MDR 600 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 600 Series Technology

Brigade's MDR-641 Series and MDR-644 Series are advanced Mobile Digital Recorders (MDRs) designed to record and playback 4+1 or 4+4 channels.

Brigade's DC-204-AI Series is an AI Connected Dashcam, designed to record and playback various channels. The AI connected Dashcam has two built in channels; The road facing 'Advance Driving Assistance System' (ADAS) camera and the driver facing 'Driver Safety Cockpit' (DSC) camera.

All systems use 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, FULL HD/1080p or 1920p). 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 logged in the MDR Software (MDR-Dashboard 6.0 and MDR-Player 6.0). This information is referred to as 'Metadata'.

Recordings can be searched, viewed and downloaded (clipped and saved locally) using the MDR-Dashboard 6.0 software. This allows you to access all the vehicle's travel information, including route tracking. Recordings can be downloaded in three different ways: as an audio/video MP4 file, playable by consumer media players, as native proprietary format clips or as a password protected .exe file with an embedded MDR-Player 6.0.

The Mobile network and Wi-Fi settings found in this manual relate to the wireless features of the MDR-600 series that either come standard on selected models or can be purchased as a 4G/Wi-Fi upgrade module.

Mobile network and Wi-Fi settings for DC-204-AI can be found in *DC-204-AI Series Installation & Operation Guide – ENG*.

It is recommended that Brigade products are installed and commissioned by approved professionals. It is the installers responsibility that the installation and setup have been carried out correctly, adhering to relevant regulations and legislation.

Warning: Prior to attempting the system setup, please ensure the MDR 600 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.

Table 1: Software for MDR 600 Series Products:

WINDOWS PC SOFTWARE	MOBILE PHONE APPS
(1) MDR-Dashboard 6.0	(1) Brigade MDR 6.0 (Android)
(2) MDR-Player 6.0	(2) Brigade MDR 6.0 (iOS)
(3) MDR Server 6.0	

1.1 Product Features

Table 2: Differences between MDR-641XX-X-XXX(XX), MDR-644XX-X-XXX(XX) and DC-204-AI(XXXX)

MDR-641XX-X-XXX(XX)	MDR-644XX-X-XXX(XX)
500GB / 1TB / 2TB HDD or SSD with anti-vibration mounts (2TB maximum)	500GB / 1TB / 2TB HDD or SSD with anti-vibration mounts (2TB maximum)
SD Card not supported	Industrial grade 64GB (256GB maximum) internal SD card for mirror, sub-stream and alarm recording
Simultaneous 5 channel recording up to Analogue: 1080P @ 11fps (PAL) / (NTSC) for 4 channels IP (direct connection only): 1080P @30fps for 1 channel	Simultaneous 8 channel recording up to: Analogue: 1080P @ 11fps (PAL) / (NTSC) for 4 channels IP (direct connection only): 1080P @30fps for 4 channels IP (with direct connection and an extra 4-Port PON Switch) 1080P @ 30fps for 8 channels
5x Select video connectors typical to camera inputs with audio	8x Select video connectors typical to camera inputs with audio
Packed Weight: 2.9Kg	Packed Weight: 3.8Kg

DC-204-AI(XXXX)
2x 128GB Micro-SD card (256GB maximum each, 512GB maximum in total)
2 channels for built-in ADAS and DSC camera recording up to 1920P @ 25 / 30fps (PAL) / (NTSC) 1080P @ 25 / 30fps (PAL) / (NTSC) Extra 1x AHD channel and 1x IPC channel (requires transfer cable): 1080P @ 25fps for AHD channel 1080P @ 30fps for IP camera channel
Packed Weight: 0.73Kg

2 MDR Server Software Requirements and Installation

MDR Server 6.0 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 Licence** and **Authentication**. When the **Yearly License** is nearing the expiration date (1st Dec every year), please visit Brigade's website (www.brigade-electronics.com) to download the new license file. This file needs to be copied onto the Windows Server running the MDR Server 6.0 Software. Copy this file to the following path **C:\Program Files (x86)\MDR Server\TransmitServer** and overwrite the existing version. For **Authentication**, please contact Brigade support to obtain available auth file. Without an auth file, the server provides 1 month trial with 20 vehicle connectivity in maximum.

2.1 MDR Server Software Requirements

To use the mobile network and Wi-Fi connectivity features, networking expertise are recommended for implementation. The mobile network server is accessed by the device externally through a public IP (Internet Protocol) address. The Wi-Fi server is accessed by the device using a Wi-Fi network. This setup requires all parts (Server, Client and device) to be connected to a shared network. 'Client' refers to MDR-Dashboard 6.0 or BRIGADE MDR 6.0 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: Video and Metadata are only stored on the server they are linked to. These cannot be shared across multiple servers

Table 3: The minimum requirements below for the MDR Server 6.0 Software with 1-10 MDR units

COMPONENT	RECOMMENDED REQUIREMENTS
CPU (Central Processing Unit)	8 Core/16 Threads or greater
RAM (Random Access Memory)	12GB or greater
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 2016 Standard or greater
Framework	Microsoft .Net Framework v3.5 SP1 version must be installed on both server and client**

**'Client' refers MDR-Dashboard 6.0 software

Table 4: The recommended requirements below are for the MDR Server 6.0 with >10 MDR units <100

COMPONENT	RECOMMENDED REQUIREMENTS
CPU (Central Processing Unit)	8 Core/16 Threads or greater
RAM (Random Access Memory)	16GB
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 2019 Standard or greater
Framework	Microsoft .Net Framework v3.5 SP1 version must be installed on both server and client**

**Client refers MDR-Dashboard 6.0 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.

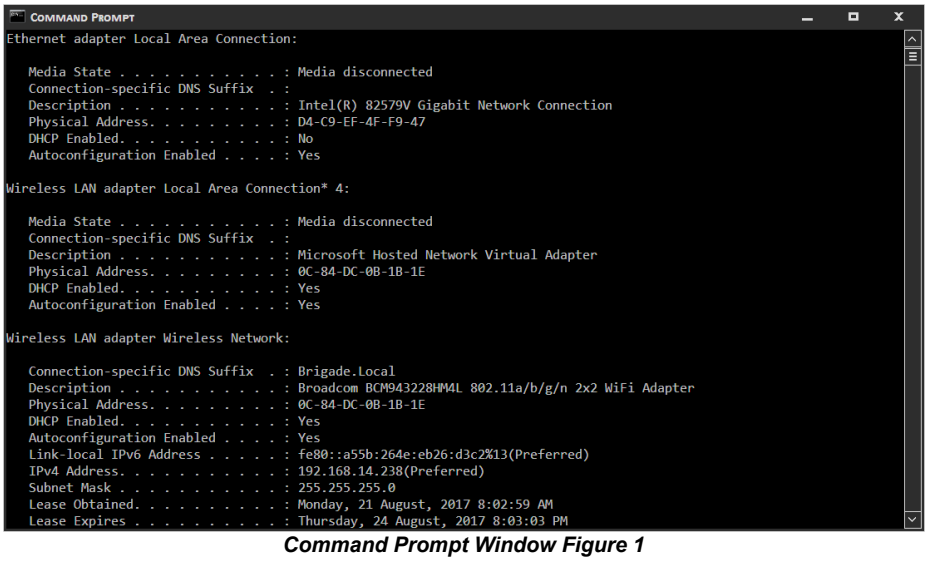
2.2 MDR Server Installation

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 5: Port Forwards List and Services List

