

6.2.3 MDR Server

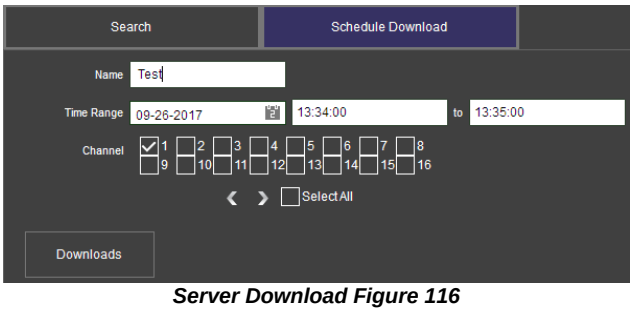
You can search the server for MDR downloads. These searches can be based on dates, speed and events. See *Server Search Figure 115*.

You can schedule downloads from the MDR to the server based on time, dates and video channels. See *Server Download Figure 116*.

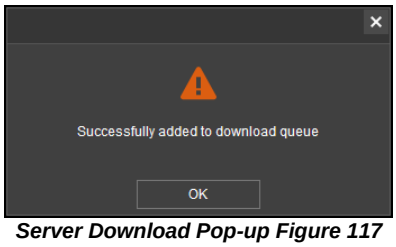
Once a user creates a scheduled download, a window pops up to indicate this has been added successfully. See *Server Download Pop-up Figure 117*.



Server Search Figure 115



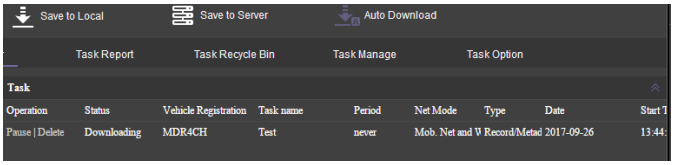
Server Download Figure 116



Server Download Pop-up Figure 117

Server Download Notification Figure 118

This scheduled download appears under auto downloads. You click on **DOWNLOAD** as shown in *Server Download Notification Figure 118*.



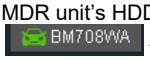
Server Download Queue Figure 119

Table 13 of Scheduled Downloads vs Auto Downloads

SCHEDULED DOWNLOAD	AUTO DOWNLOAD
Download is a once off process	Can be set as a recurring download
Setup based on time and channel	Setup based on time, channel, alarms and events
Will download over any available network	Can be configured to either wi-fi, mobile network or both
Not Applicable	Configurable to downloads metadata and/or video

6.2.4 Online MDR

This is used to remotely access an MDR unit's HDD content.

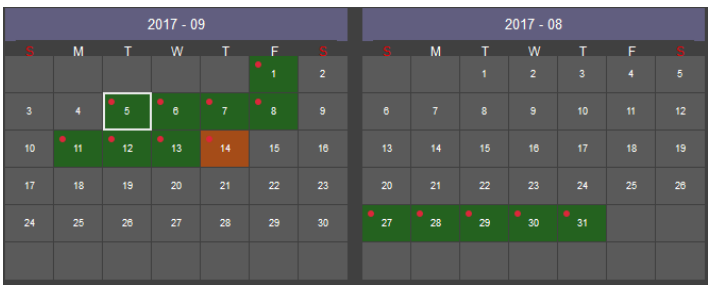
Double-click the online vehicle icon 

to open the calendar view as shown in *Online MDR Calendar View Figure* 120.

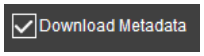
Ensure that the **DOWNLOAD METADATA** option is ticked as shown in *Metadata Figure 121*. This is found bottom left of the calendar view.

- Green dates represent normal recordings (01/09/2017 - 13/09/2017)
- Orange dates represent alarm recordings (14/09/2017)
- Red dot only (no colour) represents only metadata
- White outline represents the date you are viewing (05/09/2017)

Double-click the desired date and choose which camera channels to view. See *Channel Selection Figure 122*.



Online MDR Calendar View Figure 120



Metadata Figure 121

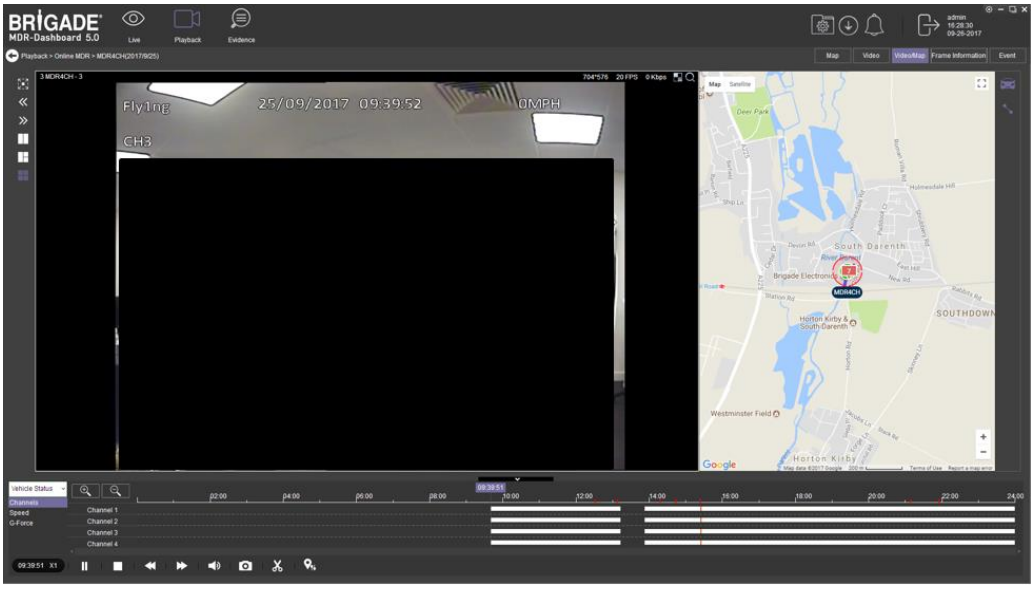
Then click the **PLAY** button located above the channel selection. See *Channel Selection Figure 122*.

Once you click play, the video will be displayed as shown in *Playing a Video Figure 123*.

You may view graphical data related to the recording such as:

- Vehicle Status – Channels, Speed and G-Force.
- Device Status – Device temperature, Environment temperature and MDR voltage.

Channel Selection Figure 122



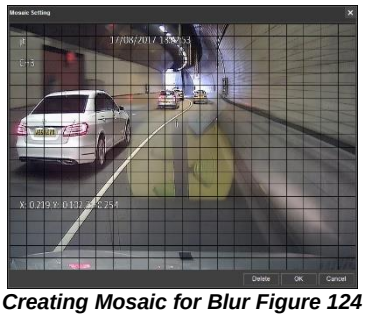
Playing a Video Figure 123

Each camera channel has two additional features, **BLUR** and **ZOOM**.

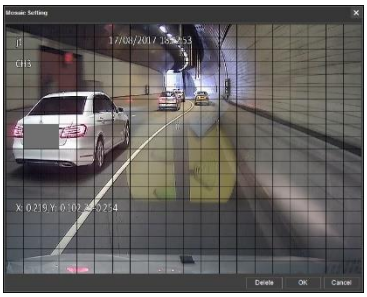
Note: **ZOOM** is available in **LIVE** mode. **BLUR** cannot be used in **LIVE** mode.

You can use blur to create a mosaic setting of an area which will be blurred throughout video playback. See *Creating Mosaic for Blur Figure 124*, *Setting the Blur Area Figure 125* and *Blur Activated Figure 126*.

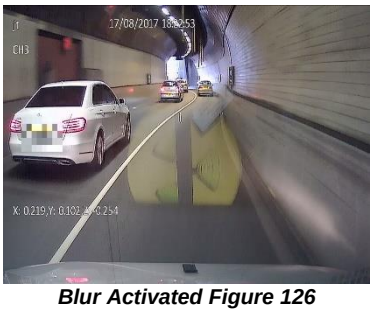
ZOOM is used to create a magnified view of a selected area of a camera channel. Click the magnifying glass and then choose the desired box area. This is now the only area that will be visible during playback. To exit this view, double-click the camera channel. See *Choosing Zoom Area Figure 127* and *Zoom area Figure 128*.



Creating Mosaic for Blur Figure 124



Setting the Blur Area Figure 125

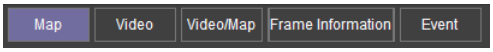


Blur Activated Figure 126

Choosing Zoom Area Figure 127

Zoom area Figure 128

is used to **ZOOM** in or out of the time scale. Maximum **ZOOM** in is 5 seconds and maximum **ZOOM** out is 24 hours.



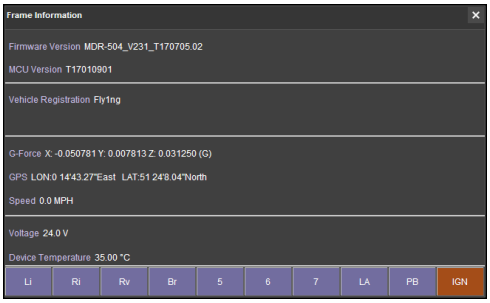
Extended View Settings Figure 129

To view further information regarding the recording you can access **FRAME INFORMATION** and **EVENT** as shown in *Extended View Settings Figure 129*.

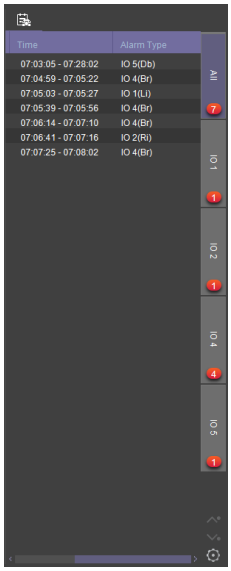
See *Frame Information Figure 130*. **FRAME INFORMATION** consists of:

- Firmware version
- MCU version
- Vehicle Registration
- G-Force
- GPS
- Speed
- Voltage
- Device Temperature
- Trigger Activity Indicator

See *Event Information Figure 131*. Event information consists of device alarms which have event names and times.



Frame Information Figure 130



Event Information Figure 131

6.2.5 HDD/SD and Local Files Playback

6.2.5.1 Local Files Playback

This procedure applies to recordings previously downloaded from the MDR and saved onto a USB flash drive or recordings saved onto a PC.

To read downloaded files click on the **LOCAL FILES** tab found on the Data Source Access (area 1). See *Data Source Figure 132*.

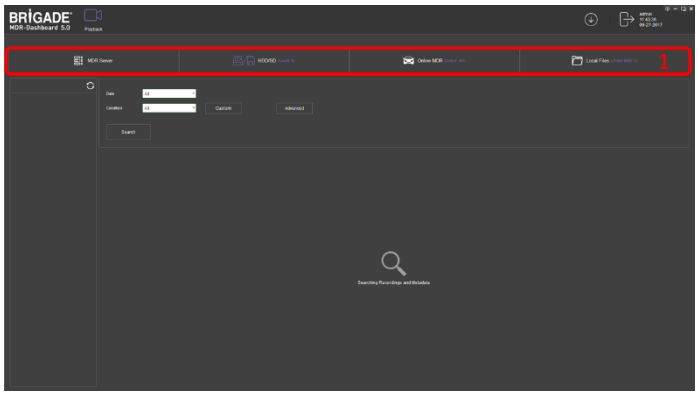
You click on the **LOCAL FILES** tab as shown in *Local Files Tab Figure* 133.

Click the **ADD** button as shown in *Local Files Add Figure* 134. Browse to the relevant folder and click **SELECT FOLDER**.

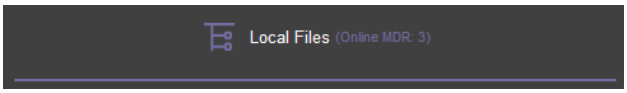
This brings up a Windows™ Explorer dialogue box (*Windows Explorer Folder Figure 135*) which allows you to select the folder that contains the recordings. Select the MDR Vehicle name, in this example 3-3.

Once the folder has been successfully loaded, it will appear as shown in *Device Directory Figure 136*.

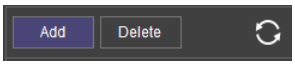
If there was a local file specified previously, click the refresh icon  to get the local file to appear. This will be a green icon to indicate it is available for browsing.



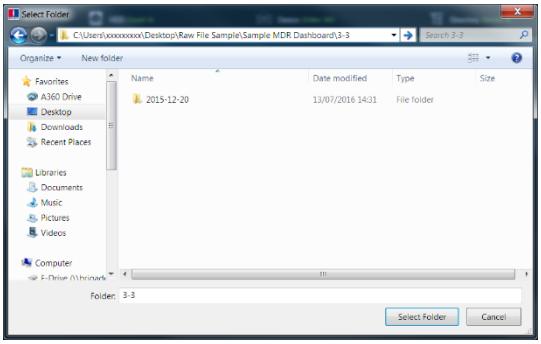
Data Source Figure 132



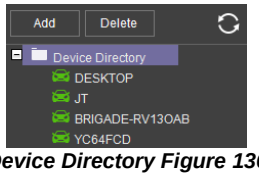
Local Files Tab Figure 133



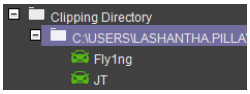
Local Files Add Figure 134



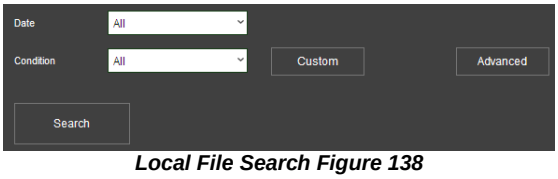
Windows Explorer Folder Figure 135



Device Directory Figure 136



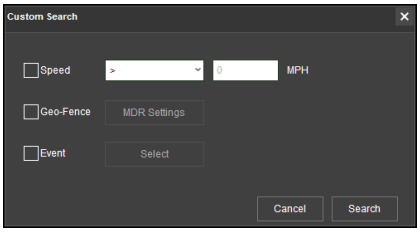
Clipping Directory Figure 137



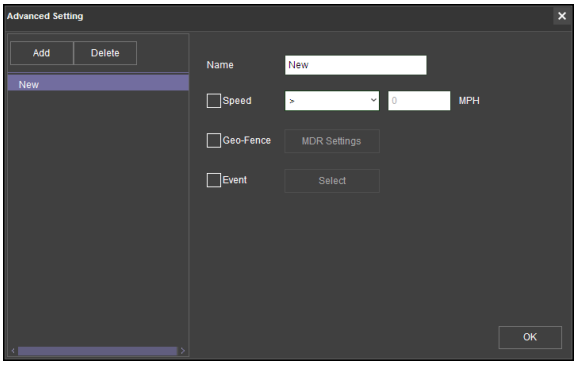
Local File Search Figure 138

The local file will now appear in the left pane as shown in *Device Directory Figure 136*. **DEVICE DIRECTORIES** show when a specific vehicle folder is chosen, these are added individually. If you would like to add multiple vehicles simultaneously, choose a folder top level folder that contains multiple vehicles. Using this method will result in a **CLIPPING DIRECTORY** to be added to the local file list.

Multiple local files can be specified. Directories may be searched. See *Local File Search Figure* 138. Custom and Advanced searches can be configured. See *Custom Search Figure 139, Windows Explorer Folder Figure 135* and *Advanced Search Settings Figure 140*.



Custom Search Figure 139



Advanced Search Settings Figure 140

6.2.5.2 HDD/SD Playback

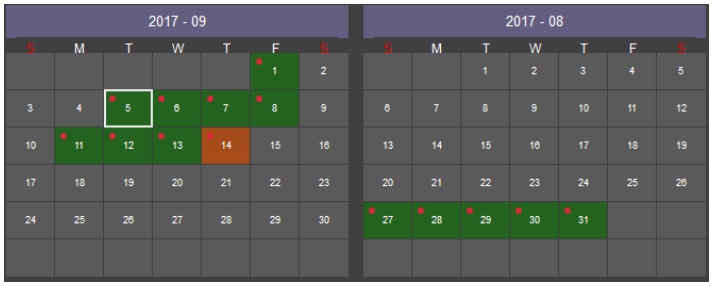
Double-click the vehicle icon 

. This will display **ALL** calendar events. A typical example of a calendar is shown in *HDD Calendar Figure 141.*

Each colour represents:

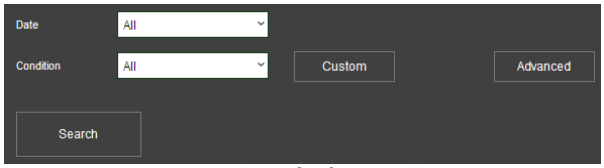
- Green dates represent normal recordings (01/09/2017 - 13/09/2017)
- Orange dates represent alarm recordings (14/09/2017)
- Red dot only (no colour) represents only metadata
- White outline represents the date you are viewing (05/09/2017)

A typical example of a calendar is shown in *HDD Calendar Figure 141*.



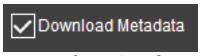
HDD Calendar Figure 141

To refine the data displayed, you should setup search criteria. Custom and Advanced searches can be created. *HDD Search Figure 142*.



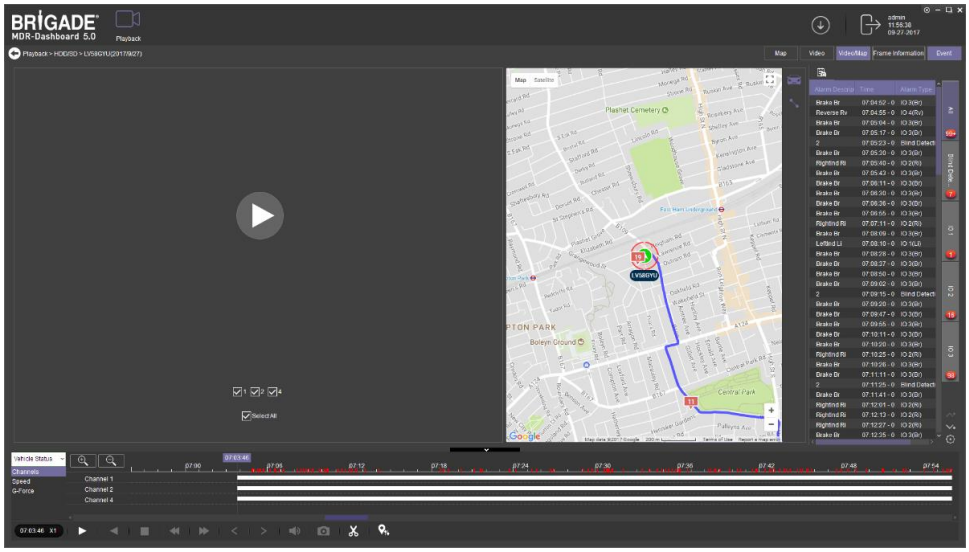
HDD Search Figure 142

Ensure that the **DOWNLOAD METADATA** is always ticked. See *Metadata Setting Figure 143*. This will ensure that all metadata is shown with playback video.



Metadata Setting Figure 143

You double-click on the relevant calendar date. This will then display the pre-playback screen. See *Pre-playback Figure 144*. You can choose which channels to view during playback.



Pre-playback Figure 144

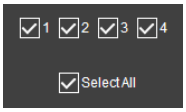
You can access different view settings such as, **MAP**, **VIDEO** and **VIDEO/MAP**. See *View Options Figure 145*.