Port Forwards List					
#	**PORT NAME**	**PORT NUMBER (HTTP)**	**PORT NUMBER (HTTPS)**	**PORT FUNCTION (CLIENT REFERS TO MDR-DASHBOARD 6.0 / BRIGADE MDR 6.0 APP)**	**CORRESPONDING PROCESS**
(1)	FileZilla Server	21; 3001~3100;		For FTP server, retrieve related configurations when remote upgrade is used.	FileZilla server.exe
(2)	WCMS5REACT	3113	23113	For Evidence Centre playback	node.exe
(3)	Message Service	5556	6556	Device registration will be used when uploading a device to the server and issue commands from the server	MessagerServer.exe
(4)	Client Balance	7264	8264	Balance the load for clustering servers - (for future clustering of servers) – specify this port when logging in – creates initial connection. Has login authentication and return IP address and ports to client.	ServiceProxy.exe
(5)	NgnixBroker	8081	28081	1. Nginx proxy service, proxy N9M2.0 remote setting resources 2. HTTPS protocol proxy	NgnixBroker.exe
		12040	22040		
		12055	22055		
(6)	Client Access Service	12020	22020	Transfer request from client and return message (online/offline status, real-time GPS and others) from server	ClientAccessService.exe
(7)	Server playback service	12045	22045	For server playback function	ServiceSTPlay.exe
(8)	HttpSdkService	12047	22047	Https SDK	HttpSdkService.exe
(9)	EvidenceStoreService	12048	22048	File storage service, N9M2.0 (Gen 2) evidence data, N9M2.0 (Gen 2) remote setting web resources	EvidenceStoreService.exe
(10)	Proxy Server (Remote Setting) Client Data	12050	22050	For the remote config (within MDR-Dashboard 6.0) feature via TLS connection– from Server to Client	HttpProxyServerNP.exe
(11)	Proxy Server (Remote Setting) Device Data	12051	22051	For the remote config (within MDR-Dashboard 6.0) feature via TLS connection– from device to Server	HttpProxyServerNP.exe
(12)	Proxy Server (Remote Setting) Client Data	12052	22052	For the remote config (within MDR-Dashboard 6.0) feature via non-TLS connection– from Server to Client	HttpProxyServerNP.exe
(13)	Proxy Server (Remote Setting) Device Data	12053		For the remote config (within MDR-Dashboard 6.0) feature via non-TLS connection – from device to Server	HttpProxyServerNP.exe
(14)	WCMS5	12056	22056	For supporting web service.	node.exe
(15)	Media Server	8090	28090	For the live view and playback function on the web client.	media_service.exe
		8091	28091		
		12060	22060		
		12061	22061		
		12062	22062		
		12063	22063		
		12198~12203			
(16)	Evidence Service	12065	22065	Upload evidence from MDR, handle evidence, and any other feature related to evidence centre.	EvidenceService.exe
(17)	MDR4 Streaming Media Server	12091		Video streaming data transmission for MDR 400 Series. To retrieve video streaming from MDR and dispatch to client after receiving the live view request from the client.	DVRGTService.exe
(18)	MDR5 Streaming Media Server	12092	22092	Video streaming data transmission for MDR 500 Series. To retrieve video streaming from MDR and dispatch to client after receiving the live view request from the client.	DVRGTService.exe
(19)	Transmit Server	17891	27891	Video streaming data transmission for Clients. To retrieve video streaming from TLS connected devices and dispatch to client after receiving the live view request from client.	DVRGTService.exe
(20)	Transmit Server	17892	27892	Video streaming data transmission for Clients. To retrieve video streaming from non-TLS connected devices and dispatch to client after receiving the live view request from client.	DVRGTService.exe
(21)	GTBalance	12075	22075	Scales video delivery by distributing streaming load across multiple server processes.	GTBalance.exe
(22)	DVRGTService2	12093		Video streaming data transmission. To retrieve video streaming from non-TLS devices and dispatch to client after receiving the live view request from client.	DVRGTService2.exe
		12094			
Additional Services List (Does not require Port Forwarding)					
(1)	MySql5.5	3307		To store basic data	MySql5.5.exe
(2)	Client Access Service	9528		Transfer request from client and return message (online/offline status, real-time GPS and others) from server	ClientAccessService.exe
(3)	AdsServer	7857~7861		For auto-download function.	ADSServer.exe
(4)	DVRGTService	10001		Video streaming data transmission. To retrieve video streaming from devices and dispatch to client after receiving the live view request from client.	DVRGTService.exe
(5)	CenterManageService	12000		For internal process message management	ServiceDAMgr.exe
		12003			
(6)	Redis Service	12004		Cache online status, GPS, alarm and other data	redis-server.exe
(7)	Message Service	12012		Alarms push from MessageService to AlarmService	MessagerServer.exe
(8)	OnlineServer	12035		For online statistics service. Collect devices online information.	ServiceOLStatistivs.exe
(9)	ARMSRestServer	12044		Read black box data from MonggoDB	ARMS.RestServer.exe
(10)	BaseDataServer	12046		Java basic data query	BaseDataServer.exe
(11)	FileManagementService	12049		File storage service, and determine file storage path	FileManagementService.exe
(12)	IIS	12054		Evidence upload, server playback picture query, devices automatic adding interface	System
(13)	Alarm Service	12125		Push real-time alarm and GPS to ClientAccessService	AlarmService.exe
(14)	FileZilla Server	14147		For FTP server, retrieve related configurations when remote upgrade is used.	FileZilla server.exe
(15)	N/A	20000		For MDR server control tool	DVRServerCtrl.exe
(16)	Monggodb	27017		To store user's old meta data	mongod.exe
(17)	Monggodb_3.2	27018		To store metadata	mongod.exe
(18)	WCMSRunning	54321		For devices upgrade	WCMS.Running.exe
(19)	HttpSdkService	65531		Https SDK	HttpSdkService.exe

(20)	ARMStorageServer	N/A	For parsing metadata and writing into MongoDB.	ARMS.StorageServer.exe
(21)	DVRRTService	N/A	MDR-Dashboard guard service. To switch on/off services, and reboot services automatically after suspension.	DVRRTService.exe
(22)	PushService	N/A	For APP alarm push function	PushService.exe
(23)	CmdServer	N/A	Panic Button alarm configuration strategy command issuance, and configuration is obtained from the database regularly and issuance	CmdServer.exe
(24)	CommandDispatch	N/A	Instruct issued service	CommandDispatch.exe
(25)	EvidenceCmdServer (EvidenceReportService)	N/A	Strategy service, N9M2.0 evidence upload	EvidenceReportService.exe
(26)	EvidenceAnalyService	N/A	Evidence analysis service, transcoding evidence video data, generating relevant evidence files	EvidenceAnalyService.exe
(27)	TaskPlanService	N/A	Scheduled task service, regularly delete evidence black box, video data	TaskPlanService.exe
(28)	WCMSWebCenterService	N/A	For remote upgrade function and upload devices automatically	WCMS.Server.WindowsService.exe

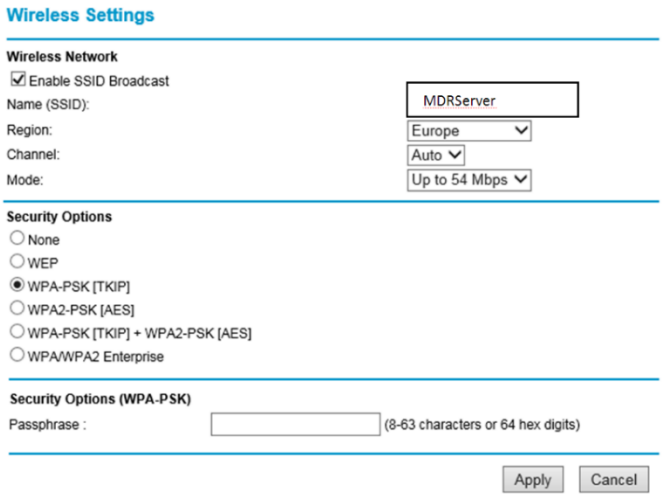
Note: Ports can differ depending on if the HTTPS method is chosen or not.

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. Devices are compatible with **WPA/WPA2-PSK**, **WPA2_Enterprise** or **WEP** encryption.

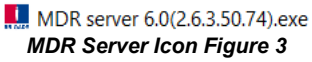
Wi-Fi: *Wireless Router Settings Figure 2* shows an example of a wireless network created. The **SSID** (Service Set Identifier) is **MDRServer** and **WPA-PSK** security has been used. Please be advised, the SSID is case sensitive. SSIDs should be created without spaces.

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 6.0 on the same Windows Server.