View Options Figure 145

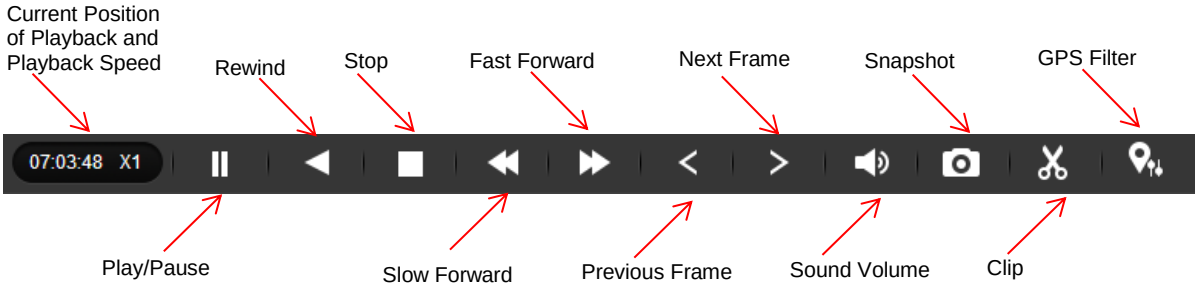
Frame information and Event information can also be accessed from this panel. To return to the calendar view from the current playback, click the back arrow. See *Return to Calendar Figure 146*.

Return to Calendar Figure 146

Choose which channels to playback.



Click the Play button to display the data.



MDR-Dashboard 5.0 Controls Panel Figure 147

Fast Forward options (1x, 2x, 4x, 8x, 16x, 32x). Maximum **Slow Forward** option is x1/32.

Double-clicking an individual channel to make it full screen. There are other video viewing options as shown in

Video View Options Figure 148, such as:

- Full Screen
- Previous Page
- Next Page
- Three Windows
- Four Windows
- Six Windows
- Nine Windows

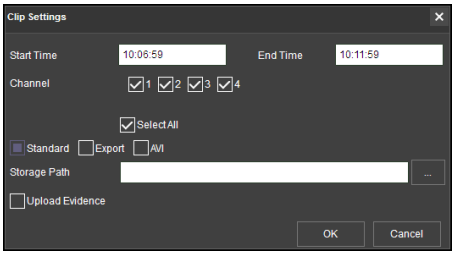
Video View Options Figure 148

6.2.5.2.1 Downloading Videos

Click on the **CLIP** button .
Clip markers appear (broken vertical lines). See *Clipping a Video Figure 149.*
Drag the markers to set the **START** and **END TIME** for the clip.
Alternatively, click **OK** and **TYPE** the start and end times in the *Standard Clip Settings Figure 150.*
Choose the number of channels you wish to download.
Choose the type of download, there are three types of downloads:

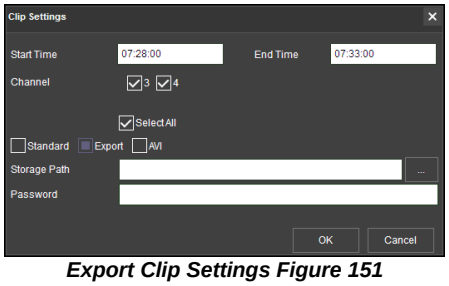
- **STANDARD** creates a folder structure containing the video files in original proprietary format (H264) onto a local storage device (e.g. USB Flash drive). Note: You are not allowed to use the same location as the original folder. Once clipped, the files will be found in a folder named with the following format: \Company_Name-Vehicle_Number\YYYY-MM-DD\record.

Clipping a Video Figure 149



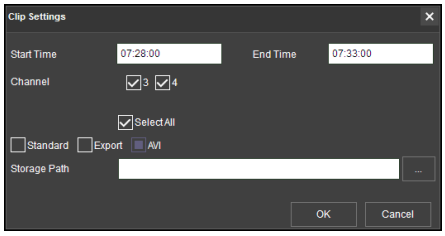
Standard Clip Settings Figure 150

- **EXPORT** allows you to export clips into a single .exe file with an embedded MDR-Player 5.0. This option is the recommended solution as it contains metadata and video. It also can be password protected and played without the need of any additional player software. This does not require any installation. Note, this file should not be larger than 1.5GB.



Export Clip Settings Figure 151

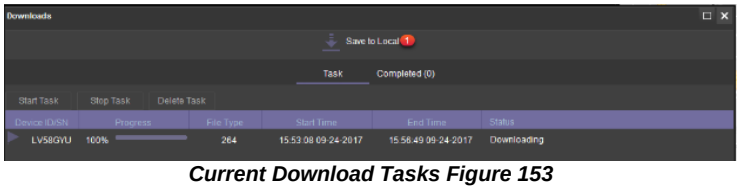
- **AVI** creates .AVI files playable by common players such as Windows Media Player (WMP™) and Video Lan Client (VLC). The advantages of this solution are the portability of the format. The disadvantage is the lack of protection and missing metadata. These files can be played and edited by anyone. The only information contained in the video image is selected by the OSD Overlay options in the firmware. Note, these files are split per channel.



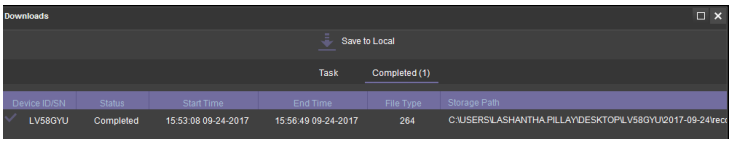
AVI Clip Settings Figure 152

Choose the Storage Path using  . Brigade recommends choosing your desktop.

Once satisfied click on the **OK** button  .

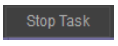
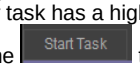
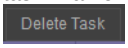


Current Download Tasks Figure 153



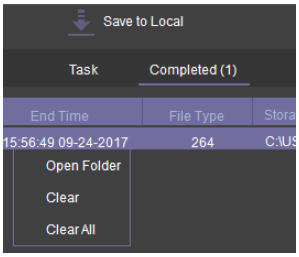
Completed Download Tasks Figure 154

You may monitor the progress of current/completed download tasks under the downloads area. Click the download  button.

See *Current Download Tasks Figure 153*. Task priority is a first come first serve basis. If another task has a higher priority, use  to stop a task and the  to start the priority task. If an error is made, tasks may be deleted using the  button.

Completed tasks automatically move to the Completed tab, see *Completed Download Tasks Figure 154*.

Right-click a completed task to access a sub-menu as shown in *Completed Sub-Menu Figure 155*.



Completed Sub-Menu Figure 155

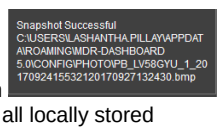
6.2.5.2.2 Saving Snapshots

Click the desired channel; this will be highlighted by a **WHITE OUTLINE**. See *Choosing a Channel Figure 157*.

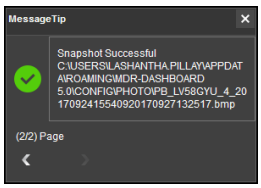
Click on the **SNAPSHOT** button  in the Controls Panel.

A pop-up window will be displayed on the bottom right corner of the desktop (next to the time/calendar) The snapshot location is also shown here (See *Snapshot pop-up Figure 156*).

Choosing a Channel Figure 157

Click on the Snapshot Successful information 

to access the **IMAGE FILTER**, this shows all locally stored snapshots. See *Snapshot Image Filter Figure 158*.



Snapshot pop-up Figure 156

Snapshot Image Filter Figure 158

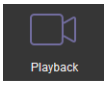
6.2.6 Evidence

Evidence refers to clippings, video screenshots and map screenshots that are uploaded to the server.

Note: Evidence upload is only available when MDR-Dashboard 5.0 is logged into **SERVER** mode.

6.2.6.1 Evidence Upload

To create evidence packages please follow the steps described below. These files are accessible via MDR-Dashboard 5.0. It will display the video and snapshot files that were added during the clipping process.

Click **PLAYBACK** 

to enter playback mode.

Choose the desired data source – **MDR SERVER**, **HDD/SD**, **ONLINE MDR** or **LOCAL FILES**.

During playback of a video, click the clipping icon  and set the clipping markers to the desired times.

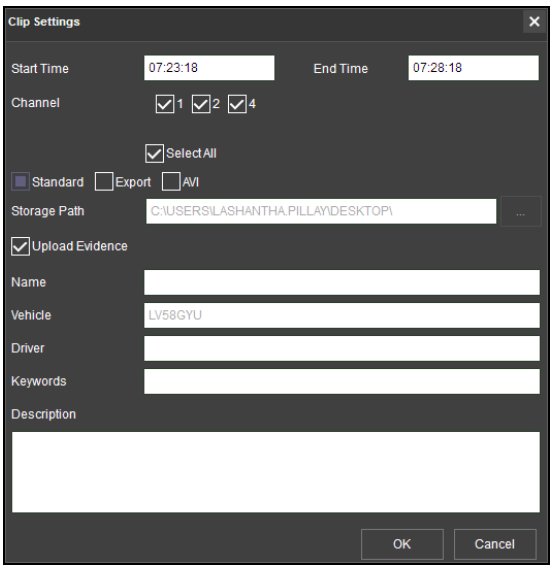
Create the desired snapshot list using the evidence buttons 

which will be associated with this video clipping.

Once satisfied with the clipping duration and snapshot list, click **OK**.

The Clip Settings window will now be displayed. See *Clipping Markers Figure 111*.

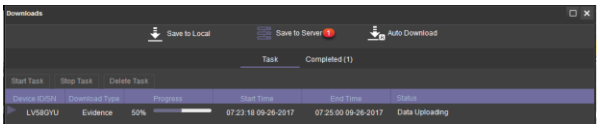
Ensure **STANDARD** is ticked then tick **UPLOAD EVIDENCE**. This means that the path specified under **PATH** is now void. See *Evidence Upload Figure 159*.



Evidence Upload Figure 159

Fill in all details shown in *Evidence Upload Figure 159*. The following details can be completed: Name, Vehicle (automatically populated), Driver, Keywords, and Description. Click **OK** once all details are filled in. **Name** and **Driver** are required fields.

To confirm that this evidence upload task has been created, click **DOWNLOAD → SAVE TO SERVER**. See *Evidence Upload Download Window Figure 160*.



Evidence Upload Download Window Figure 160

This task will appear under **COMPLETED** once it has finished. See *Evidence Upload Download Window Figure 160*.

6.2.6.2 Evidence Playback

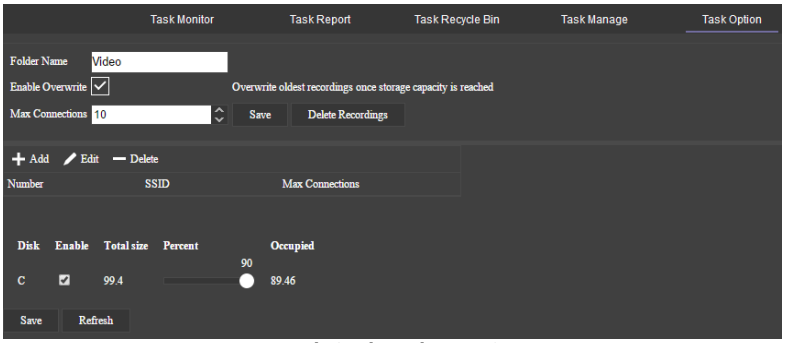
Due to the nature of evidence (contains sensitive information), it can **NEVER** be clipped or copied locally. Evidence is stored on the server and can only be accessed via MDR-Dashboard 5.0.

You access playback by clicking on the **EVIDENCE** icon. See *Evidence Icon Figure 162*.

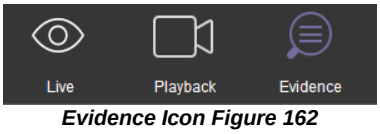
Server directory for evidence video file storage: C:\Program Files (x86)\MDR Server\WCMS4.0\EvidenceData.

Navigate to the desired vehicle/company name (fleet) as shown in *Evidence Vehicle Figure 163.*

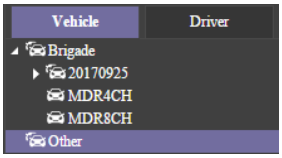
Note: The vehicle does not need to be online to access evidence. Evidence data is stored on the server**.**



Task Option Figure 161

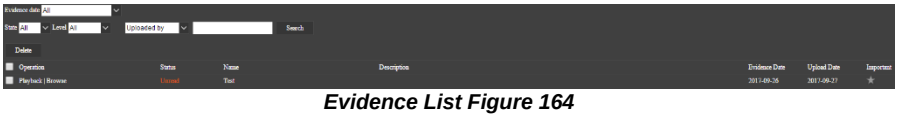


Evidence Icon Figure 162



Evidence Vehicle Figure 163

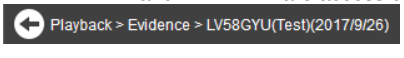
A full list of evidence is now displayed as shown in *Evidence List Figure 164*. This list can be filtered by state (read or unread), importance level (mark evidence as important using ), keywords, name and description.



Evidence List Figure 164

Click on **PLAYBACK** button 

which will begin the evidence playback. Please give the snapshot list approximately 10 seconds to load its data. **FRAME INFORMATION** and **EVENTS** are accessible within evidence. See *Evidence Playback Figure 165*.

Click on the back arrow 

to return to the evidence list.

Evidence Playback Figure 165

6.2.6.3 Browsing Evidence

Click on the **BROWSE** button  which will open an evidence report. See *Evidence Report Top Figure 166*.

There are several details that are displayed in this report, such as: Name, Driver, Vehicle Registration, uploading user, evidence date, creation date, keyword, description, maps and pictures.

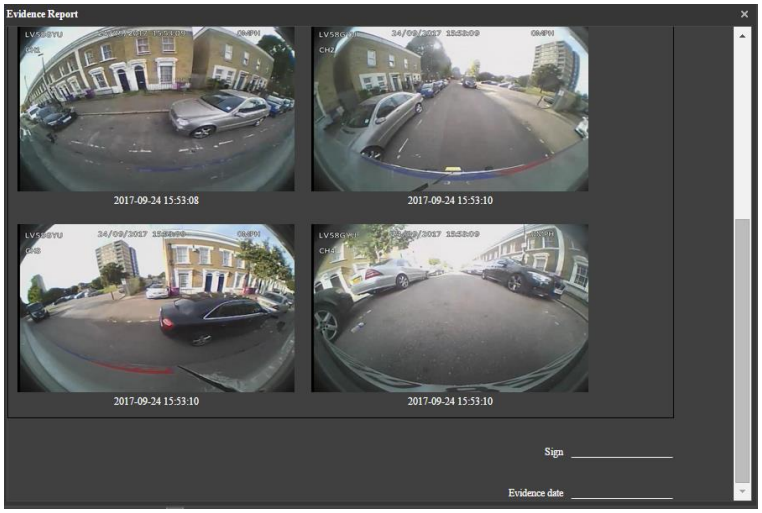
This report is easily printed using the  button found at the top of the report. There is also an area for a handwritten signature and evidence date. See *Evidence Report Bottom Figure 167*.

Uploaded evidence can be modified afterwards. This is to correct any erroneous data such as vehicle registration number, Name, Driver, Keyword, and Description.

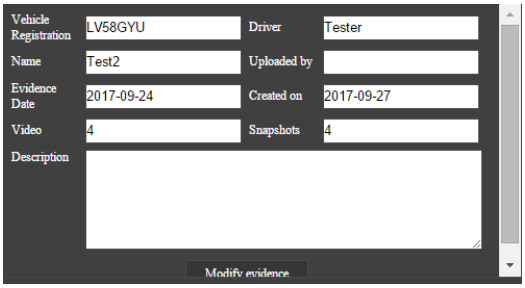
You must highlight the evidence to be modified and then change the configurable data shown in *Evidence Modification Figure 168*.

MDR-Dashboard also tracks who accessed which evidence and when. This information is found under **QUERY USERS** which is shown in *Query Evidence Figure 169*.

Evidence Report Top Figure 166



Evidence Report Bottom Figure 167



Evidence Modification Figure 168

Query Evidence Figure 169

6.3 Downloads and Alarm (Area 3)

DOWNLOAD allows you to setup local/server downloads and auto download schedules. **ALARM** lets you access the **ALARM CENTER** which allows for searching alarms, setting alarm strategies and alarm e-mails. **SYSTEM MANAGEMENT** allows you to set **FLEET INFORMATION**.

6.3.1 Downloads

Warning: Downloads do not occur if the free space on the server disk is less than 500MB.

Click on the download icon which will display the window shown in *Download Window Figure 170*.

There are 3 download options: **SAVE TO LOCAL**, **SAVE TO SERVER** and **AUTO DOWNLOAD**.

AUTO DOWNLOAD connections to the server are limited to the number of MDRs that can be downloaded at a given time. If there are many online MDRs then downloads enter a "wait" state.

AUTO DOWNLOAD is more suited to a Mobile Network connection as the MDR can transfer data regardless of location. If **AUTO DOWNLOAD** is setup with a Wi-Fi connection, the MDR will only run the auto download schedule once it is powered on and connected to the Wi-Fi network.

Tasks appear under **TASK MANAGE**. Any manually setup downloads, known as Appointments also appear here. See section 6.2.2 Playback. The number of manual downloads is unlimited.

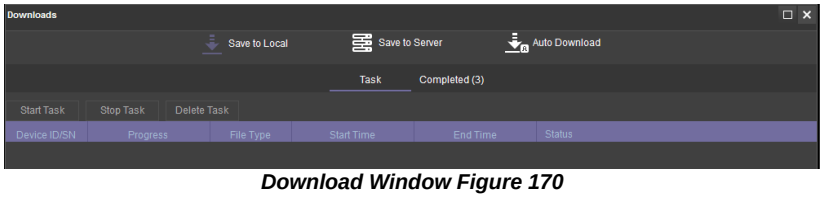
Download priority is based on a first come first serve basis.

Tasks appear under **SAVE TO SERVER** when the clippings are being uploaded as **EVIDENCE**.

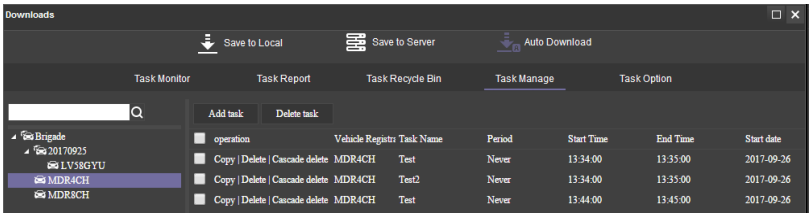
Auto Downloads are setup differently to Clippings and Appointments.

Select the vehicle and then click **TASK MANAGE**. See *Auto Download Figure 171*.

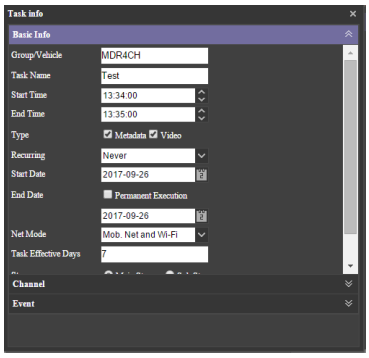
- Click **ADD TASK**. You will now be presented with a **TASK INFO** window which is shown in *Auto Download Basic Information Figure 172*.
- You must now setup all details found under **BASIC INFO**, **CHANNEL** and **EVENT**. See the below figures, *Auto Download Basic Information Figure 172*, *Auto Download Channel Figure 173* and *Auto Download Event Figure 174*.
- **GROUP/VEHICLE** - this represents the vehicle name as shown in the group list in the left pane
- **TASK NAME** – this is the User's choice – name appropriately for easy understanding
- **START TIME** – this represents start time of the clipping.
- **END TIME** - this represents end time of the clipping.
- **TYPE** – choice of either metadata / Video or both.
- **RECURRING** – Options to repeat this task such as Never, Every day, Weekly or Monthly
- **START DATE** – this allows you to set the date for when the clipping must be taken from, this can also be set in the future. Must ensure that this setup when the MDR will be powered and online.
- **END DATE** – this refers to the final date clippings will be completed
- **PERMANENT EXECUTION** – If this clipping must be completed indefinitely, tick this box.
- **NET MODE** – The options are Mob. Net, Wi-Fi and Mob. Net/Wi-Fi.
- If an MDR has post alarm set to 7 seconds and auto download and the dashboard post alarm set to 10 seconds. The auto download recording will have post alarm of 7 seconds as there is no further alarm recording to be downloaded.
- **TASK EFFECTIVE DAYS** – defines for how many days a recurring task should occur.
- **STREAM** – The options are Main Stream or Sub Stream. Main Stream is higher quality.



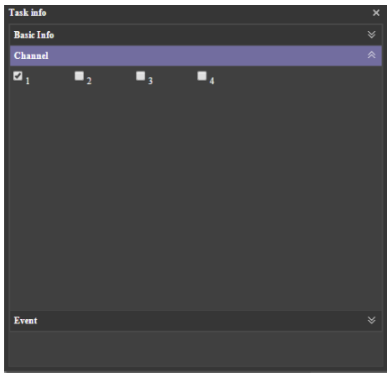
Download Window Figure 170



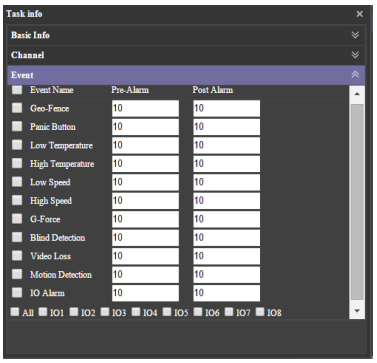
Auto Download Figure 171



Auto Download Basic Information Figure 172



Auto Download Channel Figure 173



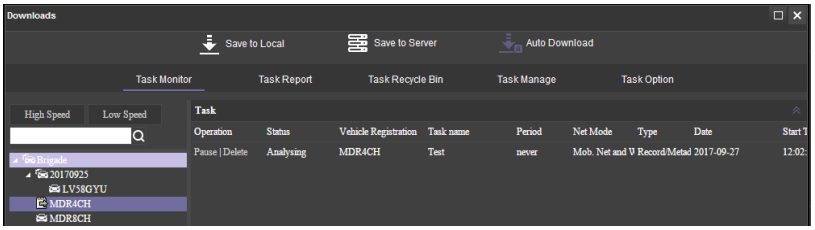
Auto Download Event Figure 174

- **VIDEO TYPE** – The options are All, Normal Video and Alarm Video.

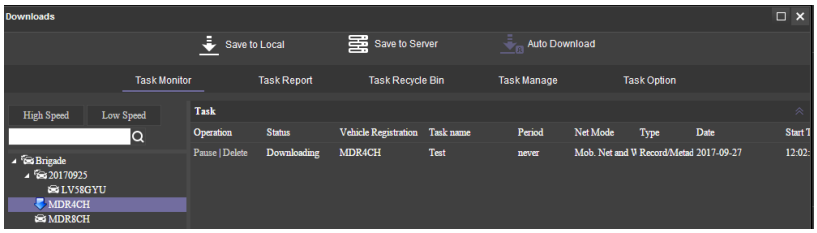
You can view the status of the **AUTO DOWNLOAD** tasks by clicking **TASK MONITOR**. See *Task Monitor Analysing Figure* 175.

A download list is created, then the status becomes waiting, analysing, analysing finished and begins the downloading.

See *Task Monitor Analysing Figure* 175, **HIGH SPEED** will download files at quicker speeds. **LOW SPEED**, MDR will download files at slower speed.



Task Monitor Analysing Figure 175



Task Monitor Downloading Figure 176

TASK REPORT is used to search all tasks based on dates and task status. See *Task Report Figure 177*.

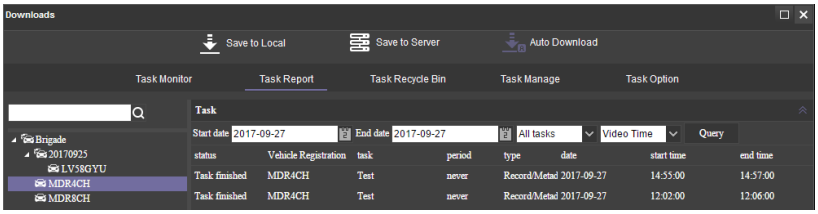
QUERY is used to update the list. See *Task Report Figure 177*.

TASK RECYCLE BIN shows tasks that have been deleted by the user. See *Task Recycle Bin Figure 178.*

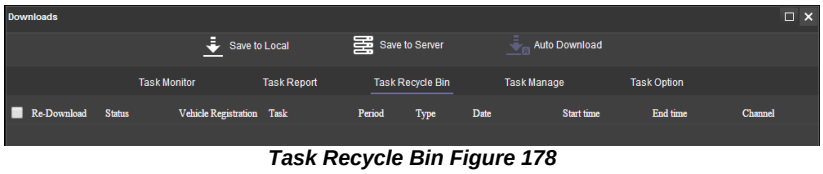
TASK OPTION is used to set the folder for the **AUTO DOWNLOAD** files. See *Task Option Figure 179*.

AUTO DOWNLOAD files are located on the Windows Server.

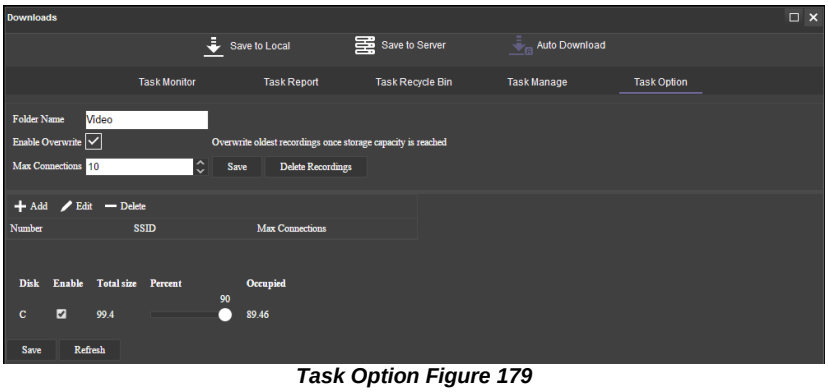
These files are accessed via **PLAYBACK → MDR SERVER**.
Server directory for video file storage: C:\Video*Vehicle Name*.



Task Report Figure 177



Task Recycle Bin Figure 178



Task Option Figure 179

Table 14: Auto Downloads Task Status Information

STATUS	DESCRIPTION
Suspended	The task is in suspension.
Limited number of connections	Vehicle downloads has exceeded the limit of allowed connections
Parsing	Analysing in preparation to download file
Task has not been finished	Download not complete, since the time required is greater than the current MDR system
Insufficient space on the disk	There is not enough space on the server disk
Loading	Task is waiting to be downloaded
Parsing successfully	Completed analysing the file to be downloaded
Downloading	File is currently being downloaded
No record file	No file exists based on analysis. (No qualified record file)
Download successfully	Download successfully and the file has been downloaded.
Task failed	Analysis task could not be completed. (e.g. Fail to access data, abnormal data)
Task deleted	Task has been deleted by user
Download failed	Task is successfully added but the file fails to download

6.3.2 Alarm Center

Alarm Center refers to an area which contains the following options:

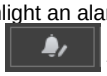
- Alarm Search
- Alarm Settings

6.3.2.1 Alarm Search

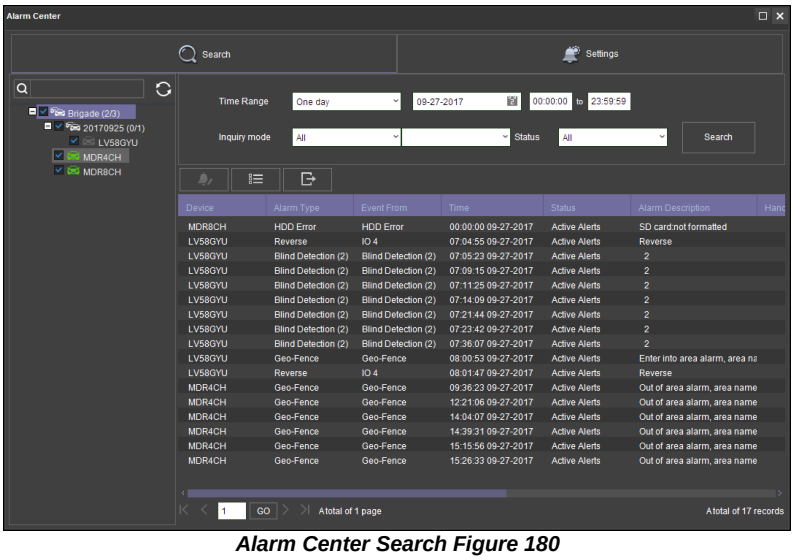
This area is used to search all alarms based on the vehicle, time range, date, event type and alarm status.

You will set search parameters and then click on the **SEARCH** button. Once clicked the MDR Server will be queried.

See a typical list shown in *Alarm Center Search Figure 180*. The total number of alarm records is shown in the bottom right corner of the window.

Alarms are processed here. Highlight an alarm entry and then click the **PROCESS** button  to enter the relevant description. See *Alarm Center Search Figure 180*. **BATCH PROCESSING** is achieved by clicking the  icon. See *Alarm Center Search Figure 180*.

The entire alarm log can be exported as an excel table (.xls) to a chosen local directory. This is done by clicking the **EXPORT ALARM** button  . See *Alarm Center Search Figure 180*.



Alarm Center Search Figure 180

6.3.2.2 Alarm Settings

Tick a fleet group or a specific vehicle you would like to apply the alarm strategy to. Once you have ticked the vehicle/group, choose what alarm type you would like to be notified about.

MDR-Dashboard Strategy has the following options:

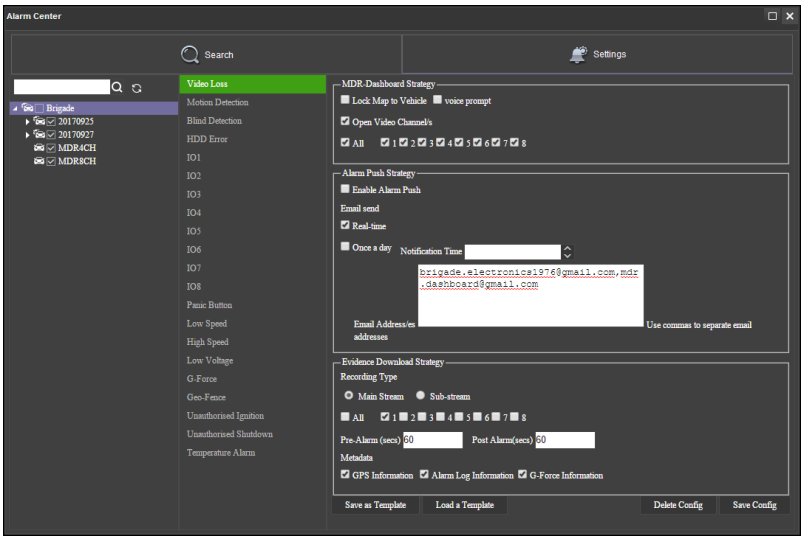
- **Lock Map to Vehicle**: When an alarm is triggered, maps will lock onto the specific vehicle on the map.
- **Voice Prompt**: An audible siren alarm will be played through your PC speakers to alert you of a triggered alarm. Note: Muted PC speakers will not be unmuted for this feature.
- **Open Video Channel/s**: If you tick a channel, MDR-Dashboard will automatically open the chosen channels in the live view.

Alarm Push Strategy has the following options:

- **Enable Alarm Push**: When an alarm is triggered, notifications will be sent to your mobile apps. Note: Requires apps to be logged in and running as a background service.
- **Real-time**: When an alarm is triggered, email notifications will be sent to your listed email addresses instantly. Note: Requires email account to be configured.
- **Once a day**: When an alarm is triggered, email notifications will be sent to your listed email addresses at the specified time. Note: Requires email account to be configured.

Evidence Download Strategy has the following options:

- **Main Stream**: Downloads high quality video.
- **Sub-stream**: Downloads low quality video.
- **Tick channels** you would like to download
- **Pre-Alarm**: refers to how many seconds before the alarm you want to download.
- **Post Alarm**: refers to how many seconds after the alarm you want to download.
- **GPS Information**: tick this to download GPS metadata with the associated video.
- **Alarm Log Information**: tick this to download alarm logs (metadata) with the associated video.
- **G-Force Information**: tick this to download G-Force metadata with the associated video.



Alarm Configuration Figure 181

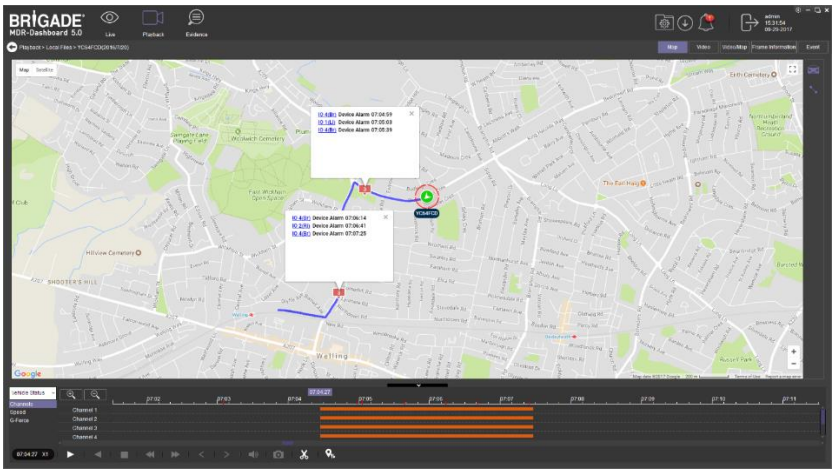
6.4 View Settings (Area 5)

This area contains the following view options:

- Map
- Video
- Video/Map

6.4.1 Map

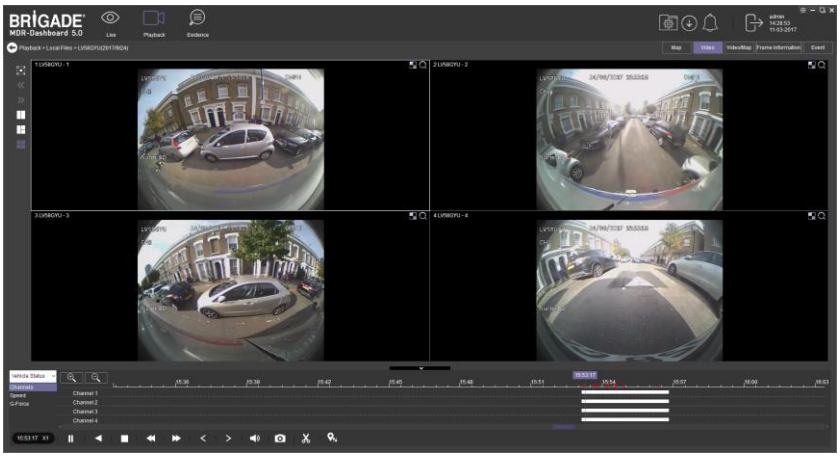
This view is accessed by clicking the **MAP** button. See *Map View Figure 182*. It will display the MDR GPS tracking data. This can be used in both **LIVE** and **PLAYBACK** mode. A hazard symbol on the map will show points where an alarm was triggered. If there are multiple alarms in close succession, a box indicating the number of alarms will be shown on the map .



Map View Figure 182

6.4.2 Video

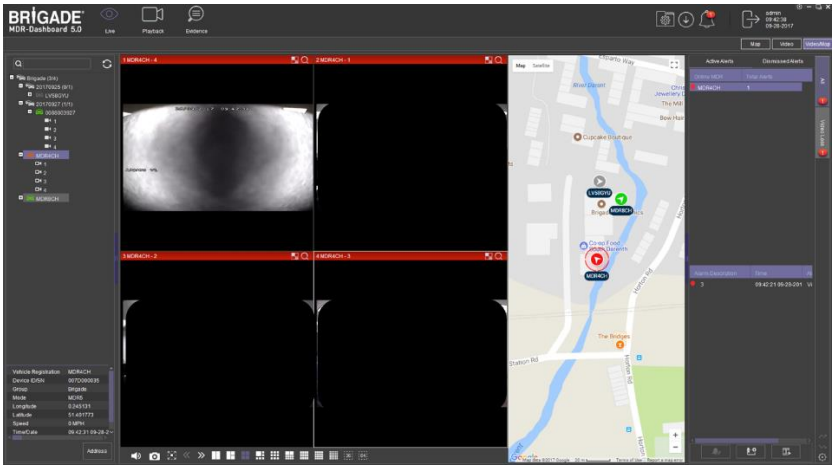
This mode is used to view video channels only. See *Video View Figure 183*. The order of the video channels may be changed by dragging the channel to another slot.



Video View Figure 183

6.4.3 Video/Map

This view is used to access both video and map data. See *Video/Map View* Figure 184 for an example.



Video/Map View Figure 184

6.5 Real-Time Alarm Log (Area 6)

Real-time Alarm Log Figure 185 shows alarms that are currently occurring on all online MDRs.

At the bottom of the Real-Time Alarm Log area is a menu as shown in *Alarm Menu Figure 186*.

Click on **LOCKING CAR** symbol  to access the Video/Map view with the vehicle locked in the center of the map.

Use the **OPEN VIDEO** button  to access Video/Map view with the video displayed below the map.

The bottom right gear icon  represents **SETTINGS** for the alarm hierarchy. The order in which alarms will appear. See *Alarm Settings Figure 187*.

There is an alarm count which indicates the number of alarms that have occurred. Once this number is higher than 99, the alarm log will display "99+".

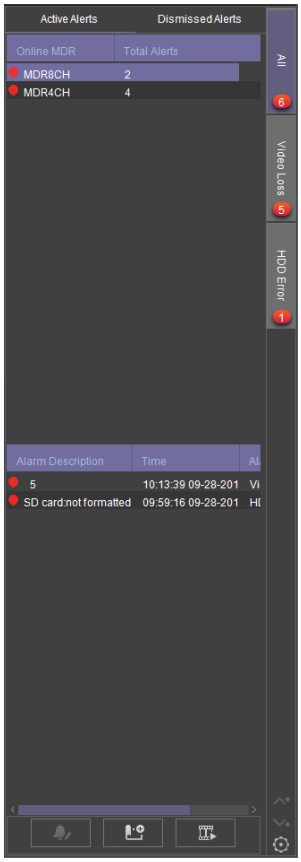
Processing alarms refers to when a user clears an alarm (marks an alarm as dismissed) once the alarm has been reviewed.

ACTIVE ALERTS show alarms that have not been processed by a user. See *Real-time Alarm Log Figure 185*.