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

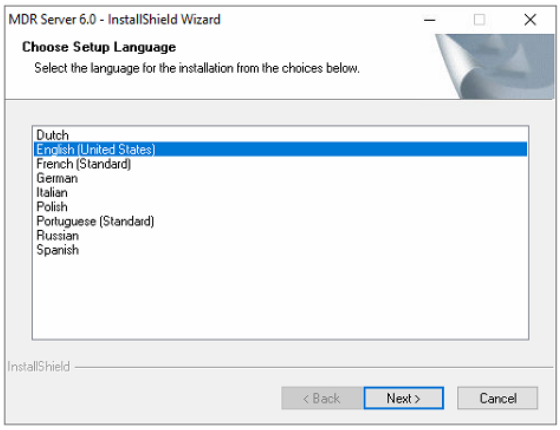
Right-click the installation file found in *MDR Server Icon Figure 3* and **RUN AS ADMINISTRATOR**. You may be prompted to back up any data if there is previously installed MDR Server software on this Windows Server.

Choose the language for the software, as shown in *MDR Server Language Setup Figure 4*. Give the software a few minutes to prepare the setup.

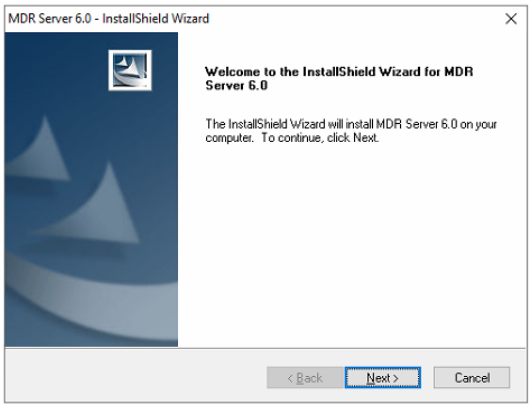
Warning: The same language used for the server software installation must be used for the client software.

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

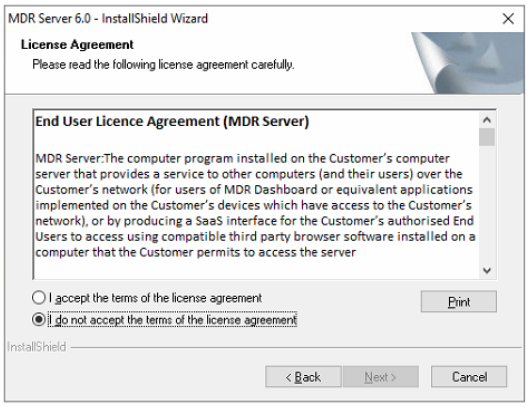
By default, the MDR Server will be installed in *C:\Program Files (x86)\MDR Server 6.0* path, and cannot be customised.



MDR Server Language Setup Figure 4



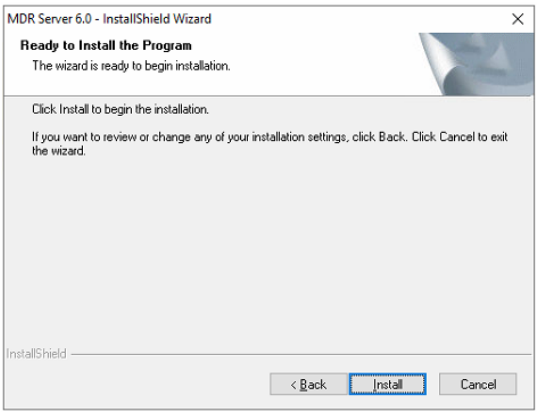
MDR Server Installation Figure 5



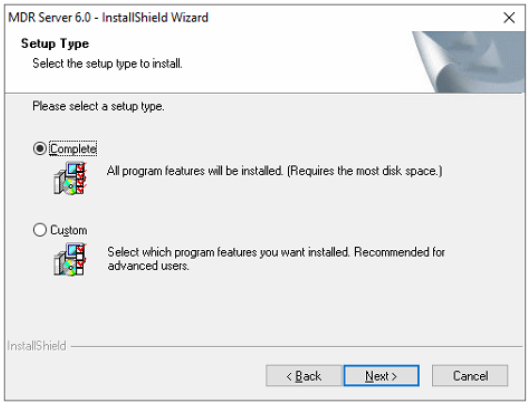
MDR Server Declaration Figure 6

The next step is to select the MDR Server features. *MDR Server Install Folder 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.

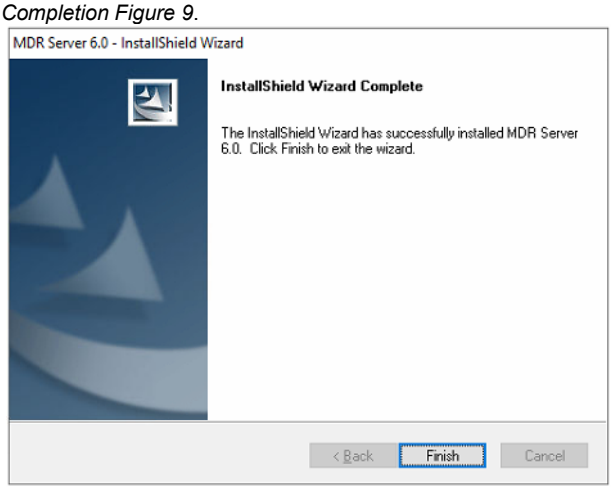


MDR Server Install Folder Setup Figure 8

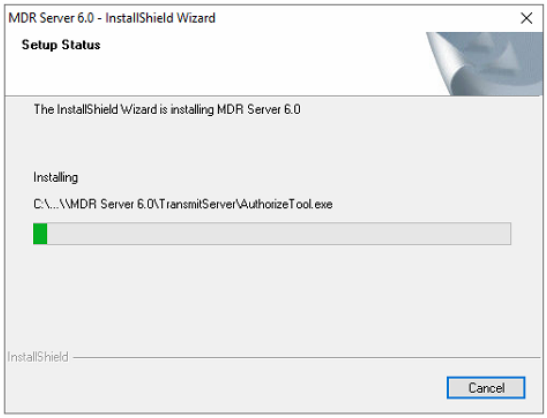


MDR Server Install Mode Figure 7

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.
Click **FINISH** to complete the final step of the installation. See *MDR Server Install Completion Figure 9*.



MDR Server Install Completion Figure 9



MDR Server Setup Status Figure 10

2.3 MDR Server Configuration

2.3.1 Port Configuration Tool

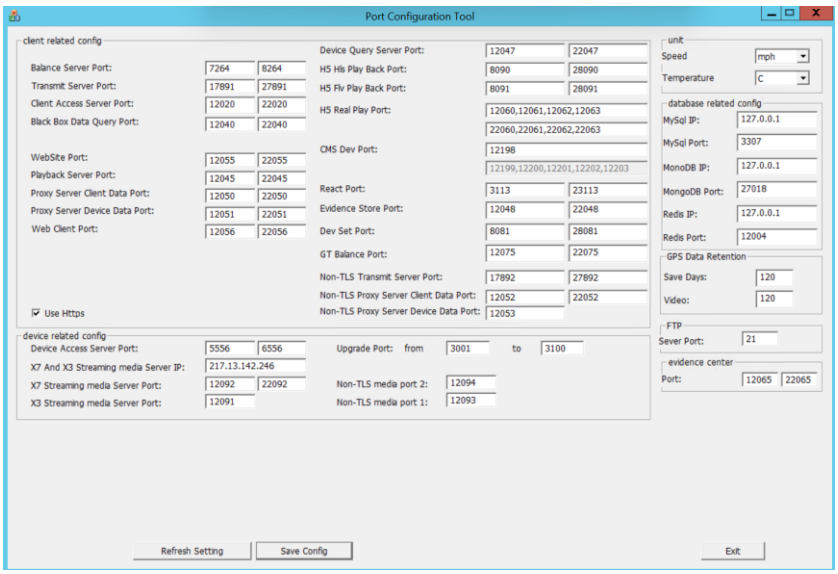
After installing MDR Server, the port configuration tool will be automatically opened, which is used mainly to manage an MDR Server's ports and IP address.