To process an alarm, click an alarm event found in the active alert log (below Event Name), then click on the **PROCESS** button  . A pop-up window will appear as shown in *Alarm Processing Figure 188*. Write a description of the event, for example, false alarm.

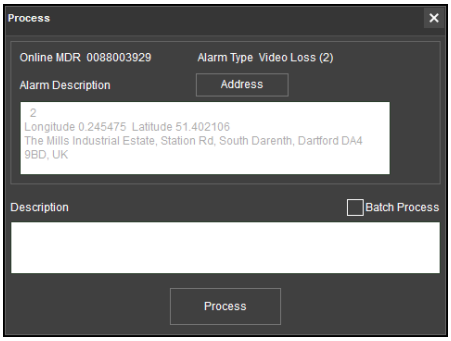
Click **PROCESS** to process an alarm event. Once processed, it will appear automatically under the **DISMISSED ALERTS** log.

BATCH PROCESSING is used to process multiple alarms of the same type. This is done by ticking **BATCH PROCESSING** in the process window. See *Alarm Processing Figure 188*.

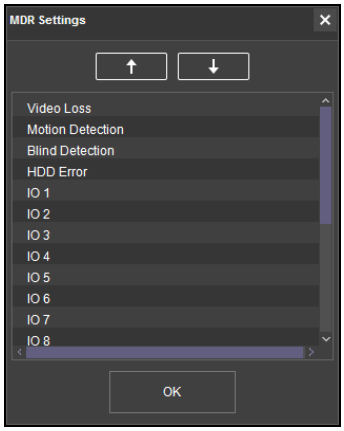


Real-time Alarm Log Figure 185

Alarm Menu Figure 186



Alarm Processing Figure 188



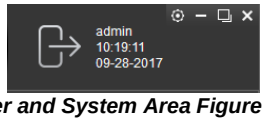
Alarm Settings Figure 187

6.6 User and System settings (Area 4)

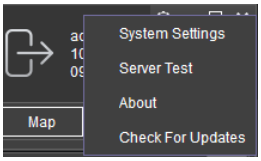
The current logged in username, date (Client PC) and time (Client PC) is displayed. See *User and System Area Figure 189*.

This area is used to **LOGOUT**. This is achieved by clicking on the door icon  . This brings up a confirmation window for logging out. Click **YES** or **NO** and thereafter the MDR-Dashboard 5.0 login screen will be displayed. See *Logout Screen Figure 193*.

Click on the gear icon  to display a submenu containing **SYSTEM SETTINGS**, **SERVER TEST**, **ABOUT** and **CHECK FOR UPDATES** options. See *MDR-Dashboard Settings Menu Figure 190*.



User and System Area Figure 189



MDR-Dashboard Settings Menu Figure 190

SERVER TEST is used to aid troubleshooting server connections, the feature is used to determine which port is not functioning. See *Server Test Figure 191* and *Server Test Results Figure 192*.

ABOUT displays the window shown in *About Figure 194*. This will show the current MDR-Dashboard and MDR Server version.

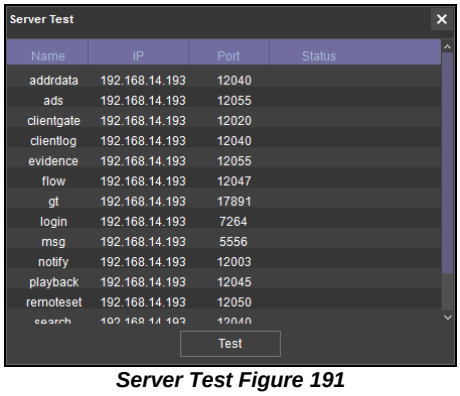
Additional information of which server ports are used will be shown in the **ABOUT** window when the MDR-Dashboard is logged in as server mode. See *About Figure 194*.

CHECK FOR UPDATES is used to check for software updates. This will redirect you to webpage (brigade-electronics.com/MDR-Software-Update). Here you will be able to find new MDR-Dashboard software releases.

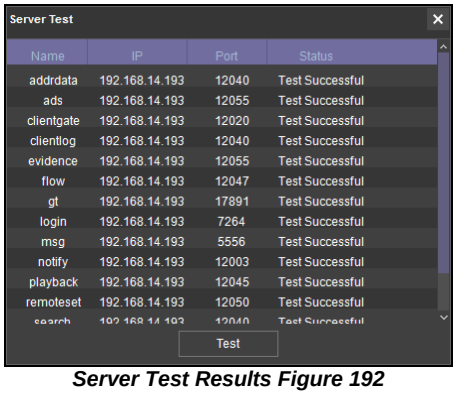
SYSTEM SETTINGS are shown in *System Settings Figure* 195.

This area is used to configure the following:

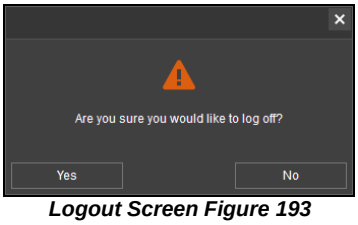
- Set Path for Snapshots
- Map Mode
- Language
- Speed Unit
- Temperature Unit
- Automatically Switch to Main Stream – tick this box to use the main stream (higher quality) or leave unticked to use the sub-stream. This is not supported for the MDR 400 Series.
- Loop Video Playback – this will play the entire selected video on repeat. This feature can be used for HDD or directory playback
- Auto-logout
- Auto-Close Video
- Total Alarms Shown – shows the historical alarms and events in the real-time alarm log area. By default, it is 200.
- Alarm Period Shown – shows the alarms and events for the past time range setting in the real-time alarm log area. By default, it is 30 minutes.
- Enable Dual Monitor Map View (Server Mode – Live view only) – this will expand the map to a separate window. This helps when monitoring multiple online vehicles.



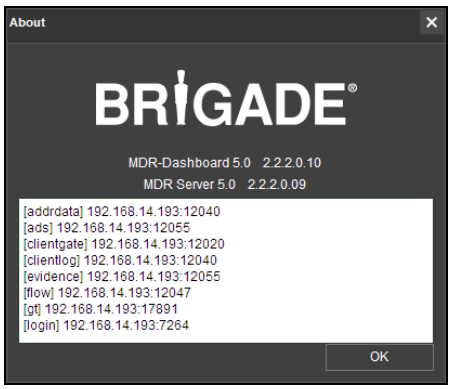
Server Test Figure 191



Server Test Results Figure 192



Logout Screen Figure 193



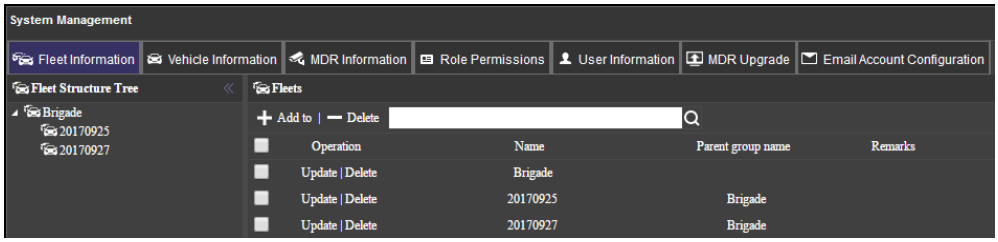
About Figure 194

System Settings Figure 195

Browse to **SYSTEM MANAGEMENT** by clicking on the following icon  . See *System Manage Figure 196*.

System Management is used to configure the following options:

- Fleet Information
- Vehicle Information
- MDR Information
- Role Permissions
- User Information
- MDR Upgrade
- Email Account Configuration



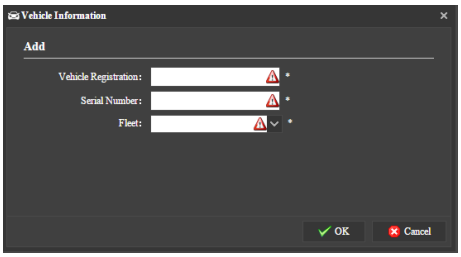
System Manage Figure 196

6.6.1 Fleet Information

You can use this area to setup **VEHICLE FLEETS** (e.g. Brigade) under the **COMPANY VEHICLE STRUCTURE TREE**. This area can also be used to setup sub-groups which will be found under Vehicle Fleets.

6.6.2 Vehicle Information

This area is used to setup **VEHICLE INFORMATION**. When setting up the vehicle registration and serial number, you must choose under which **FLEET** this vehicle will be stored in. See *Vehicle Device Information Figure 197*.



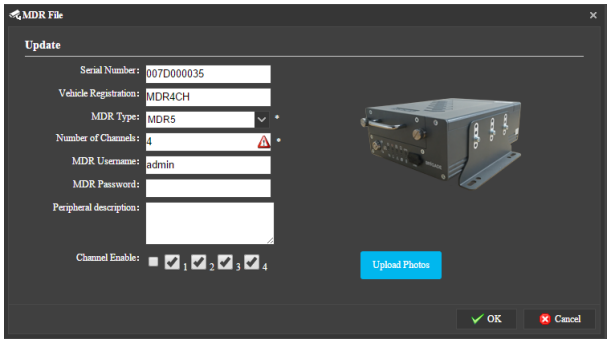
Vehicle Device Information Figure 197

6.6.3 MDR Information

This area gives the user further information on a specific MDR unit. This is also used to **UPDATE** the **EQUIPMENT FILE** (window that contains detailed information on a specific MDR). See *MDR File Figure 198*.

This allows you to track serial number, vehicle registration, MDR type, number of channels, MDR username, MDR password, peripherals and enables channels. If a channel is disabled, it will not be available to view in live view pane. See *MDR File Figure 198*. **SERIAL NUMBER must match the serial number shown in MDR firmware**.

Note: If an 8-channel device is showing only 4 channels, please update the **NUMBER OF CHANNELS** within MDR information. Log out and log in to confirm that this device now shows up correctly. See *MDR File Figure 198*.

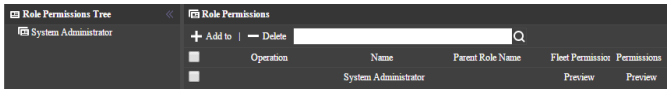


MDR File Figure 198

6.6.4 Role Permissions

This area is used to create more permission types which **USERS** will be assigned to.

ROLES TREE shows the structure of permissions. See *Creating New Roles Group Figure 199*.

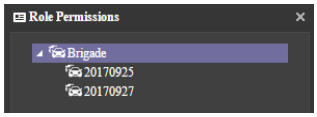


Creating New Roles Group Figure 199

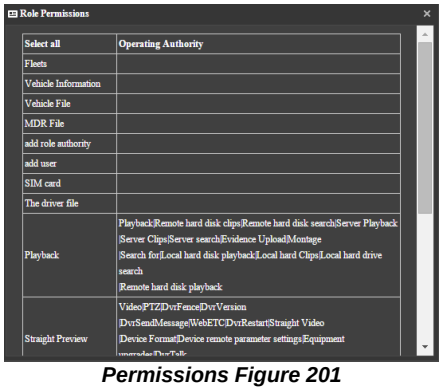
Clicking on **GROUP PERMISSIONS PREVIEW** shows the **ROLE AUTHORITY** window which will indicate the **VEHICLE FLEETS** and the sub-groups a role has access to. See *Group Permissions Figure 200*.

PERMISSIONS PREVIEW shows a quick view of the options that this role would have access to. See *Permissions Figure 201*.

Certain permissions are only accessible depending on your parent role. If the parent role is system administrator, then all permission will be shown for editing. See *Role Authority Details 1 Figure 202* and *Role Authority Details 2 Figure 203*.

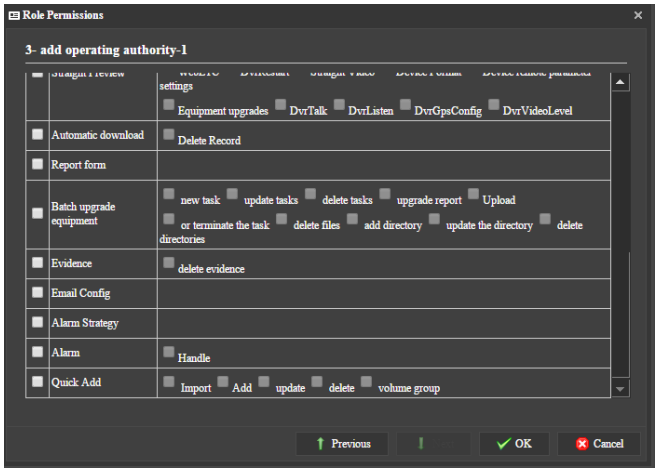


Group Permissions Figure 200



Permissions Figure 201

Role Authority Details 1 Figure 202



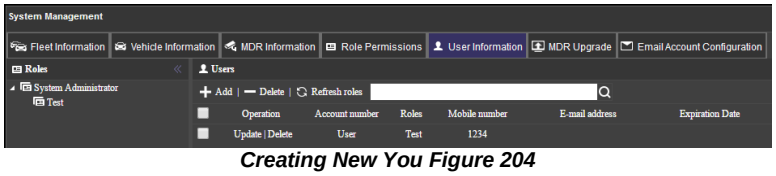
Role Authority Details 2 Figure 203

Table 15: User Permission Explanations:

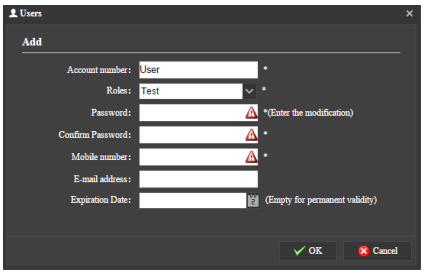
#	OPTIONS	OPERATING AUTHORITY	EXPLANATIONS
(1)	Vehicle fleet	N/A	Allows the user to manage the vehicle group.
(2)	add vehicle	N/A	Allows the user to add/edit/delete vehicle.
(3)	Vehicle file	N/A	Edit the Device (MDR) Information settings.
(4)	Equipment file	N/A	Not supported for MDR 400 Series
(5)	add role authority	N/A	Allow user account to manage role authority (add /edit /delete)
(6)	add user	N/A	Allow user account to manage user accounts (add /edit /delete)
(7)	SIM card	N/A	Not supported for MDR 400 Series
(8)	The driver file	N/A	Not supported for MDR 400 Series
(9)	Playback	(9.1) Playback(9.2.) Remote hard disk clips (9.3) Remote hard disk search (9.4) Server Playback (9.5) Server Clips (9.6) Server search (9.7) Evidence Upload (9.8) Montage (9.9) Search for (9.10) Local hard disk playback (9.11) Local hard Clips (9.12) Local hard drive search (9.13) Remote hard disk playback	(9.1) Local directory files playback; (9.2) Remote clip MDR recording files (9.3) Remote search MDR recording file search (9.4) Remote playback MDR server recording files (9.5) Remote clip MDR SERVER recording files (9.6) Remote search MDR SERVER recording files (9.7) Evidence recording files, snaps, alarm information to Evidence Center (9.8) Local direction files clip (9.9) Local direction files search (9.10) Local HDD/SD card playback (9.11) Local HDD/SD card clip (9.12) Local HDD/SD card search (9.13) Remote MDR recording files playback
(10)	Straight Preview	(10.1) Video (10.2) PTZ (10.3) Straight Video (10.4) Device Format (10.5) Device remote parameter settings (10.6) Equipment upgrades	(10.1) Live view (10.2) PTZ control (10.3) Live view record to local PC (10.4) MDR storage remote format (10.5) MDR parameters remote setting (10.6) MDR MCU/firmware remote upgrade
(11)	Automatic download	N/A	Auto download recording files
(12)	Report form	N/A	This feature is not supported with MDR 400 Series products
(13)	Batch upgrade equipment	(13.1) new task (13.2) update tasks (13.3) delete tasks (13.4) upgrade report (13.5) Upload (13.6) or terminate the task (13.7) delete files (13.8) add directory (13.9) update the directory (13.10) delete directories	(13.1) New auto download task creating (13.2) auto download task update (13.3) auto download task delete (13.4) MCU/firmware upgrade report (13.5) MCU/firmware files upload to the server computer (13.6) execute or terminate upgrade task (13.7) Delete MCU/firmware files (13.8) Add MCU/firmware files storage file folder in server computer (13.9) Update MCU/firmware files storage file folder in server computer (13.10) Delete MCU/firmware files storage file folder from server computer
(14)	Evidence	N/A	This gives user accounts access to the Evidence Tab, see *Evidence Icon Figure 162*.
(15)	Email Config	N/A	This gives you the ability to setup the Email Account Details, see *Email Configuration Figure 216*.
(16)	Alarm Strategy	N/A	This gives you access to the Alarm Strategy settings found in the alarm center, see *Alarm Configuration Figure 181*
(17)	Email Plan	(17.1) Add (17.2) Update (17.3) Delete	(17.1) Add email setting to send some alarm information to somebody's email address (17.2) Update email setting (17.3) Delete email setting
(18)	Alarm	(18.1) Handle	Allow user account to manage alarm message (event), including LOCK vehicle in map, turn on/off alert voice when new alarm happen, open channel live view. Not including PUSH authority.

6.6.5 User Information

To setup **USER LOGIN** accounts, see *Creating New You Figure 204*. These are the accounts that are used to login into MDR-Dashboard 5.0. If a user has forgotten their password the system administrator has the access to reset their password. Passwords can be reset in this area. See *Updating User Accounts Figure 205*.



Creating New You Figure 204

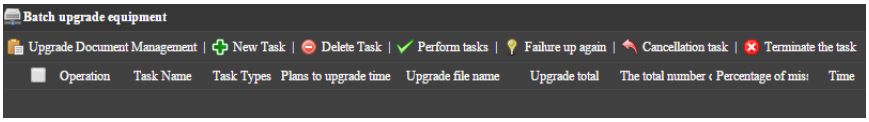


Updating User Accounts Figure 205

6.6.6 MDR Upgrade

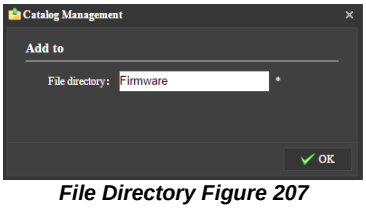
This area is used to setup **BATCH UPGRADES** for MDR units.

Click on Upgrade Document Management to create a new directory and upload the upgrade file. See the *Catalogue Management Figure 206*.



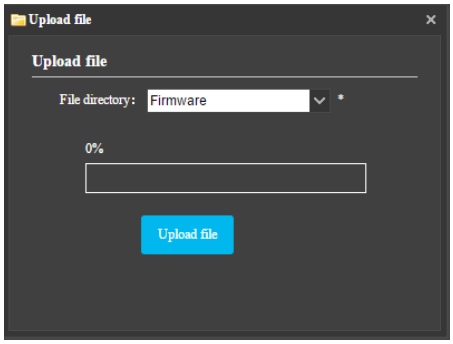
Catalogue Management Figure 206

Click New Directory and type in a desired name. See *File Directory Figure 207*. Select the newly created directory



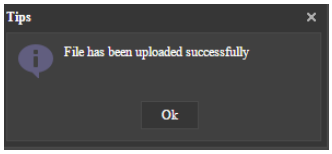
File Directory Figure 207

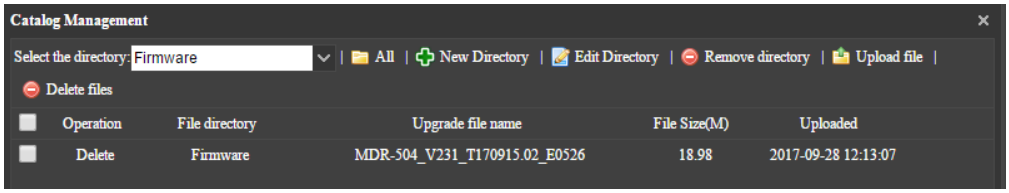
Click Upload file which will open the window displayed in *Upload File Figure 208*. The upgrade file must be located on the local PC to specify the **FILE DIRECTORY**.