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: Streaming Media Server IP MUST be a STATIC PUBLIC IP address of the Mobile Network Server (Firewall in some cases).

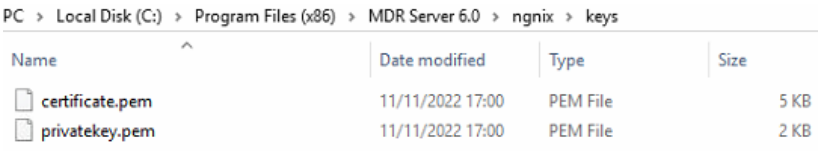
HTTPS is enabled by default for communication encryption. User can disable it by ticking the option "Use Https". HTTPS requires ports change, please refer to above port forward and service table.

Note: Brigade does not provide HTTPS certificate, which must be applied by individual user because it is bound to dedicated server domain names.



Port Configuration Tool Figure 11

After obtaining a HTTPS certificate, rename the Keys following the rules below:
Public key of SSL certificate: certificate.pem
Private key of SSL certificate: privatekey.pem
Put both keys to folder: C:\Program Files (x86)\MDR Server\ngnix\keys.
Then restart the WCMS5 Service to make it effective.



HTTPS Keys Figure 12

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 any other software.

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

Video data including Evidence upload and Auto-Download records can be retained for a defined period, ranging from 0 ~ 1000 (days). If data exceeds the time set, then the oldest files will be erased automatically. If the retaining period is set to 0 then the recordings will be saved for an unlimited amount of time.

2.3.2 Server Control

After installing the MDR Server software, the Server Control program should automatically start. If not then go to the **MDR SERVER** folder as shown in *MDR Server Menu Figure 13*.

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 16*.

Now, click the **OPEN/HIDE WINDOW** option as shown in *Accessing MDR Server Control Window Figure 14*.

It is recommended to **RUN AS ADMINISTRATOR** to ensure the correct opening and full functionality of the software, as shown in *MDR Server Control Menu Figure 19*.

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

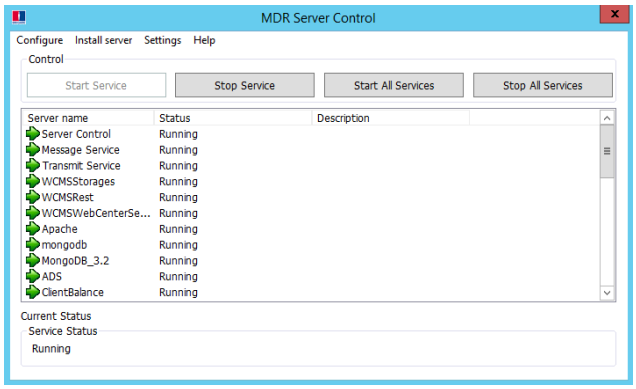
- Right-click MDR Server (*MDR Server Right click menu Figure 15*) then click **Properties**.
- Go to the **Compatibility** tab, under **Privilege Level**, tick **Run this program as administrator**. See *Privilege Level Figure 17*.

Click **Apply** to ensure all changes are saved.

Once the window opens as shown in *MDR Server Control Window Figure 18*, click **CONFIGURE** then **CONFIGURE MESSAGE SERVER.**

The window shown in *MDR Server Message Server Configuration Figure 20* will be displayed. The following configuration is used:

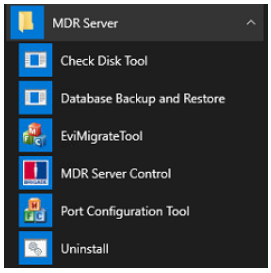
- Server IP: 127.0.0.1 (loopback IP address of server)
- Server Port: 5556



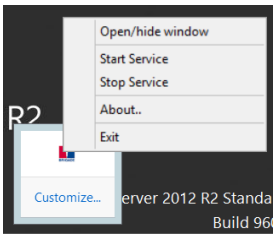
MDR Server Control Window Figure 18

Note: If not all the MDR Server services are running (*MDR Server Control Window Figure 18*). Please follow the following steps to attempt to fix the issue:

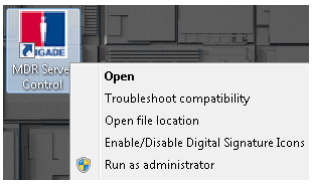
- Exit the MDR Server control window and run the application as administrator. See *MDR Server Control Menu Figure 19*.
- Ensure that the MDR Server installation is not expired – check Brigade website for the latest license files.
- Install the Microsoft .NET Framework 3.5.
- Check the MDR Server IP in *MDR Server Message Server Configuration Figure 20*. Click **SAVE** on the configuration of the Message Server window.



MDR Server Menu Figure 13

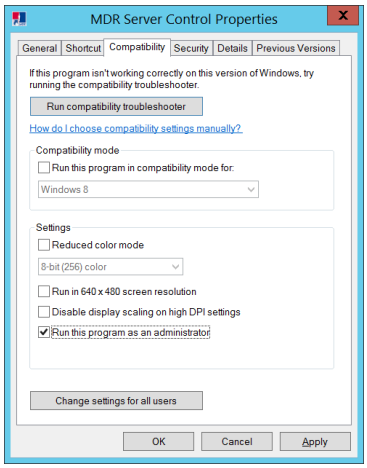


Accessing MDR Server Control Window Figure 14

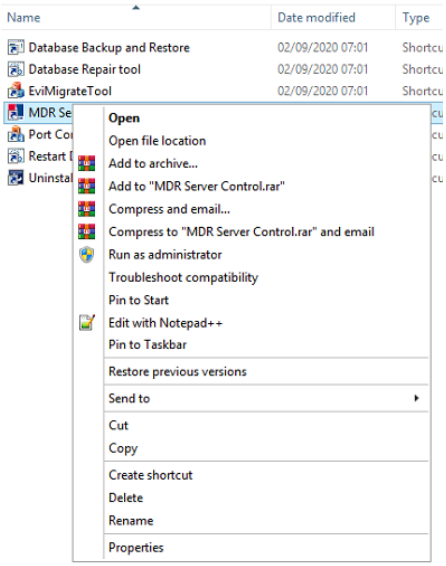


MDR Server Right click menu Figure 15

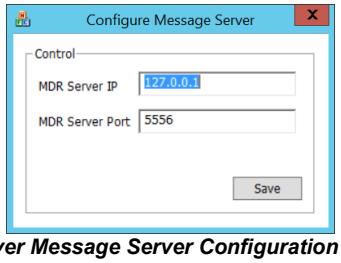
Displaying MDR Server Control Figure 16



Privilege Level Figure 17



MDR Server Control Menu Figure 19



MDR Server Message Server Configuration Figure 20

- Restart the Windows Server.
- If none of the above solve the issue, please reinstall the software.