Upload File Figure 208

Click Upload file and choose your firmware, once completed, the below window will show:





Catalogue Management List Figure 209

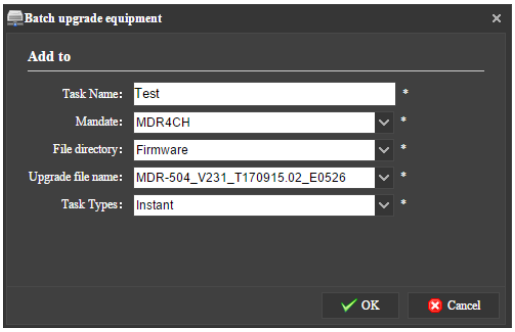
Click New Task which will display the *Batch Upgrade Equipment Figure 210* window.

TASK NAME can be chosen by the user. All other details are chosen from drop-down lists comprised of the **CATALOGUE LIST**. See *Catalogue Management List Figure 209*.

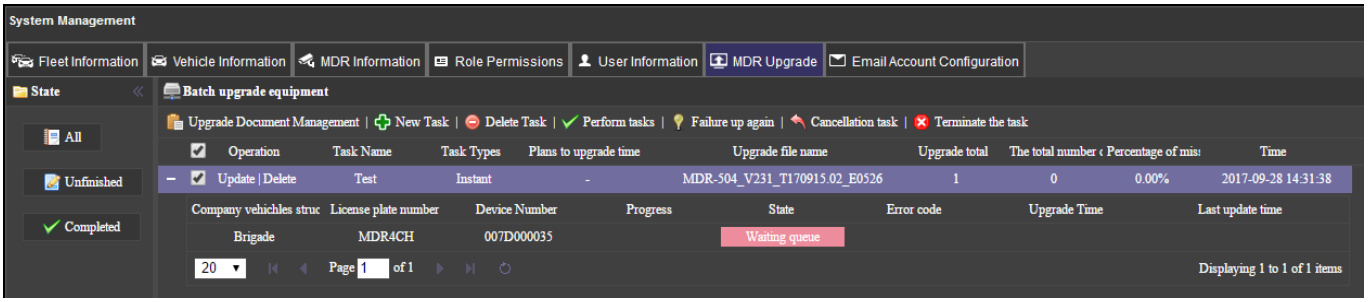
These upgrades can be done instantly or by appointment which is configured using **TASK TYPE**.

The state of the upgrades can also be determined from this area. See *Batch Upgrade Queue Figure 211* and *Successful Batch Upgrade Status Figure* 214.

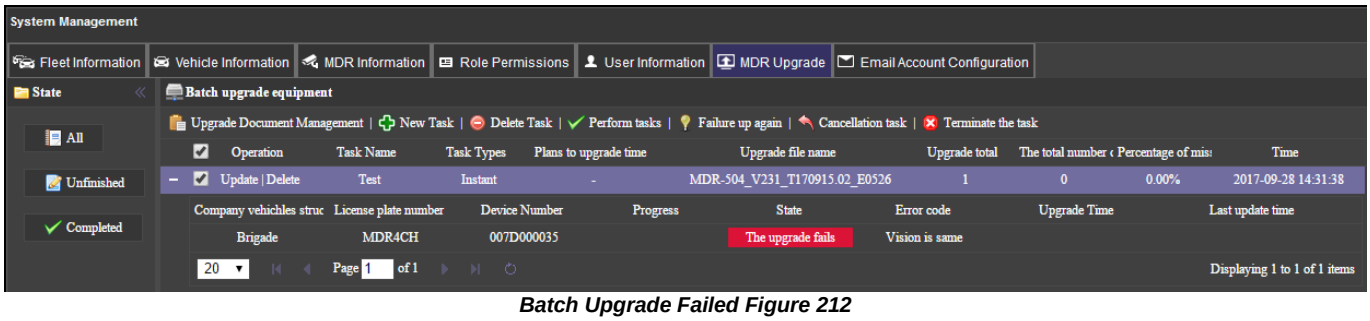
To begin the task, highlight the task and the click Perform tasks.



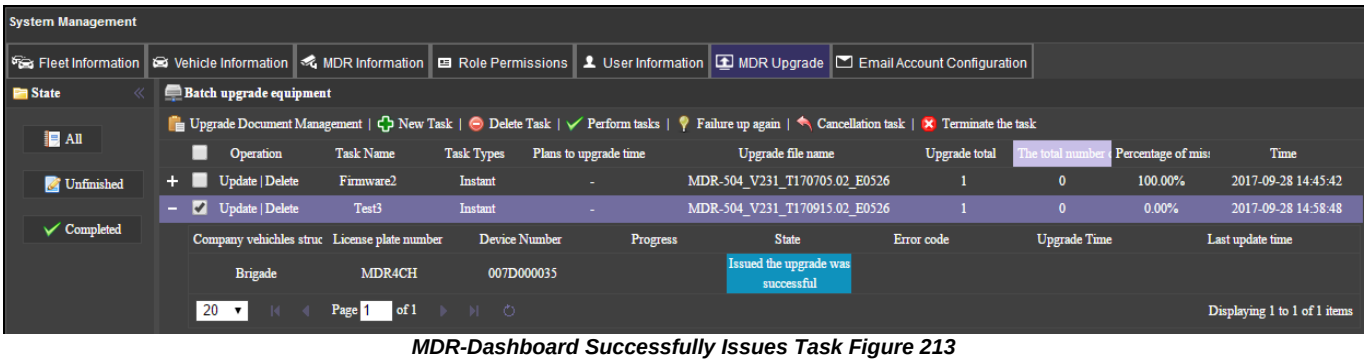
Batch Upgrade Equipment Figure 210



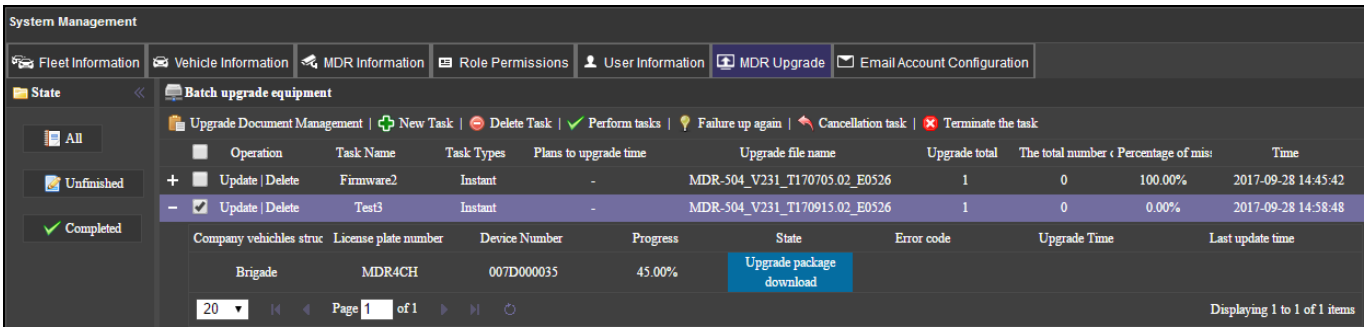
Batch Upgrade Queue Figure 211



Batch Upgrade Failed Figure 212



MDR-Dashboard Successfully Issues Task Figure 213



Successful Batch Upgrade Status Figure 214

Remote Upgrade Firmware Figure 215

6.6.7 Email Account Configuration

Only the **SYSADMIN** account has privileges to access this area.

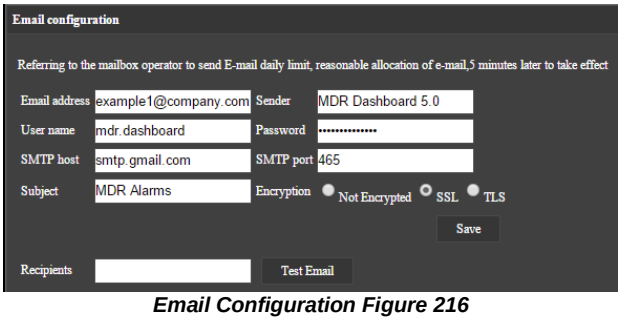
Under **SYSTEM MANAGEMENT**, browse to the **EMAIL** tab.

The **SENDING** server IP must also be allowed to relay email.

It is advised to request your IT department to setup a Microsoft Exchange account to be used. Ensure that this is named appropriately (MDR-Dashboard 5.0) to ensure that email alerts are clearly understood.

Email testing can be completed in this area. This is achieved by entering the email address recipient and then clicking the Test Email button. This area is used to configure the following email settings:

- Email Address
- User name
- SMTP host (Simple Mail Transfer Protocol)
- Subject
- Sender
- Password
- SMTP port
- Encryption has the following: Not Encrypted, SSL (Secure Sockets Layer) and TLS (Transport Layer Security)



Email Configuration Figure 216

Alarm Email Notification Figure 217

The configuration shown in *Email Configuration Figure 216* may be used to send email alerts. Alternatively, you may create your own email address e.g. Company123@gmail.com.

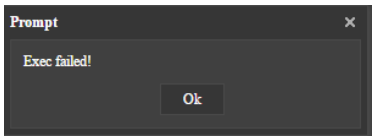
Ensure your mail filtering has an exception to allow these emails through. Usually emails take approximately 5 minutes to be delivered.

Email configuration should be tested before use.
To test your email configuration. Insert your email under **RECIPIENTS** and click the **TEST EMAIL** button.

All emails are marked with high importance as you can see in *Alarm Email Notification Figure 217*. The email will contain a "Test Success" message as shown in *Alarm Email Content Figure 218*.

Alarm Email Content Figure 218

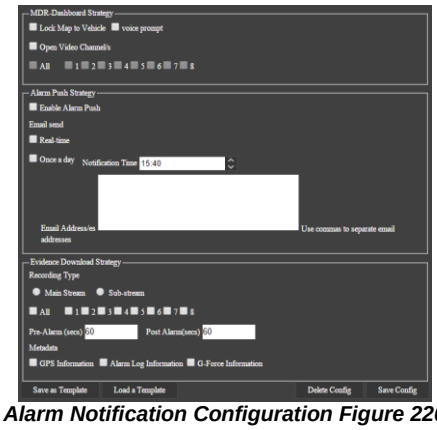
If the failure message (Execution failed!) shown in *Email Failure Message Figure 219* is displayed, then please confirm all details in *Email Configuration Figure 216* are correct.



Email Failure Message Figure 219

Email alerts may be set up by **ALARM QUERY** → Settings

Tick Real-time or Once a day as shown in *Alarm Notification Configuration Figure 220.*

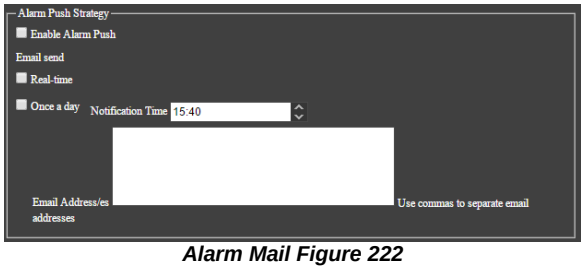


Alarm Notification Configuration Figure 220

The following details must be entered to use this feature:

- **Email Send** – can choose between Real-time or Once a day.
- **Notification Time** – Choose a time for once a day notifications.
- **E-mail Address/s** – enter multiple email addresses using a comma (,) to separate them

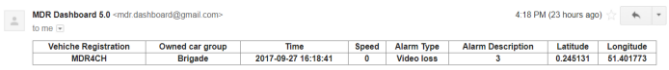
Once the *Alarm Notification Configuration Figure 220* has been completed and **OK** has been clicked, the new alert will be added to the list shown in *Alarm Mail Figure 222*.



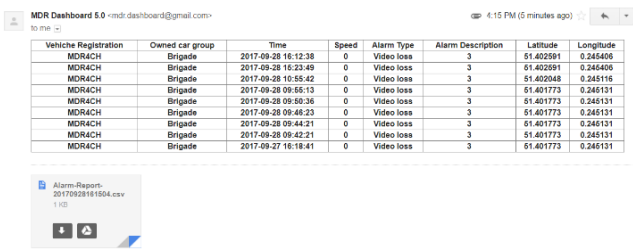
Alarm Mail Figure 222

An example of the email received when using Send real-time is shown in *Real-time Email Figure 221*.

An example of the email received when using **Once a day** is shown in *Once a day Email Figure* 223. Regularly send emails will contain alarm reports in excel spreadsheet format



Real-time Email Figure 221



Once a day Email Figure 223

7 Mobile Apps

MDR 5.0 is a free mobile application, available for both Android and iOS operating systems. The **MDR 5.0** application has the following features:

- Live View
- Map positions of MDRs (MDR must have GPS connected and locked signal)
- Remote Snapshot one channel at a time - saved to local device

7.1 iOS App

7.1.1 iOS App Requirements

Table 16: Minimum requirements for MDR 5.0 to run on iOS

DEVICE	MINIMUM REQUIREMENTS
iPhone	iPhone 5 iOS 9.0
iPad	iPad 3 iOS 9.0
iPad mini	No Requirement
iPad Pro	Currently not supported

7.1.2 iOS App Installation

On your Apple device, go to the App Store.

Search for “Brigade Electronics” or “MDR 5.0”.

Click the **DOWNLOAD** button to begin the installation.

The app will then begin to install. The progress will be shown.

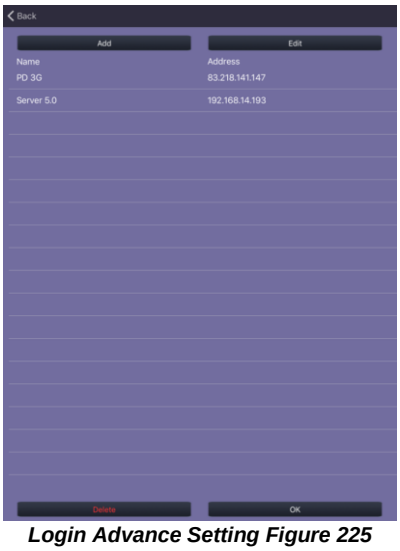
Once the installation has completed, click the **OPEN** button.

In the next window, click **OK** to allow MDR 5.0 to send you notifications, this is a generic request.

The login window will be displayed, see *iOS App Login Figure 224*. These login details correspond to MDR-Dashboard 5.0 login details.

It is advised to create User accounts (in MDR-Dashboard 5.0 System Management Area) for MDR 5.0 app logins so this can be tracked in the MDR-Dashboard 5.0 Alarm processing area.

iOS App Login Figure 224



Login Advance Setting Figure 225

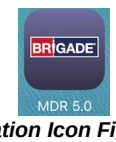
7.1.3 iOS App Operation

Depending on the MDR features and location, you can connect to an MDR Mobile Network Server or an MDR Wi-Fi Server.

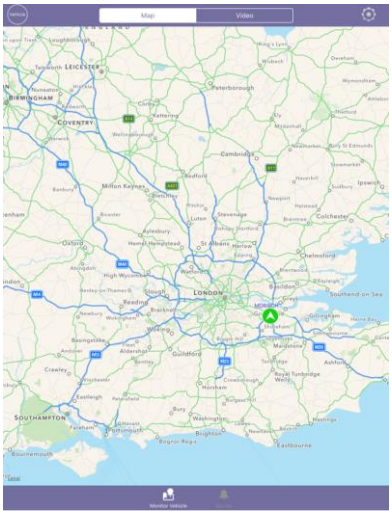
If MDR Center Server 1 and/or Center Server 2 are connected, then this MDR will be available in the mobile application.

Tap the application icon as shown in *Application Icon Figure 226*.

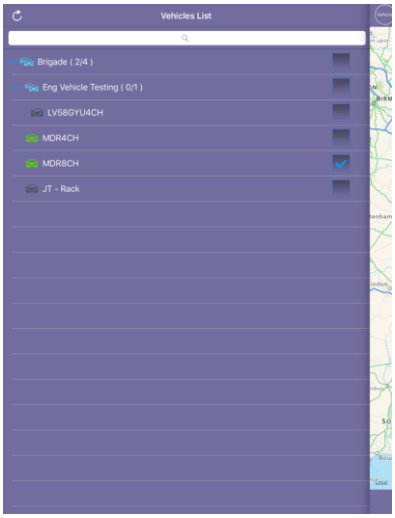
The iPhone login screen is then displayed as shown.



Application Icon Figure 226



iOS Map View Figure 227



iOS Group List Figure 228

To log into the Mobile Network server, ensure the mobile device is connected to the internet using its mobile network.

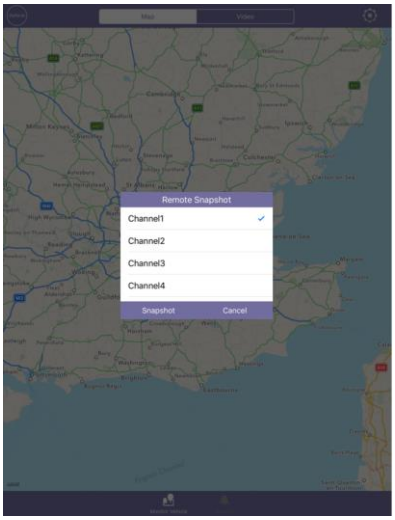
Type in the Mobile Network server address (public IP address of the firewall) into MDR 5.0 e.g. 12.345.6.78.

To log into the Wi-Fi server, ensure the device is connected to the SAME Wi-Fi network that the MDR Server and MDR unit is connected to.

Type in the Wi-Fi server address in MDR 5.0, e.g. 192.168.1.14.

The **USER** by default is **admin** and the **PASSWORD** by default is **admin**. Brigade does NOT recommend using **LOGIN AUTOMATICALLY** if there are several servers available.

iOS Map sub-menu Figure 229



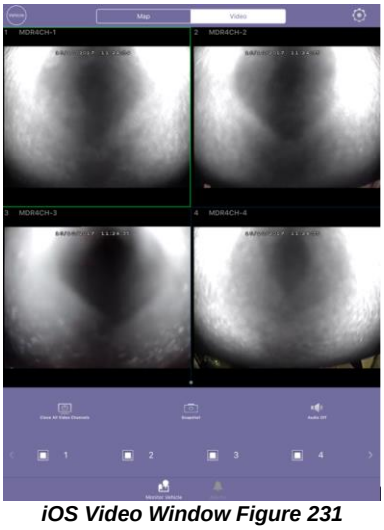
iOS Remote Snapshot Figure 230

Note: When connecting to the Wi-Fi server, if the Wi-Fi network does not have internet access then the map function will appear blank. The Wi-Fi router may be configured to have internet access if necessary, please contact your IT department.

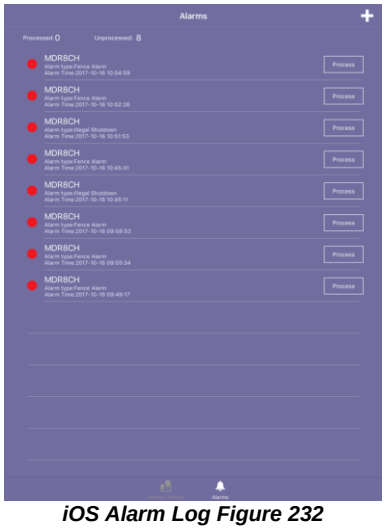
Once logged in you will be presented with the **MAP** window.

Tap on **VEHICLE** to bring up the **GROUP** list as shown in *iOS Group List Figure 228*.

The blue icon represents the fleet group (company name). This can be collapsed or expanded. The green icon represents online vehicles. The grey icons represent offline vehicles.



iOS Video Window Figure 231



iOS Alarm Log Figure 232

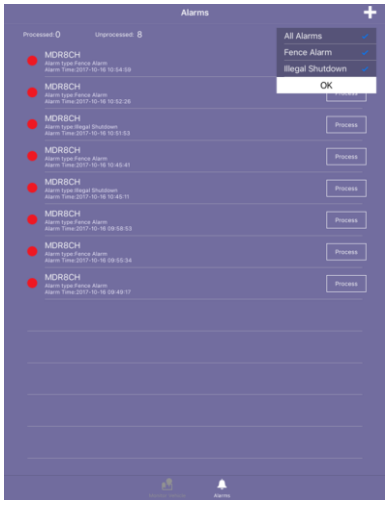
If a tick box under **GROUP** is ticked then that vehicle will be shown on the map.

To exit the **GROUP** list, tap on **VEHICLE**. See *iOS Group List Figure 228*.

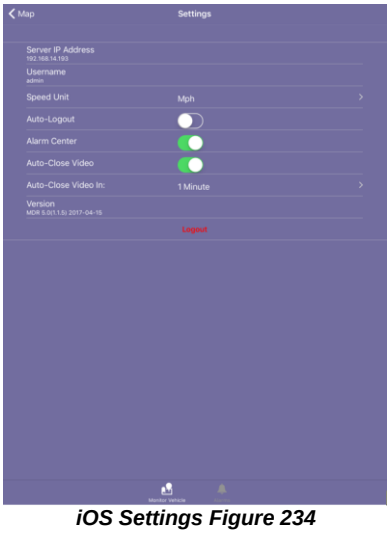
Tapping on an MDR will bring up the map sub-menu.

Online vehicles are depicted by green icons and offline vehicles are depicted by grey icons .

The map menu can be used to access Live video from an online MDR (*iOS Map View Figure 227*).



iOS Alarm Log Filter 233



iOS Settings Figure 234

To access **SETTING** you must be on the **MAP** window. Tap the gear icon will to open the menu:

Server displays the IP address the app is connected to.

Username displays the currently logged in user.

Speed Unit controls the speed unit shown within the app, this can be mph or km/h.

Auto-Logout logs out the user after 5 minutes.

Alarm Center displays current alarms in the alarm log. Maximum is 30 alarms.

Auto-Close Video will automatically close open video channels. This helps saves data. The options are 1, 5 and 10 minutes.

Version displays the app version details.

7.2 Android App

7.2.1 Android App Requirements

Table 17: The minimum requirements below are for MDR 5.0 to run on Android

DEVICE	MINIMUM REQUIREMENTS
Android Phone	Android 4.0 (Ice Cream Sandwich) Screen Resolution of 720P Screen Size of 4 inch
Android Tablet	Android 4.0 (Ice Cream Sandwich) Screen Resolution of 720P

7.2.2 Android App Installation

Open the Google Play Store App

Search for “Brigade Electronics” or “MDR 5.0”.

Tap the MDR 5.0 app. Click the **INSTALL** button.

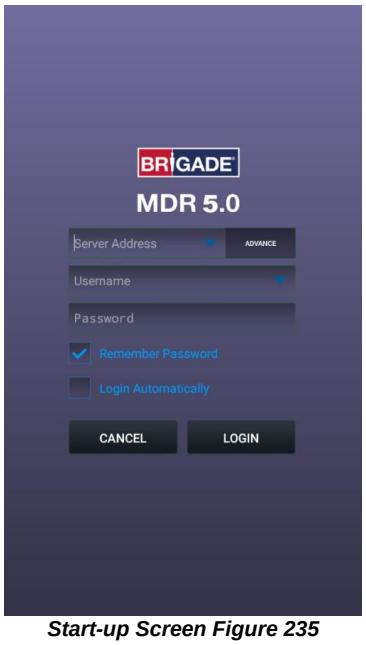
Click the **ACCEPT** button to allow the app access to the required device areas.

The app will then begin to install. The progress will be shown.

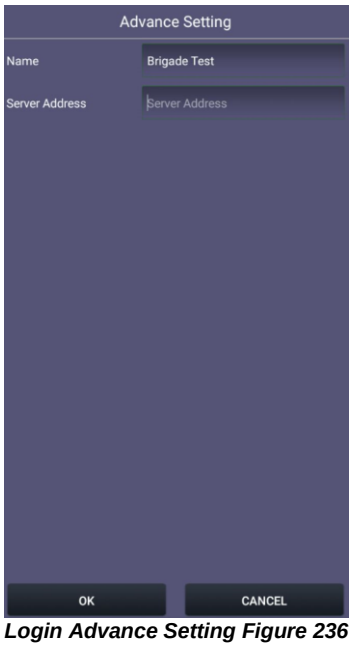
Once the installation has been completed. Click the **OPEN** button.

The login window will be displayed. These login details correspond to MDR-Dashboard 5.0 login details.

It is advised to create User accounts (in MDR-Dashboard 5.0 System Management Area) for MDR 5.0 app logins so this can be tracked in the MDR-Dashboard Alarm processing area.



Start-up Screen Figure 235



Login Advance Setting Figure 236

7.2.3 Android App Operation

Depending on the MDR features and location, you can connect to a MDR Mobile Network Server or MDR Wi-Fi Server.

If an MDR states that Center Servers 1 and 2 are connected then this MDR will be available in the mobile application.

Tap the application icon as shown in *Application Icon Figure 237*.

The start-up screen will be displayed.

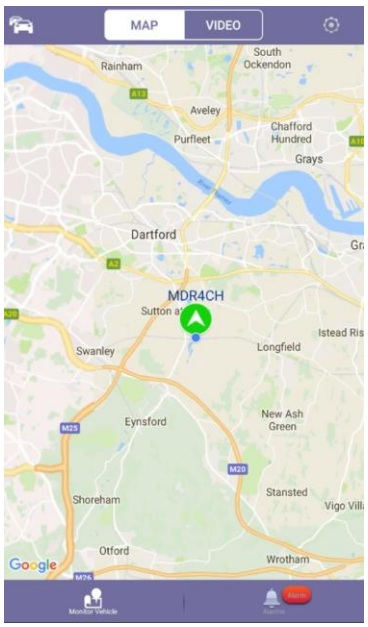
The Android login screen is then displayed as shown in *Android Login Figure 238*.

To log into the Mobile Network server, ensure the mobile device is connected to the internet using its mobile network.

Type in the Mobile Network server address (public IP address of the firewall) into MDR 5.0 e.g. 12.345.6.78.

Application Icon Figure 237

Android Login Figure 238



Android Map View Figure 239

To log into the Wi-Fi server, ensure the device is connected to the **SAME** Wi-Fi network that the MDR Server and MDR unit is connected to.

Type in the Wi-Fi server address in MDR 5.0, e.g. 192.168.1.14.

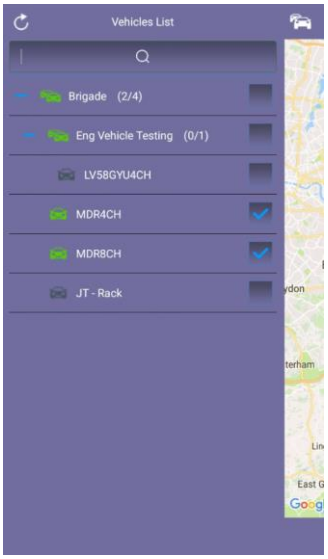
The **USER** by default is **admin** and the **PASSWORD** by default is **admin**. Brigade does not recommend using **LOGIN AUTOMATICALLY** if there are several servers available.

Note: When connecting to the Wi-Fi server, if the Wi-Fi network does not have internet access then the map function will appear blank. The Wi-Fi network may be configured to have internet access if necessary, please contact your IT department.

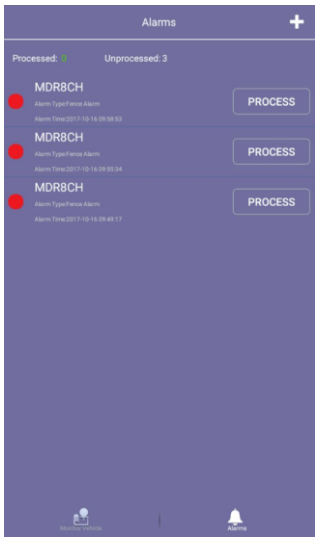
The operation of the Android application MDR 5.0 is explained in the above section 7.1 iOS App.

See Android Settings Figure 244, Android Snapshot Options Figure 245, Android Video Window Figure 247 and Android Settings Figure 248 for examples of Android application windows.

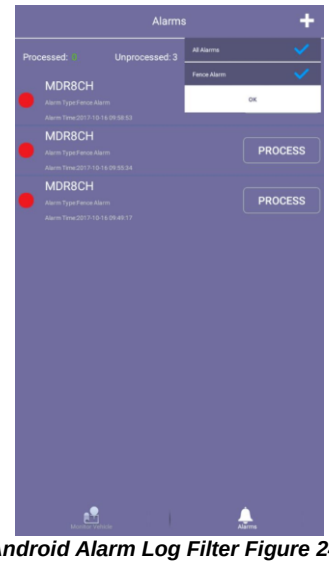
Android Map Alarm Figure 240



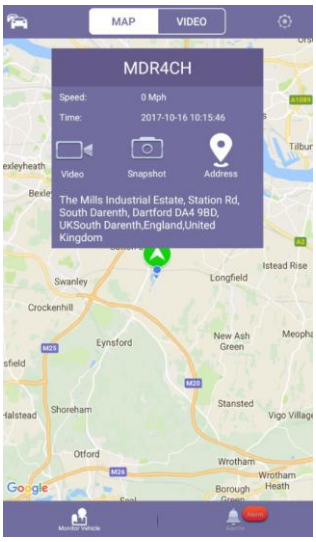
Android Cars List Figure 241



Android Alarm Log Figure 242



Android Alarm Log Filter Figure 243



Android Settings Figure 244

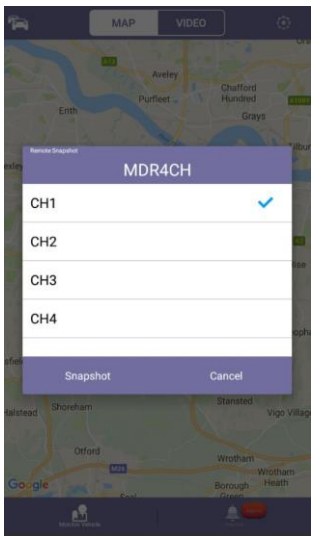
Further examples of typical android windows are shown *Android Snapshot Save Figure 246* onwards.

Android MDR 5.0 has an additional feature, which is channel zoom.

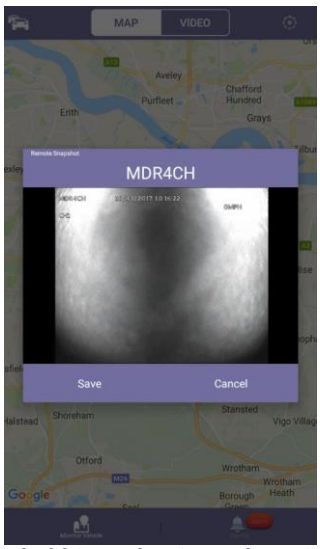
Open a single channel in full screen.

To view a channel area in greater detail, use two fingers in a pinch to zoom manner.

Push outwards to zoom in on a point and inwards to zoom out.



Android Snapshot Options Figure 245



Android Snapshot Save Figure 246

Server IP Address displays the IP address the app is connected to.

Username displays the currently logged in user.

Speed Unit controls the speed unit shown within the app, this can be mph or km/h.

Auto-Logout logs out the user after 5 minutes.

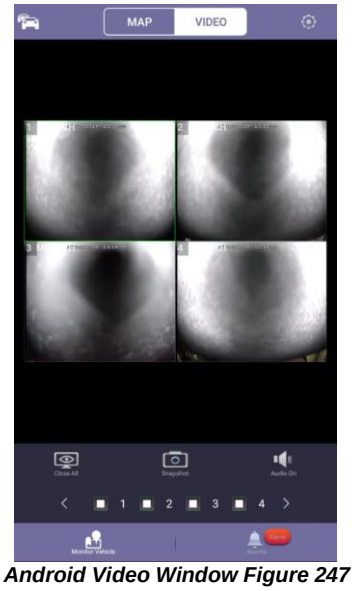
Alarm Center displays current alarms in the alarm log. Maximum is 30 alarms.

Auto-Close Video will automatically close open video channels. This helps saves data. The options are 1, 5 and 10 minutes.

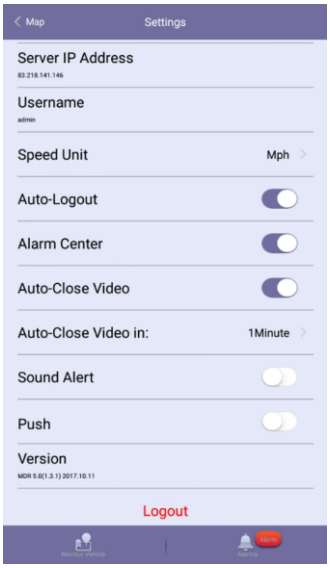
Sound Alert controls whether an audible alert is played for push notifications.

Push displays push notifications from the MDR app, if it is running in the background. (phones notification bar, usually top bar).

Version displays the app version details.



Android Video Window Figure 247



Android Settings Figure 248

8 MDR Server 5.0 Advanced Features

8.1 Database Backup and Restore

When completing database backups and restorations please read the warnings below:

(1) Do not operate the system and ensure there is no power cut during backing up or restoring data.

(2) If a backup or restoration operation fails, please attempt to do it again. If it fails once more, please contact Brigade Technical Support.

Backup:

(1) Backup only includes basic information of the vehicle system, such as fleet/group information, device information and driver information.

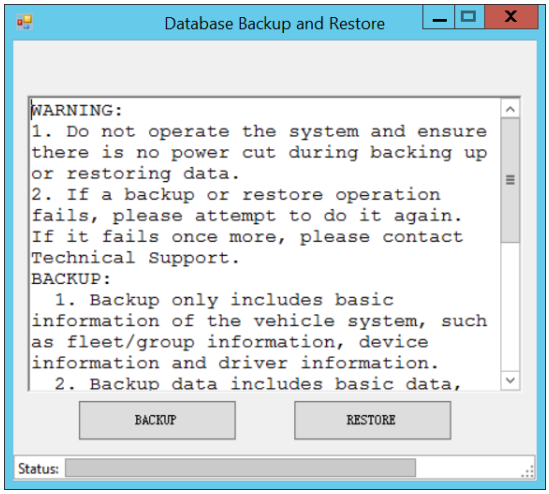
(2) Backup data includes basic data, such as GPS data and alarm information.

Restore:

(1) When restoring data from older MDR Server versions to newer versions, it will only restore the basic information, such as vehicle groups and device information.

(2) Restoring using the same MDR Server versions, it will restore both basic data and configuration items.

(3) To restore the GPS and alarm data from older MDR Server version to newer versions, use the Data Migration Tool.



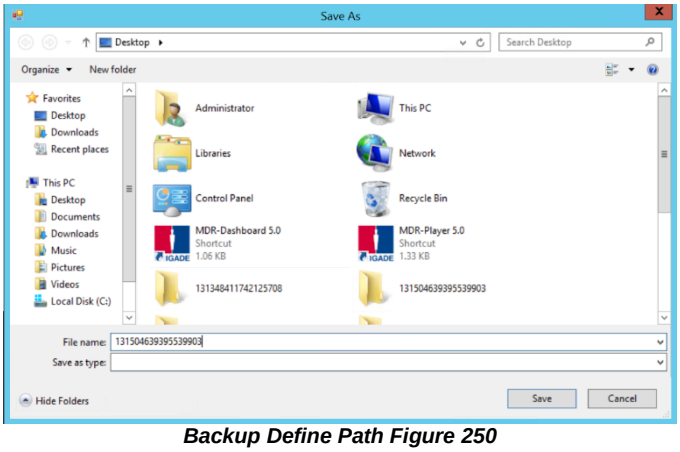
Database Backup and Restore Figure 249

8.1.1 Database Backup

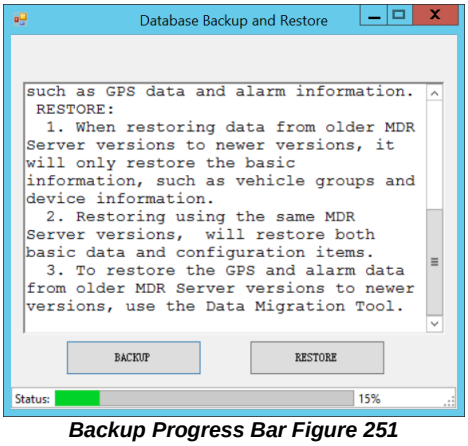
Follow the below steps to create a database backup:

- Brigade recommends backup processes to be completed after hours when the MDR Server will not be used.
- Click **BACKUP**, a windows file explorer will open.
- Choose the storage location for the backup.
- Brigade recommends creating a folder on your desktop with the creation date of the backup.
- Click **SAVE**, the backup progress bar will now be displayed.
- The period for each backup differs, this is based on content, size etc.
- Once the backup has been completed successfully, a prompt will be shown stating, “Data Backup success”.

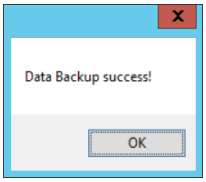
Typical Structure of an MDR Server backup is shown below. This must not be manipulated in any way. It could render the backup unusable.



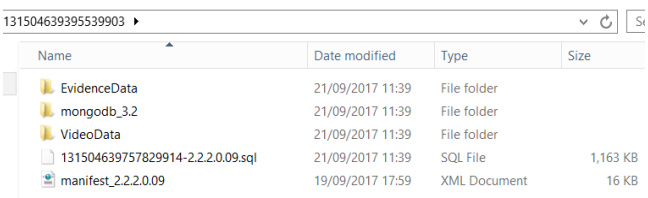
Backup Define Path Figure 250



Backup Progress Bar Figure 251



Successful Backup Figure 252

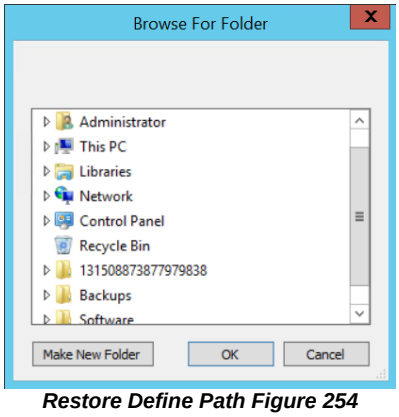


Structure of Backup Folder Figure 253

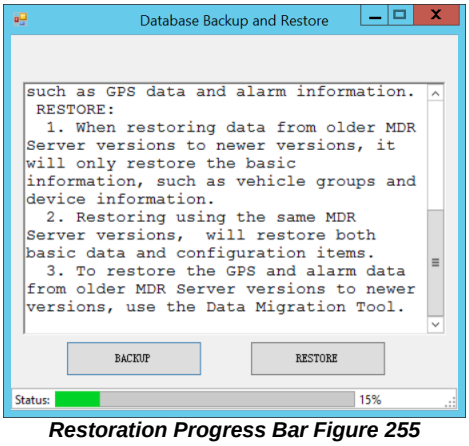
8.1.2 Database Restore

Follow the below steps to restore a database:

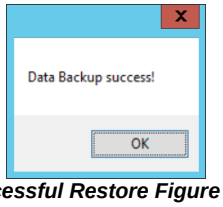
- Brigade recommends restore processes to be completed after hours when the MDR Server will not be used.
- Click **RESTORE**, a windows file explorer will open.
- Choose the location of your restoration file.
- Click **OK**, the restoration progress bar will now be displayed.
- The period for each restoration differs, this is based on content, size etc.
- Once the restoration has been completed successfully, a prompt will be shown stating, “Data Backup success”.
- If you are already logged into MDR-Dashboard 5.0, you will need to logout and login with the restored MDR Server details.
- You should now see the restored data fleet structure within MDR-Dashboard 5.0.