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

(1) Server Control: manages all services. (This can be set to restart daily via the settings)	(2) Message Service: Creates a TCP connection from the server to an MDR. It manages client software logins states and registers the device state. It also manages transport commands from the server to devices and write GPS/alarm data into mongodb using the MDR5 protocol.
(3) Transmit Service: forwards media data from devices to client software using transmit port.	(4) WCMSWebCenterService: supports MDR-Dashboard 6.0 remote firmware batch upgrades.
(5) Apache: Invoke page action via web services, such as evidence centre, ADS etc.,	(6) Mongodb: Mongo Database service, for storing GPS, alarm data and metadata from MDR 500 (MYSQL used for MDR 400).
(7) Mongodb_3.2: To store black box data	(8) ADS: Auto Download System is used to avoid too many MDR-Dashboard 6.0 connections to one Windows Server.
(9) ClientBalance: If there are multiple MDR Server installations on different servers, the system will distribute client connections evenly across the servers to balance the load.	(10) n9m_proxy: Works as a proxy server to set device parameters remotely.
(11) ARMSStorageSever: Stores metadata (from auto download function) into mongodb.	(12) ARMSRestServer: Analyses metadata file path (from auto downloads) in MYSQL database.
(13) ServiceSTPlay: For MDR-Dashboard 6.0 remote playback server data.	(14) AlarmService: For alarm service program, internal use only.
(15) CommandDispatch: For transmit command	(16) ClientAccessService: For sending device online/offline messages to clients. For MDR-Dashboard 6.0 to receive device online/offline messages. For transporting orders from MDR-Dashboard 6.0 to devices.
(17) Redis Service: Buffers device online/offline information for mobile app queries.	(18) PushService: For pushing alarms to mobile apps.
(19) OnlineServer: Manages device online/offline messages and updates clients with this information.	(20) CmdServer: commands sent to MDR Server.
(21) WCMSRunningService: For supporting MDR-Dashboard 6.0 remote firmware batch upgrades. Adds vehicles automatically to MDR-Dashboard 6.0.	(22) CenterManageService: For updating centre data to related MDR-Dashboard 6.0.
(23) HttpSdkService: For enabling web interface access	(24) EvidenceAnalyService: For analyse and creating evidence items.
(25) FTPServer: Works as FTP server for saving data (video, snapshots, firmware etc.).	(26) WCMS5: For supporting web client.
(27) WCMS5REACT: For supporting web evidence centre playback features	(28) Mysql: Database for storing basic data such as vehicle and fleet information.
(29) EvidenceRcvServer: Receiving and transmitting Evidence files from a server	(30) ServiceSTMgr: Allows the saving of Live View footage to a server.
(31) ServiceSTWorker: Execute the saving Live View footage to a server folder.	(32) rm_media_service: For web client Live View and playback.
(33) EvidenceCmdServer: For managing evidence item uploading.	(34) EvidenceStoreService: For saving evidence items and data.
(35) FileManagementService: For managing different file saves to different paths.	(36) TaskPlanService: Supports deleting GPS data and video data after a configured period of time.
(37) NginxBroker: Reverse proxy for web functionality	(38) BasedataServer: Basic data inquiry (Java)
(39) GTBalance: Queries device TLS status to assign connection ports.	(40) n9m_proxy2: Works as a proxy server to set device parameters remotely for non-TLS device.
(41) DVRGTService2: Video streaming data transmission for non-TLS device.	(42) FcgiServer: For MDR6 device remote configuration.

Double-click on **MESSAGE SERVICE** as shown in *MDR Server Control Window Figure 18*. This will open another window which shows the current state of the network. See *MDR Server Message Logs View Figure 22*.

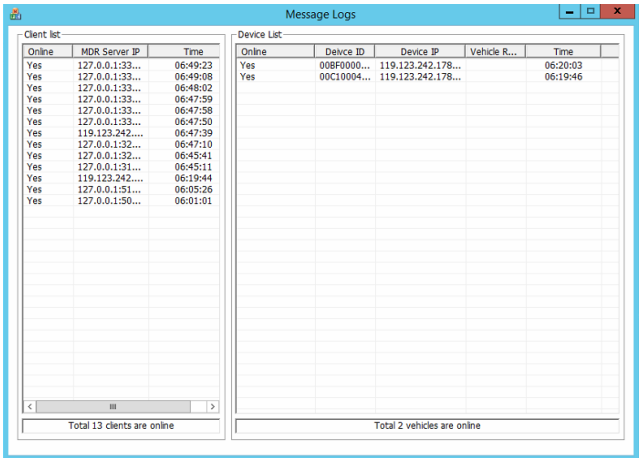
In *MDR Server Message Logs View Figure 22*, the IP addresses of the connected clients are shown in the left column. This includes the server loopback address. If a device has been configured correctly, it will appear online in the right column.

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

MDR Server 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 21*.

The system administrator will need to download a new 1-year license file from Brigade's website. 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 21



MDR Server Message Logs View Figure 22

2.4 Server Authorization

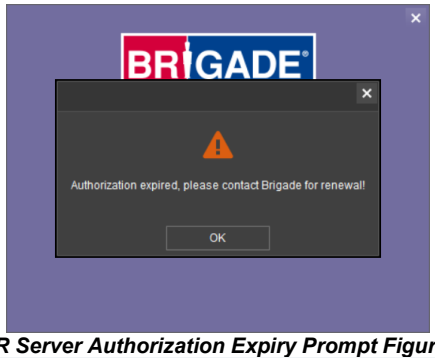
Each MDR Server has a 1-month trial after installed. Within trial period, the server can take 20 vehicles at maximum. If want to prolong the time or increase vehicle connection amount, please contact Brigade for obtaining authorization file.

When the **Authorization** expires, users cannot login to either MDR-Dashboard client or web interface. The login operation will trigger a prompt window to remind the user of current expiration state. See *MDR Server Authorization Expiry Prompt Figure 23*. Clicking on **OK** will open the standalone **Authorization Config** page to give the Machine Code for the next step. See *MDR Server Authorization Config Figure 24*.

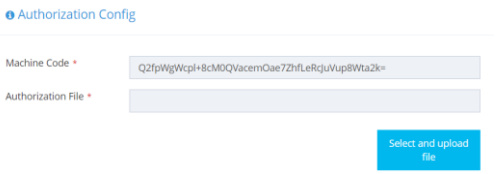
To renew the **Authorization**, please provide the Machine Code to Brigade, the new **Authorization** file will be generated based on it. After obtaining the **Authorization** file, please upload it via the **Select and upload file** button, the renewal process will take effect in 5 mins.

Brigade recommends renewing the **Authorization** before it expires to avoid any inconvenience. The Machine Code can be found on the System configuration page of the Web client, see *Authorization Figure 25*.

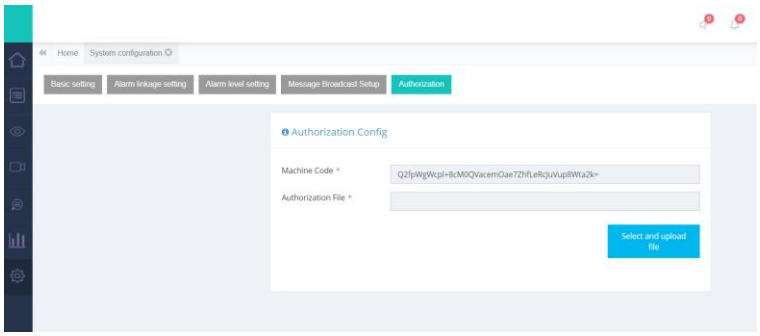
Note: The server still operates and stores device data during the expiration period, but users will be unable to login or use any functions.



MDR Server Authorization Expiry Prompt Figure 23



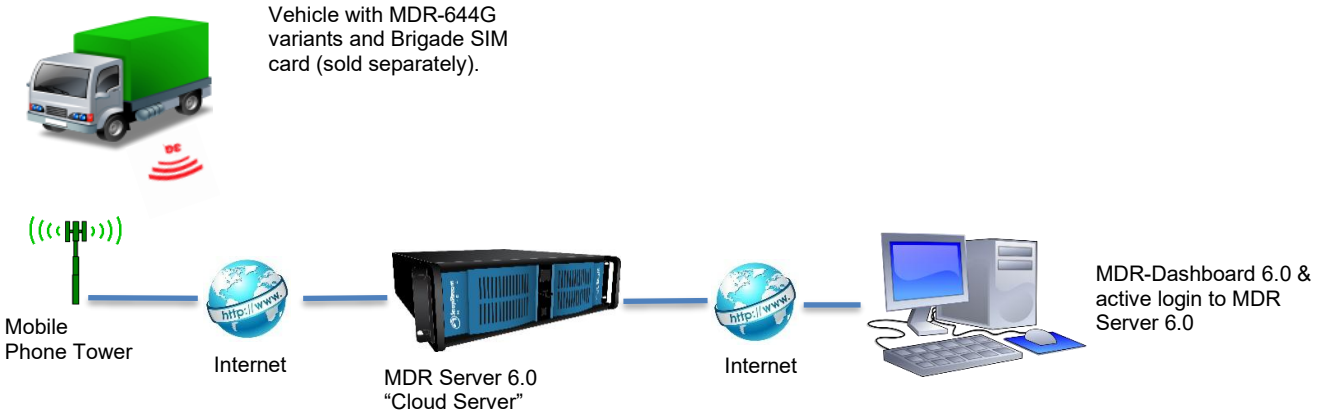
MDR Server Authorization Config Figure 24



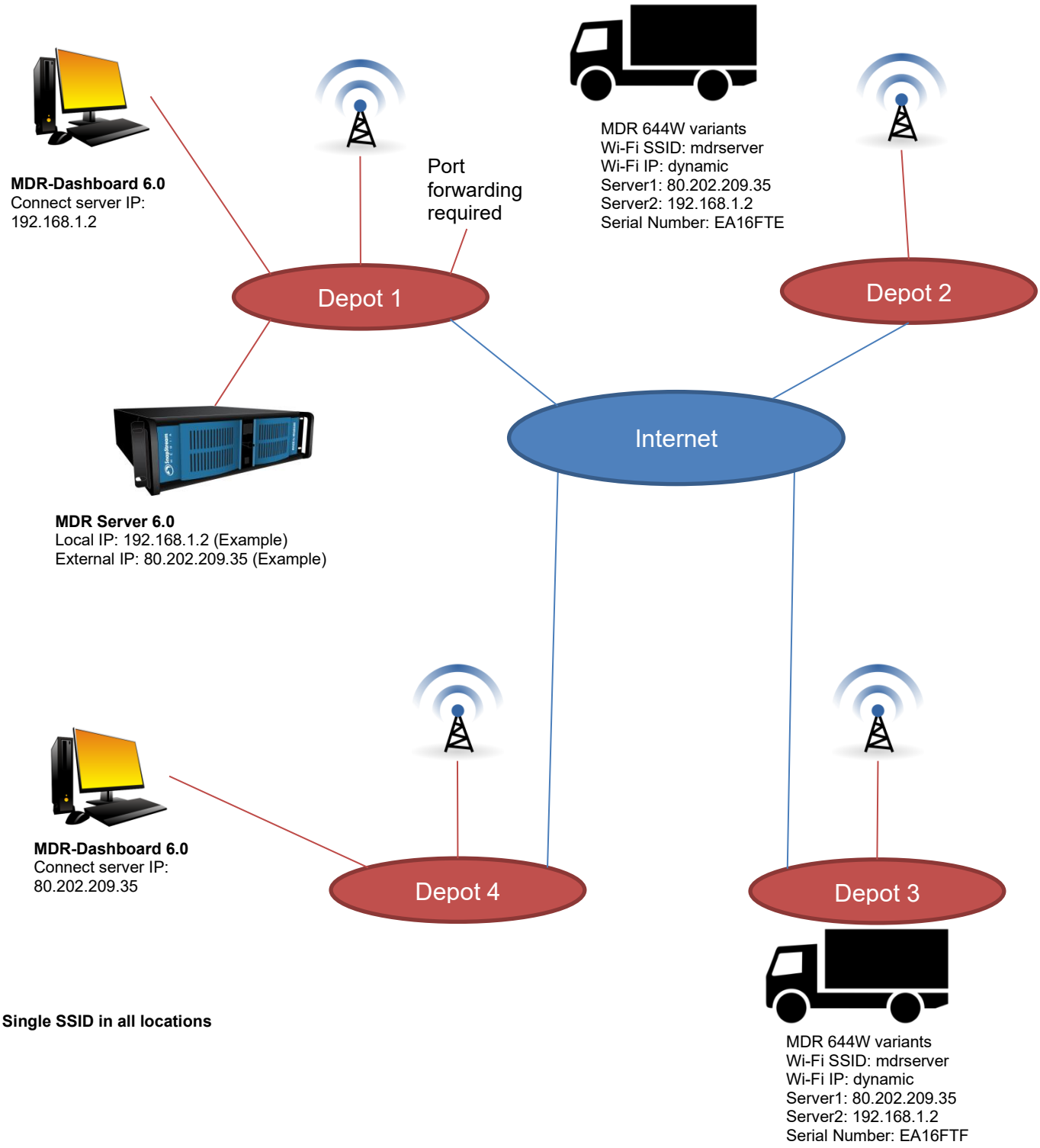
Authorization Figure 25

2.5 Hardware Communication Options

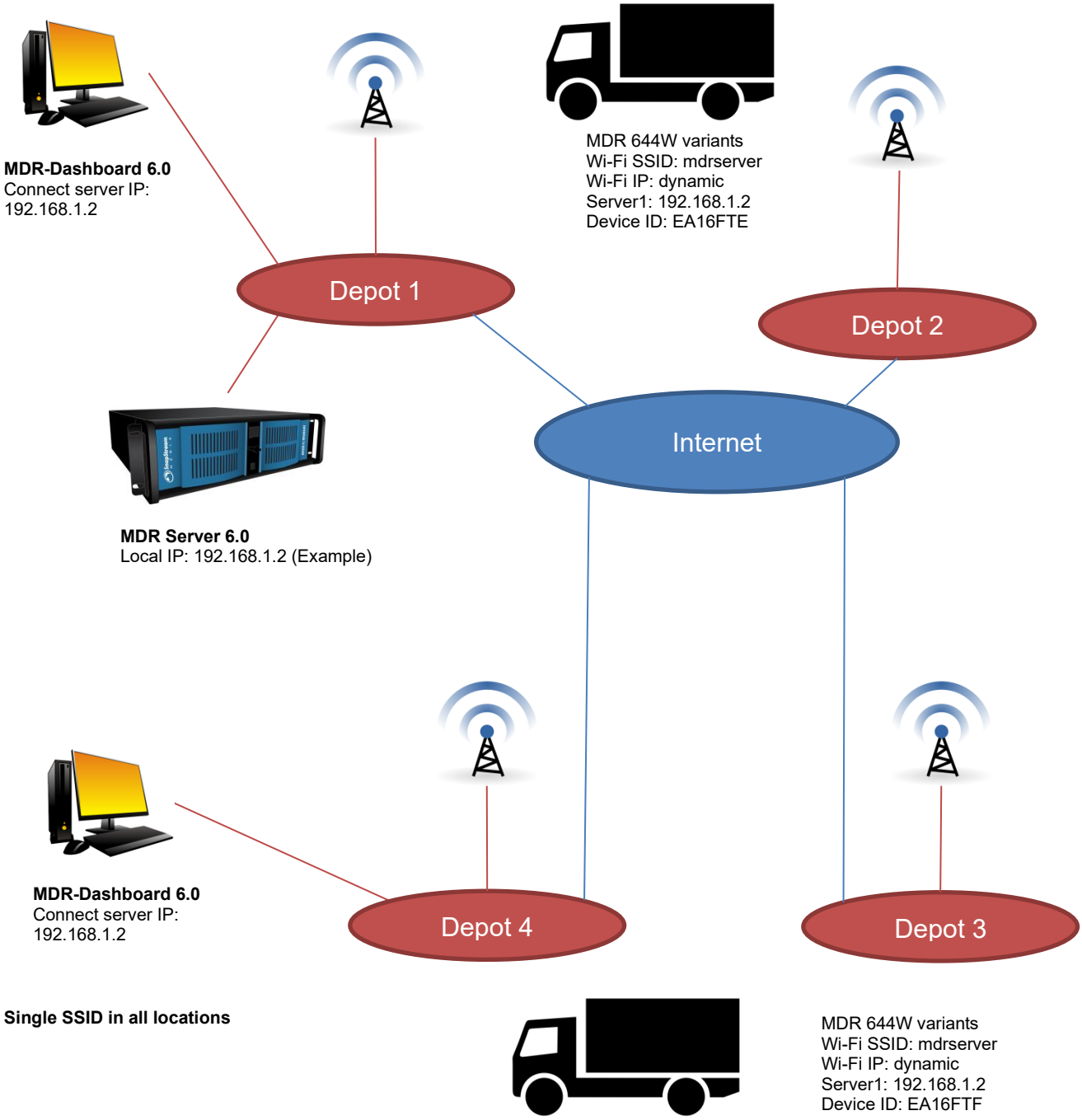
Each hardware device will need its own mobile network enabled sim card. You need to login to MDR-Dashboard 6.0 to view live video, track vehicles in real-time and download video/metadata when required.