Restore Define Path Figure 254



Restoration Progress Bar Figure 255



Successful Restore Figure 256

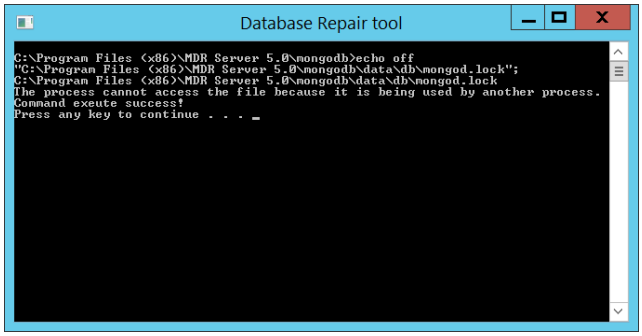
8.2 Database Repair Tool

This repair tool should only be used after hours, when the MDR Server is not in use. It is used to repair the mongodb service.

If the mongodb service does not start running, this tool can be used to attempt to start this service.

This tool can only be run if MDR Server control is closed. Using this tool will force the mongodb service to stop and then start.

Do not use this tool if it is not needed.



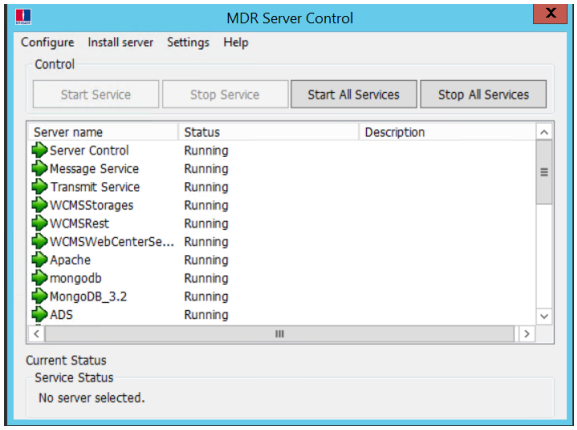
Database Repair Tool Figure 257

8.3 MDR Server Control

MDR Server Control is mainly used to check the status of services. It does have several other features that are discussed in further detail below.

Configure is used to set the MDR Server Control to autorun. This means that whenever the Windows Server is restarted, MDR Server will automatically run on start-up. The message server can also be configured here. By default, it is 127.0.0.1. This should not be changed.

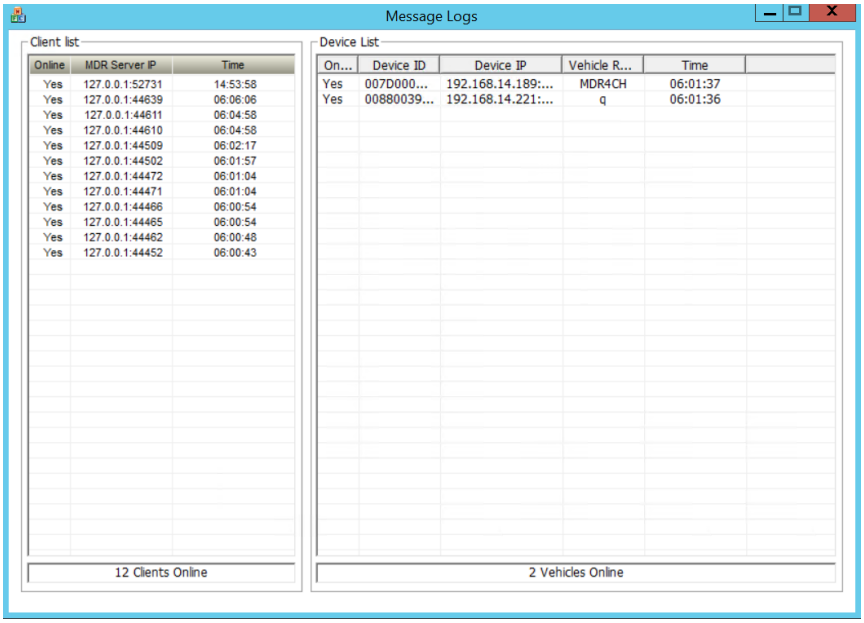
Install Server is used to install or uninstall a service. You can choose a specific service or all services.



MDR Server Control Figure 258

8.3.1 Message Logs

Double-clicking **Message Service** will open the message logs window. The client list will show MDR-Dashboard and MDR apps that are currently connected to MDR Server. Device list shows the MDR units that are currently connected to MDR Server.

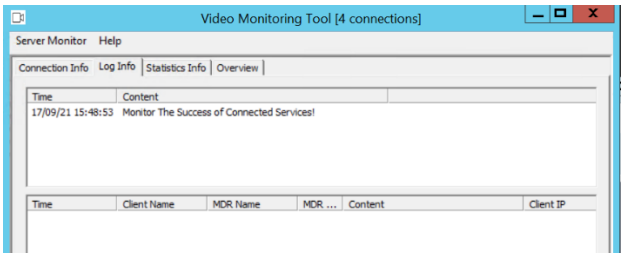


Message Logs Figure 259

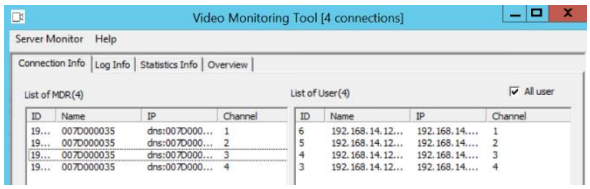
8.3.2 Video Monitoring Tool

Click **Settings** on the MDR Server control window then video monitoring tool to access it. Alternatively, double-clicking the **Transmit Service** will open the video monitoring tool.

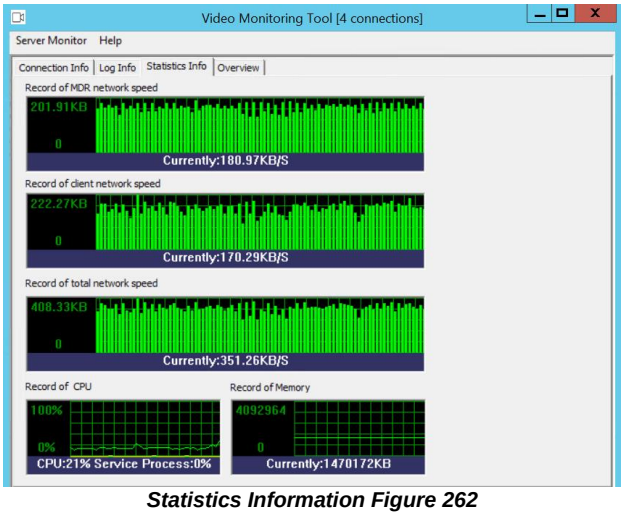
The Video monitoring tools can be used to monitor MDR/client connections to MDR Server. Network speeds can also be monitored within this tool.



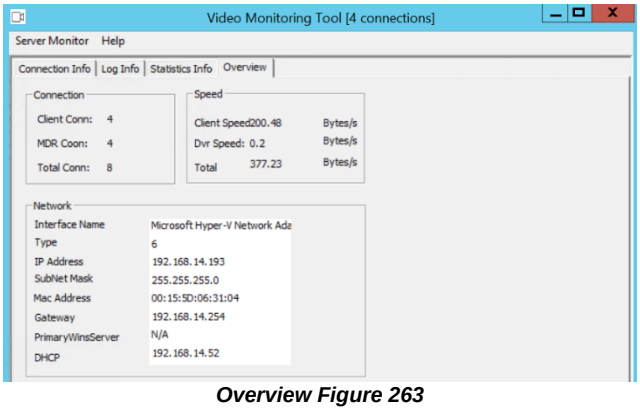
Log Information Figure 261



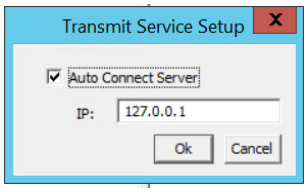
Connection Information Figure 260



Statistics Information Figure 262



Overview Figure 263



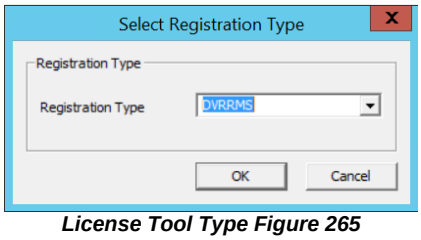
Transmit Service Setup Figure 264

8.3.3 License Tool

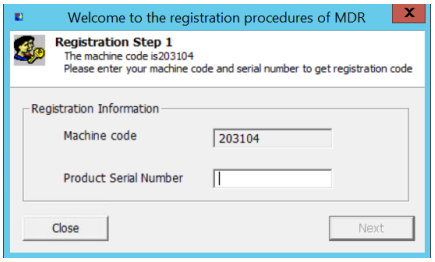
This tool is currently unused. Future purposes will be internal only (Brigade).

Follow the steps below to complete unlimited licensing:

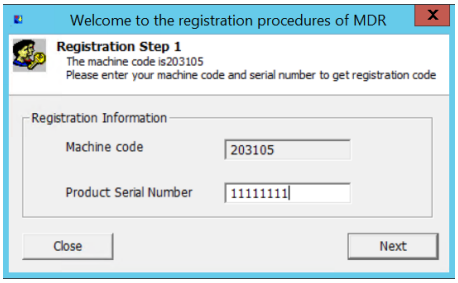
- Click **Settings** on the MDR Server control window then license tool to access it
- Choose DVRRMS and click **OK**.
- Take note of the Machine code - 203104.
- Submit this code to a Brigade engineer.
- Brigade engineer will create a registration code
- Once you have received the registration code, type in "11111111" into **PRODUCT SERIAL NUMBER**.
- Click **NEXT** then enter the registration code you received from a Brigade engineer.
- Click **REGISTER** to start the registration process.



License Tool Type Figure 265



License Registration Figure 266



Product Serial Number Figure 267

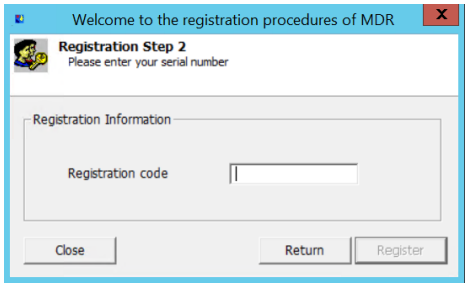


Figure 268

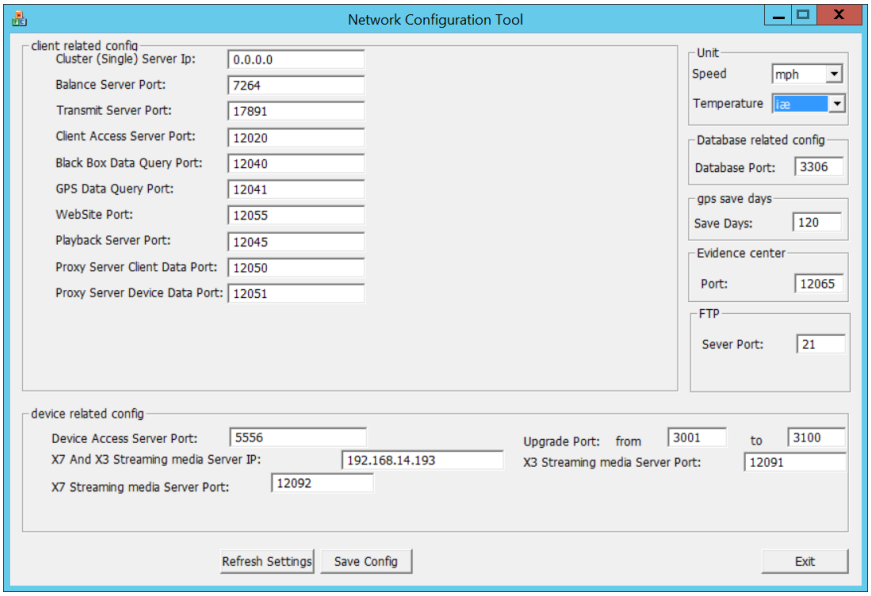
8.4 Port Configuration Tool

Port configuration tool is used mainly to manage an MDR Server's ports and IP address.

Speed and temperature units can also be changed within this tool.

Brigade recommends to not change any of these ports unless these ports are already being used by another software.

GPS data that is uploaded to the server can be retained for a defined period.

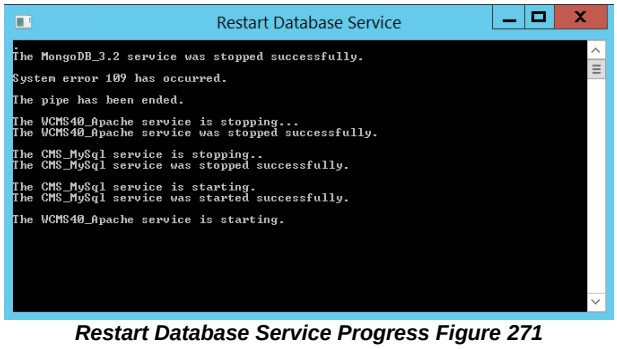


Port Configuration Tool Figure 269

8.5 Restart Database Service

This tool is used to restart all services related to the database. Brigade recommends using this tool after hours only, as this does stop several services.

Restart Database Service Figure 270



Restart Database Service Progress Figure 271

9 Appendices

9.1 Video Quality Table

Using Brigade's Resource calculator, the below tables have been compiled. Please note the following:

- The values below are for reference only
- Streaming bandwidth can vary considerably according to the level of variations in the image. Static images are more efficiently compressed than dynamic ones
- Frame rates are assumed to be set to maximum which is 25fps for PAL and 30fps for NTSC

Quality level		1 (Highest)	2	3	4	5	6	7	8 (Lowest)
Video Streaming Data Rate (Kbps) depending on resolution	D1 (Highest)	2048	1536	1230	1024	900	800	720	640
	HD1	1280	960	768	640	560	500	450	400
	CIF (Lowest)	800	600	480	400	350	312	280	250

9.2 Normal / Alarm Recording Parameters

***Warning*:The values shown below are for reference only.**

The table below summarises typical recording sizes for 1 channel at different qualities and resolutions for a one-hour duration:

Quality level		1 (Highest)	2	3	4	5	6	7	8 (Lowest)
Recording data size (MB per hour) depending on resolution	D1 (Highest)	900	675	540	450	395	351	316	281
	HD1	562	422	337	281	246	219	198	176
	CIF (Lowest)	351	264	211	176	153	137	123	110

The following table is valid for both the **MDR-504xx-500** using all **4** channels and **MDR-508xx-1000** using all **8** channels. It illustrates approximate **HDD** recording times in hours:

Quality level		1 (Highest)	2	3	4	5	6	7	8 (Lowest)	fps
Recording Time onto HDD (hours) depending on resolution	D1 (Highest)	101	160	231	299	367	425	481	539	12 (8CH) 25 (4CH)
	HD1	145	204	272	340	408	466	522	580	25
	CIF (Lowest)	199	326	435	544	652	746	837	932	25

9.3 Sub-Stream Recording Parameters

The following table is valid for both the MDR-404xx-500 using all 4 channels and MDR-408xx-1000 using all 8 channels. It illustrates approximate SD recording times in hours at CIF resolution and different frame rates. Ranges of frame rates are controlled by the sub-stream bandwidth.

Note: Sub-stream and Mainstream recording onto SD card has resource limitations, the maximum bitrate is 12Mbps.