Option 1 - Hosted Mobile Network Figure 26



Option 2 – Wi-Fi only, multi depot, without VPN Figure 27



Option 3 - Wi-Fi only, multi depot, with VPN Figure 28

3 MDR-Dashboard 6.0 Requirements & Installation

MDR-Dashboard 6.0 software is used for advanced local playback, analysis, downloading, GPS tracking, vehicle information and events/log display. When a device is out of network range, features that are network dependent will no longer function. MDR-Dashboard 6.0 has the following features:

- Real-time Preview
- Multi Vehicle Monitoring and Tracking
- Playback of MDR Server and Online device 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 Centre
- Statistic Reports
- Online Upgrade (network independent)

Table 6: Differences between MDR-Dashboard 6.0 and MDR-Player 6.0

MDR-DASHBOARD 6.0	MDR-PLAYER 6.0
Installation Required	Executable
Full Featured	Compact – limited features
View and Download Recordings	View Recordings
Sources – MDR Server, HDD/SD, Online devices and Local Files	Sources – Standard and Export Downloads

For more information on MDR-Player 6.0 please refer to **MDR 600 Series Installation&Operation Guide**.

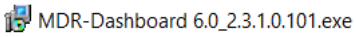
3.1 MDR-Dashboard 6.0 Requirements

Table 7: Minimum requirements for MDR-Dashboard 6.0

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	446 MB
Video	Intel® HD Graphics 5000 or equivalent
Operating System	Windows™ 10 and above
Web browser	Internet Explorer 10
Software	Flash Player (up to date)
Resolution	1440*900

3.2 MDR-Dashboard 6.0 Installation

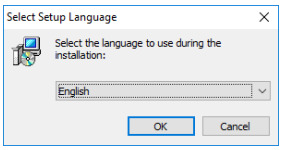
Install MDR-Dashboard 6.0 on the client PC. (Administrator rights are required). Double-click the installation file shown in *MDR-Dashboard Icon Figure 29*.



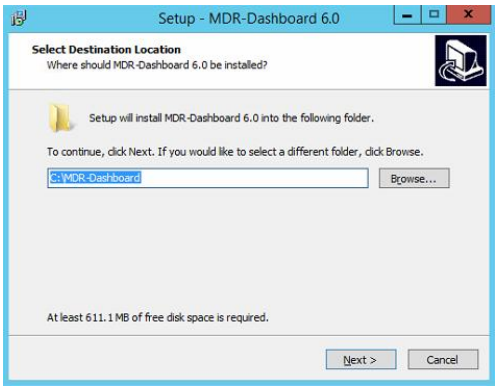
MDR-Dashboard Icon Figure 29

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 31*.

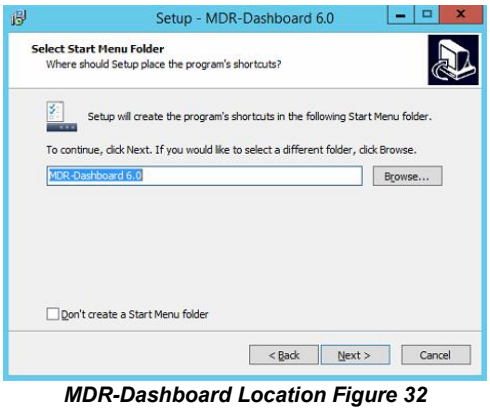
Choose the language for the software, as shown in Language Option Figure 30.You can configure the destination location (if there is not enough free disk space) which is shown in *MDR-Dashboard Location Figure 32*. **It is NOT recommended to change the default location**.



Language Option Figure 30

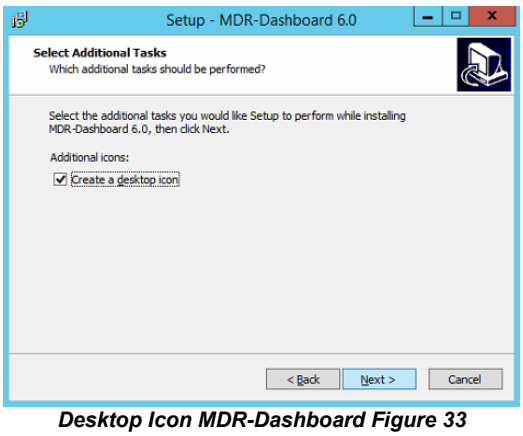


MDR-Dashboard Setup Figure 31



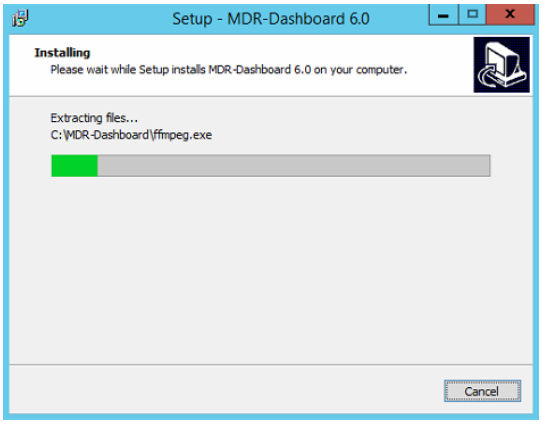
MDR-Dashboard Location Figure 32

Referring to *Desktop Icon MDR-Dashboard Figure 33*, you can choose if a desktop icon is created.



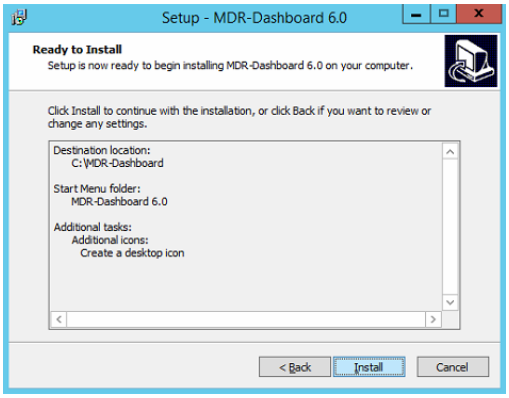
Desktop Icon MDR-Dashboard Figure 33

The progress of the installation is indicated in *MDR-Dashboard Installation Figure 35*.



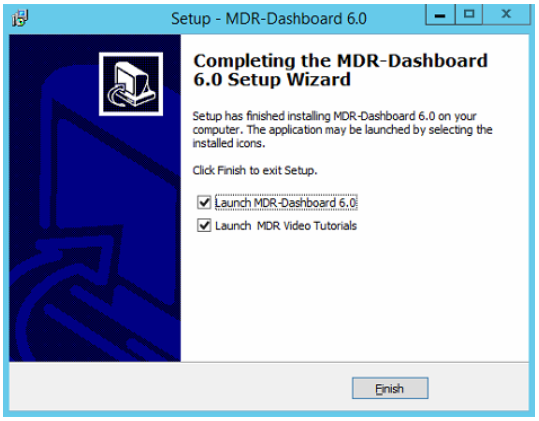
MDR-Dashboard Installation Figure 35

You are prompted to click **INSTALL** to begin the installation. This is indicated in *Install MDR-Dashboard Figure 34*.



Install MDR-Dashboard Figure 34

MDR-Dashboard Launch Step Figure 36 depicts the final step; you may choose to launch the software or open Brigade MDR Video Tutorials web page for further feature information. Tick the box and click **FINISH**.



MDR-Dashboard Launch Step Figure 36

4 Wi-Fi Configuration

MDR Server 6.0 and MDR-Dashboard 6.0 are compatible with various hardware models, such as the MDR 500 Series, MDR 600 Series and AI Dashcam Series. Their configuration follows the same rules and steps. Below steps will use the MDR 600 Series as an example.

4.1 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**.

Brigade recommends changing the default unit password. This must be documented and controlled by the end user.