Bandwidth		4096 Kbps	3200 Kbps	1500 Kbps	500 Kbps
Recording Time onto SD (hours) depending on frame rate	25 fps (fastest)	12			
	20 fps	15			
	15 fps		20		
	10 fps		29		
	5 fps				60
	1 fps (slowest)				305

Please calculate using the following steps:

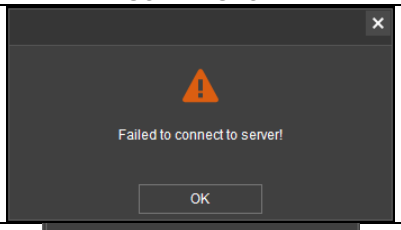
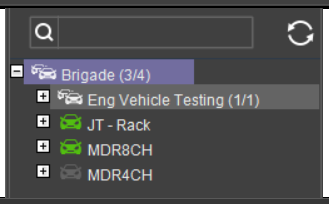
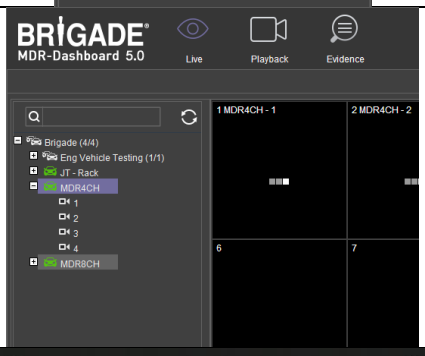
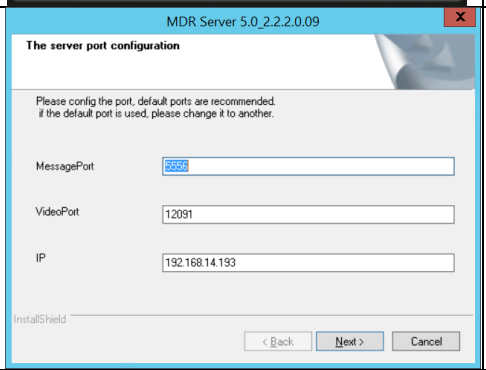
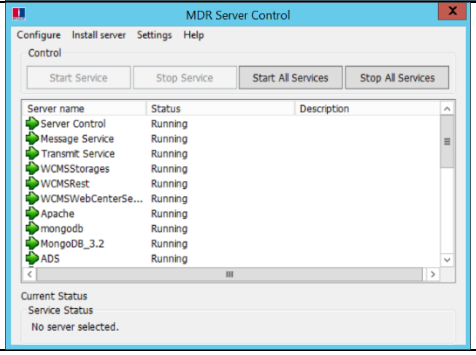
PAL: Actual Bit Rate = Actual framerate / 25 * Bit Rate (Full framerate) * transfer ratio
Transfer Ratio: Framerate (1-5):1.4; Framerate (6-11):1.3; Framerate (12-17):1.2; Framerate (18-22):1.1; Framerate (23-25):1.0

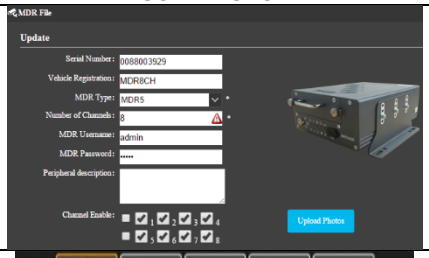
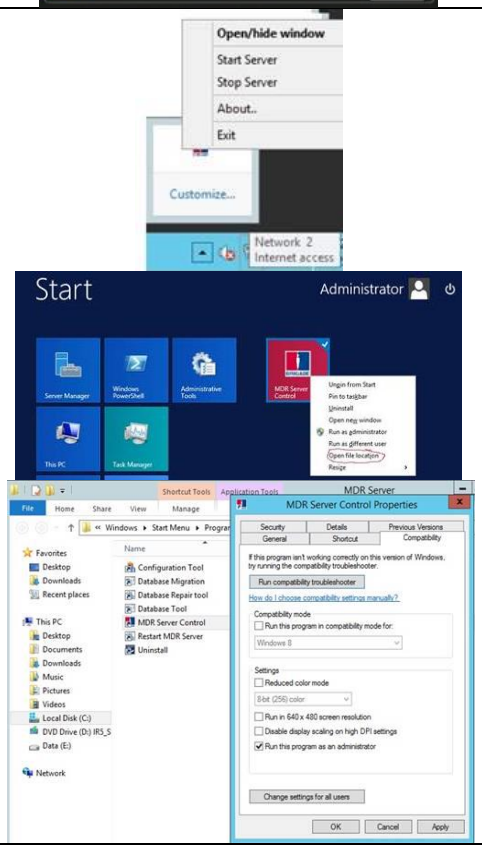
NTSC: Actual Bit Rate = Actual framerate / 30 * Bit Rate (Full framerate) * transfer ratio
Transfer Ratio: Framerate (1-6):1.4; Framerate (7-14):1.3; Framerate (15-21):1.2; Framerate (22-27):1.1; Framerate (28-30):1.0

10 Troubleshooting

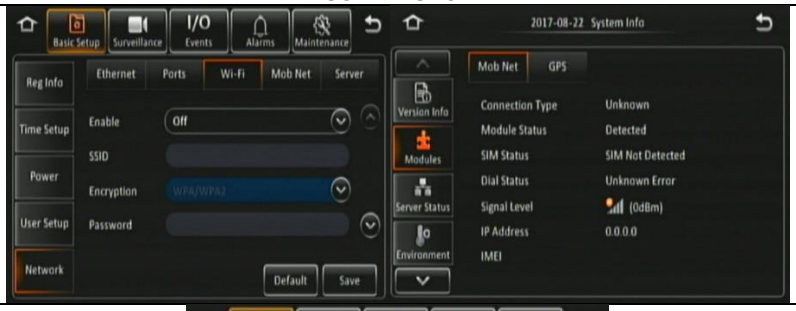
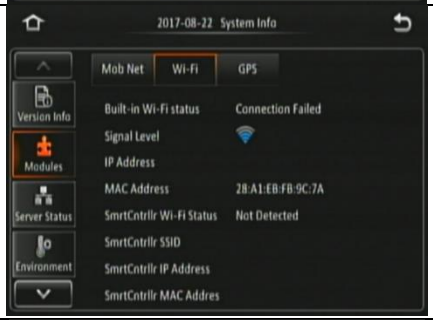
10.1 Mobile Network and Wi-Fi Troubleshooting

This chapter discusses various problem scenarios and their resolutions. This is not limited to the list below.

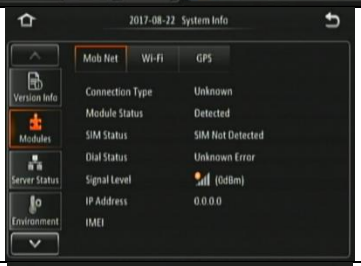
#	SCENARIO	SCREENSHOT	RESOLUTION
(1)	Unable to connect to my Wi-Fi Server		1. Check if you are connected to the MDR Server Wi-Fi network 2. Check your login details 3. Check if the Wi-Fi Windows Server is on 4. Confirm all services are running in the MDR Server software
(2)	MDR shows offline		1. Check if the MDR is out of network coverage 2. Confirm the MDR Network settings 2. Check if the Server status window indicates it is online 3. Confirm SERIAL NUMBER (in MDR-Dashboard settings) = SERIAL NUMBER (in MDR unit settings).
(3)	Able to connect to MDR, but cannot see Live Video in MDR-Dashboard		1. Check if Transmit service is running in MDR Server 2. First attempt to stop and restart the service using the MDR Server control window 3. If it is not running, obtain the new license file. Go to http://brigade-electronics.com/ to obtain this file. LIC_DVRGTSERVICE. Copy this file to the following path C:\Program Files (x86)\MDR Server\TransmitServer. Ensure the existing file is overwritten 4. Check network speeds, low speeds will result in video loading issues
(4)	MDR Dial Status says Failed Dial Up		1. Check if your SIM Data has been activated 2. Confirm the APN settings in the MDR are correct
(5)	All Features in Dashboard work apart from Live Video		1. Ensure that the MDR Server SW has been installed and the Public IP address has been used as its IP during the installation process. 2. If this was not done correctly, uninstall the SW, restart the Windows Server and re-install the SW using the correct IP.
(6)	MDR Server services refuse to start		1. Uninstall MDR Server 2. Install the latest Microsoft .NET Framework from the following website: https://www.microsoft.com/net/download This installation will replace any current .NET installation automatically 3. Re-install MDR Server 4. Run MDR Server as administrator.

#	SCENARIO	SCREENSHOT	RESOLUTION
(7)	I can only view certain channels in Live View, but I know I have 4/8 cameras		1. In MDR-Dashboard 5.0 ensure the number of channels are set correctly – system manage > MDR information.
(8)	Live View and Playback functions do not work		1. Ensure that the Media Server Port and MDR Server Port on the MDR hardware is correct
(9)	MDR Server is not running all services		1. This applies if the server is connected to a Domain and the local PC account is not being used 2. MDR server requires administrative rights. 3. Close the MDR-Server Control software by right clicking the MDR Server Control Taskbar tray icon > Exit 4. Click start, right click MDR-Server control > click Open file location 5. Right click MDR Server Control > click properties > go to compatibility tab > tick Run this program and administrator > click ok. 6. Now open the MDR server control again. You should see all services connected again.

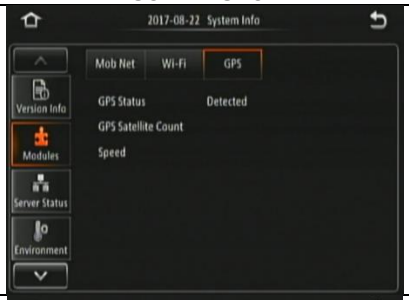
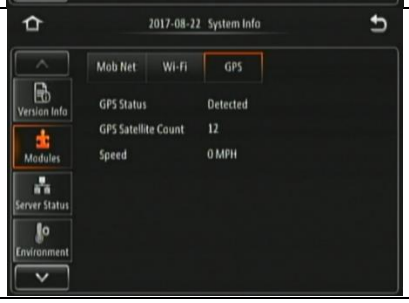
10.2 Wi-Fi MDR Status Troubleshooting

#	WI-FI STATUS	SCREENSHOT	EXPLANATION
(1)	Wi-Fi Enable: OFF		Wi-Fi is disabled in the MDR OSD Menu, this will mean the Wi-Fi tab in Sys Info will disappear
(2)	Wi-Fi Enable: ON		Wi-Fi is enabled in the MDR OSD Menu. Requires SSID, Encryption and Password.
(3)	Built-in Wi-Fi Status: CONNECTING		Access point details have just been entered, attempting to connect Status keeps switching between connecting and connection failed for an incorrect password
(4)	Built-in Wi-Fi Status: CONNECTION FAILED		SSID or Encryption has been entered wrong
(5)	IP Address: 192.168.14.240		Successfully obtained an IP address from network – confirms that there is proper connection to the network

10.3 Mobile Network MDR Status Troubleshooting

#	MOB. NET. STATUS	SCREENSHOT	EXPLANATION
(1)	Mob Net Enable: OFF		Mobile network is disabled in the MDR OSD Menu, this will mean the mobile network tab in Sys Info will disappear
(2)	Mob Net Enable: ON		Mob Net is enabled in the MDR OSD Menu. Requires Network Type, APN, Username, Password, Access Number and Certification.
(3)	SIM Status: SIM NOT DETECTED		No SIM card has been inserted in the MDR unit
(4)	Dial Status: FAILED DIAL UP		Incorrect Network Type, APN, Username, Password, Access Number and Certification.
(5)	Dial Status: UNKNOWN ERROR		Incorrect Network Type, APN, Username, Password, Access Number and Certification.
(6)	Dial Status: DIALLED UP		Dialled successfully and connected to a mobile network provider
(7)	IP Address: 10.14.33.5		Successfully obtained IP from a mobile network provider
(8)	Signal Level		Orange dot indicates that the mobile network antenna is not physically connected to the MDR antenna connector.

10.4 GPS MDR Status Troubleshooting

#	GPS STATUS	SCREENSHOT	EXPLANATION
(1)	GPS Status: NOT DETECTED		Has not detected the GPS module
(2)	GPS Status: DETECTED		GPS Satellite Count being blank indicates that the GPS antenna is not physically connected to the MDR antenna connector.
(3)	GPS Satellite Count: 1-24		GPS has valid signal and locked onto its position, the higher the value the better
(4)	Speed: 0 MPH		GPS has valid signal and locked onto its position, speed is 0 for a stationary vehicle

Approvals
CE
UNECE Regulation No. 10 Revision 5 (“E-marking”)
FCC
IC

Brigade Electronics
MDR-504xx-500/
MDR-508xx-1000

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any change or modifications not expressly approved by the responsible party responsible for compliance could void the user’s authority to operate the equipment.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. For products available in the US and Canadian markets, only channels 1~11 are available. You cannot select other channels. This device and its antennas must not be co-located or operated in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures. This device operates in the ~2.4GHz frequency range. It is restricted to indoor environments only.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. For products available in the US and Canadian markets, only channels 1~11 are available. You cannot select other channels. This device and its antennas must not be co-located or operated in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures. This device may automatically discontinue transmission if there is no information to transmit, or an operational failure. Note that this is not intended to prohibit the transmission of control or signalling information or the use of repetitive codes where required by the technology. To reduce potential for harmful interference to co-channel mobile satellite systems, this device operates in the 5150-5250 MHz band, and is for indoor use only.

11 EU Declaration of Conformity

Product Types:
Brigade Mobile Digital Recorder MDR-504GW-500, MDR-504GW-XXXX(XXX), MDR-504G-XXXX(XXX), MDR-504W-XXXX(XXX), MDR-504-XXXX(XXX), MDR-508GW-500, MDR-508GW-XXXX(XXX), MDR-508G-XXXX(XXX), MDR-508W-XXXX(XXX) and MDR-508-XXXX(XXX)

Manufacturer:
Brigade House, The Mills, Station Road, South Darenth, DA4 9BD, UK

This declaration of conformity is issued under the sole responsibility of Brigade Electronics.

Objects of the declaration:
Mobile Digital Recorder System with GPS, Wi-Fi and 4G connectivity, including accessories and cables.

The objects of the declaration described above are in conformity with the relevant Union harmonisation legislation:
Directive 2014/53/EU

Relevant Harmonised Standards:
4G
- EN 301 489-1 V2.2.0 and EN 301-489-52 V1.1.0
- EN 301 908-1 V11.1.1; EN 301 908-2 V11.1.1; EN 301 908-13 V11.1.1 and EN 301 511 V12.5.1

Wi-Fi
- EN 301 489-1 V2.2.0 and EN 301 489-17 V3.2.0
- EN 300 328 V2.1.1

GPS
- EN 301 489-1 V2.2.0 and EN 301 489-19 V2.1.0
- EN 303 413 V1.1.1

Additional information:
4G
- Operational Frequency Band: LTE: 1,3,7,8,20; WCDMA: 900/2100MHz; GSM: 900/1800MHz
- Maximum Transmitted Power: 23.5 dBm EIRP

Wi-Fi
- Operational Frequency Band: 2412 - 2472 MHz
- Maximum Transmitted Power: 15.82 dBm EIRP

The above equipment should be installed and operated with a minimum distance of 20cm between the mobile digital recorder and any human body.

Signed for and on behalf of Brigade Electronics Group PLC
11/10/2017, South Darenth, DA4 9BD, UK
David Wallin, Quality and Standards Manager

12 Glossary

3G – Third Generation Mobile Network
4G – Fourth Generation Mobile Network
AC – Adaptor Cable
ADPCM – Adaptive Differential Pulse-code Modulation
APN – Access Point Name
AVI – Audio Video Interleaved
BD – Blind Detection
CBR – Constant Bit Rate
CE – Conformité Européenne
CH – Channel
CHAP – Challenge Handshake Authentication Protocol
CIF – Common Intermediate Format (¼ D1 format)
CPU – Central Processing Unit
CU – Control Unit
D1 – D1 is full standard resolution for 25FPS (PAL) and 30FPS (NTSC)
DS – Docking Station
DST – Daylight Saving Time
EDGE – Enhanced Data GSM Environment
EIA – Electronic Industries Alliance
EXP – Expansion
FCC – Federal Communications Commission
FPB – Fireproof box
GB – Gigabyte
GHz – Gigahertz
GND – Ground
GPIO – General Purpose Input/output
GPRS – General Packet Radio Service
GPS – Global Positioning System
GSC – G-sensor Cable
G-Sensor - measure of acceleration/shock of the vehicle
GSM – Global System for Mobile Communications
GUI - Graphical user interfaces
H.264 – Video compression standard
HD1 – Half Definition compared to Full Definition (See D1)
HDD – Hard Disk Drive
HSDPA – High Speed Downlink Packet Access
HSPA – High Speed Packet Access
HSUPA – High Speed Uplink Packet Access
IC – Industry Canada
ID – Identification
IO – Input/output
iOS – i Operating System
IP – Internet Protocol
IR – Infra-red
IT – Information technology
Km/h – Kilometres per hour
LAN – Local Area Network
LED – Light Emitting Diode
MAC – Media Access Control
MB – Megabyte
MCU – Mobile Caddy Unit
MD – Motion Detection
MDR – Mobile Digital Recorder
MHz – Megahertz
MPH – Miles per hour
NET – Network
NTSC – National Television System Committee
OSD – On-screen Display
PAL – Phase Alternating Line
PAP – Password Authentication Protocol
PC – Personal Computer
PN – Part Number
PTZ – Pan, Tilt and Zoom
PWR – Power
REC – Record
RES – Resolution
RP – Remote Panel
RPC – Remote Panel Cable
S/N – Serial Number
SD – Secure Digital
SIM – Subscriber Identity Module
SMA – Sub Miniature Version A connector
SMTP – Simple Mail Transfer Protocol
SPD – Speed
SQL – Structured Query Language
SSL – Secure Sockets Layer
TB – Terabyte
TIA – Telecommunications Industry Association
TRIG – Trigger
UNECE – United Nations Economic Commission for Europe
UPS – Uninterruptable Power Supply
USB – Universal Serial Bus
V – Voltage
VBR – Variable Bit Rate
VGA – Video Graphics Array
VIC – Video Input Cable
VL – Video Loss
VOC – Video Output Cable
W – Watt, standard unit of power
WCDMA – Wide Code Division Multiple Access
Wi-Fi – Wireless Fidelity

13 Disclaimer

Mobile digital recorder systems are an invaluable driver aid but do not exempt the driver from taking every normal precaution when conducting a manoeuvre. No liability arising out of the use or failure of the product can in any way be attached to Brigade or to the distributor.

Dénégation
Les enregistreurs numériques portables sont une aide précieuse pour le conducteur, mais celui- ci doit toutefois prendre toutes les précautions nécessaires pendant les manœuvres. Brigade ou ses distributeurs n'assument aucune responsabilité résultant de l'utilisation ou d'un défaut du produit.

Haftungsausschluss
Mobile Datenaufzeichnung Systeme sind für den Fahrer eine unschätzbare Hilfe, ersetzen aber beim Manövrieren keinesfalls die üblichen Vorsichtsmaßnahmen. Für Schäden aufgrund der Verwendung oder eines Defekts dieses Produkts übernehmen Brigade oder der Vertriebshändler keinerlei Haftung.

Condizioni di Utilizzo
I sistemi di registrazione digitale mobile costituiscono un prezioso ausilio alla guida, ma il conducente deve comunque assicurarsi di prendere tutte le normali precauzioni quando esegue una manovra. Né Brigade né il suo distributore saranno responsabili per eventuali danni di qualsiasi natura causati dall'utilizzo o dal mancato utilizzo del prodotto.

Aviso legal
Sistemas móviles grabadora digital son una ayuda inestimable driver pero no exime al conductor de tomar todas las precauciones normales al realizar una maniobra. Ninguna responsabilidad que surja del uso o fallo del producto puede de alguna manera acoplarse a la brigada o al distribuidor.

Declinación de responsabilidad
Celular gravador digital de sistemas são uma inestimável driver de auxílio, mas não isentam o driver de tomar todas normal precaução ao realizar uma manobra. Nenhuma responsabilidade decorrente da utilização ou falha do produto pode de qualquer maneira ser anexado ao de bombeiros ou para o distribuidor.

Verwerping
Mobiele digitale recorder systemen zijn een waardevolle hulp voor de bestuurder, maar stelt de bestuurder niet vrij van de normale voorzorgsmaatregelen bij het uitvoeren van een manoeuvre. Geen aansprakelijkheid voortvloeiend uit het gebruik of falen van het product kan op één of andere manier aan Brigade of aan de distributeur worden toegekend.

Отказ от обязательств
Системы видеорегистрации оказывают водителю неоценимую помощь при маневрировании, но не освобождают его от обязанности соблюдения обычных мер предосторожности. В ином случае компания Brigade или дистрибьютор не несет ответственность, возникающую в ходе использования или по причине неисправности данного продукта.

Hatırlatma
Mobil Sayısal Kayıt Cihazları sürücünün önemli bir yardımcısı olmakla birlikte, manevra esnasında sürücü bir kaza olmaması için her türlü önlemi almalıdır.Brigade veya bölgesel dağıtıcıları yapılacak yanlış bir uygulama ve sonucunda oluşabilecek maddi ve/veya manevi kayıplardan sorumlu tutulamaz.

Uwaga
Systemy mobilnych cyfrowych rejestratorów są niezastąpioną pomocą dla kierowcy, ale jego posiadanie nie zwalnia kierowcy z zachowania szczególnej ostrożności podczas manewrów. Żadna kolizja drogowa ani jej skutki nie mogą obciążać producenta urządzenia oraz jego dystrybutorów.

Specifications subject to change. Sous réserve de modifications techniques. Änderungen der technischen Daten vorbehalten. Specifiche soggette a variazioni. Las especificaciones están sujetas a cambios. Wijzigingen in specificaties voorbehouden. As especificações estão sujeitas a alterações. Спецификация может изменяться. Brigade Electronics belirttiği özellikleri haber vermeksizin istediği zaman değiştirebilir. Specyfikacja techniczna może ulec zmianie.