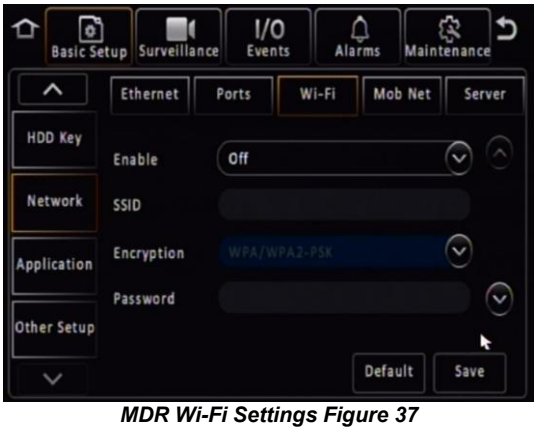
Browse to this Wi-Fi network page using **SETUP → BASIC SETUP → NETWORK → Wi-Fi.**

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 37*. Another option available to use would be the SmartController. For more information please refer to **MDR 600 Series Installation & Operation Guide**.

SSID is a 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. This is case-sensitive.

Encryption refers to protocols used to protect your network. MDR supports WEP, WPA/WPA2-PSK and WPA2_Enterprise. We suggest using WPA/WPA2-PSK, as it is the newer encryption form and thus the most secure.

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



MDR Wi-Fi Settings Figure 37

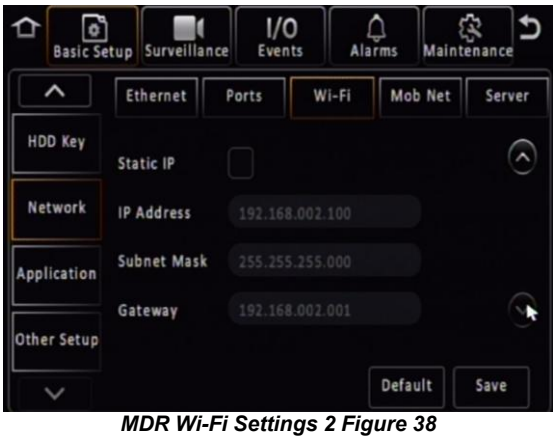
Browse to this Wi-Fi network page using **SETUP → BASIC SETUP → NETWORK → Wi-Fi → PAGE DOWN.**

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 38

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

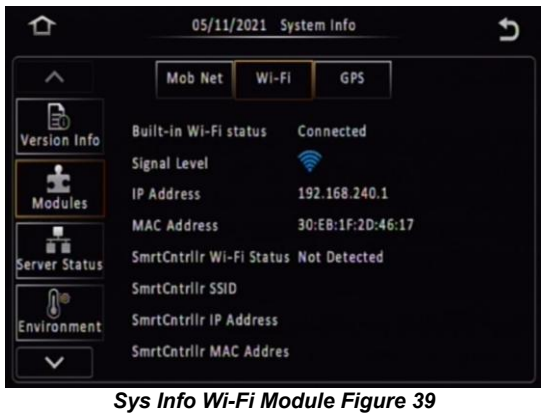
Built-in Wi-Fi status indicates the status of the Wi-Fi network connection. The different states are DETECTED, NOT DETECTED, CONNECTING, CONNECTED, CONNECTION FAILED and OBTAINING IP ADDRESS (DHCP). Once it has successfully connected to a Wi-Fi network then the status will change to CONNECTED.

Signal Level shows the signal strength. The higher the number of blue bars there are, the better the signal strength.

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 explained in **MDR 600 Series Installation & Operation Guide**.



Sys Info Wi-Fi Module Figure 39

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-641 can connect to a maximum of 2 servers; MDR-644 can connect to a maximum of 4 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.

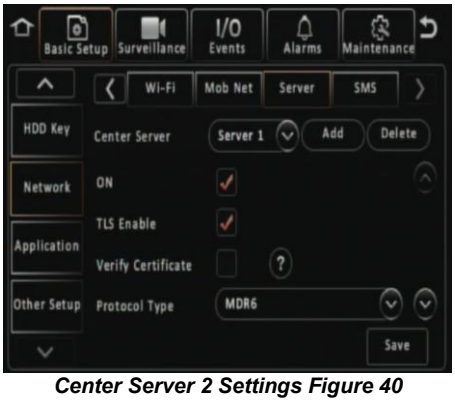
TLS Enable encrypts communication between the MDR and the Server. This is recommended to enable if the server deployed with HTTPS.

Verify Certificate ensures the authenticity of the server's certificate during every TLS connection attempt once the server's root certificate and revocation list (CRL optional) are imported into the MDR. The connection is allowed only after successful verification. This feature is disabled by default.

Warning: If enable this feature, importing the server's root certificate is mandatory prior to use; otherwise, server connections will fail. For importing toot certificate and CRLs, please refer to *MDR-64XXX-X-XXX(XX) (Various) Installation & Operation Guide.*

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 MDR6. 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 40

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

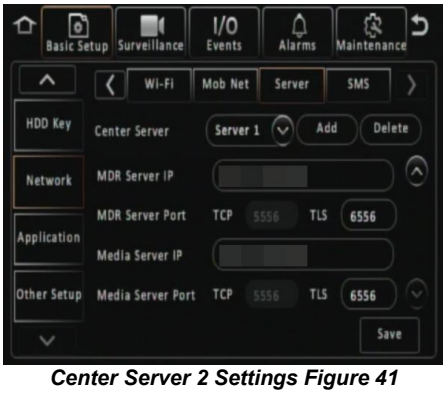
MDR Server IP is the public IP address of the firewall which forwards any traffic to the Windows Server, or IP address of the Windows Server hosting the MDR Wi-Fi Server. Example: 192.168.14.193 is the IP address of the Windows Server hosting the MDR Wi-Fi Server.

MDR Server Port is used for device access to server. When TLS function is enabled, it uses TLS port, by default, it is 6556. When TLS function is disabled, it uses TCP port, by default, it 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, it is 6556 or 5556, depends on whether enabled TLS.

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 41

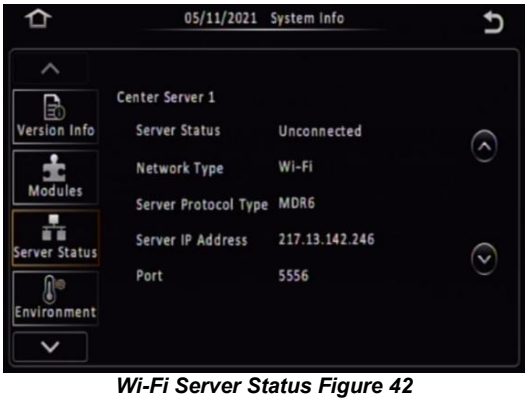
Browse to this Info page using **SYS INFO → SERVER STATUS.**

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 MDR6. Maintenance is not currently used.

Port should be the same as MDR Server Port. By default, it is 6556 or 5556.



Wi-Fi Server Status Figure 42

4.2 MDR-Dashboard 6.0 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 6.0 can display up to 500 online vehicles, any further vehicles are replaced by "**".

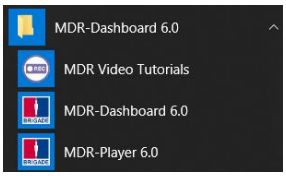
- Connect the client PC to the MDR Server Wi-Fi network.
- The client PC can also be connected to the domain with an Ethernet cable if you require network/internet access. Alternatively, the router may be configured to have internet access.

4.2.1 Logging into Server Mode (Wi-Fi)

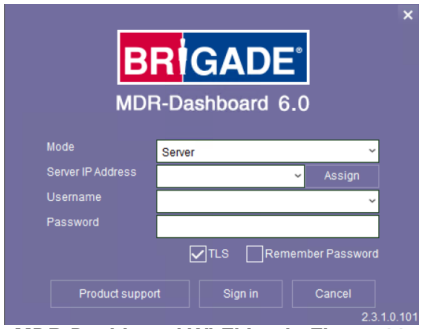
This operation is performed on the client PC. Go to **START → ALL PROGRAMS**, click on the MDR-Dashboard icon and run it as administrator as shown in *MDR-Dashboard Start Menu Figure 43*.

You are then presented with the MDR-Dashboard Login Screen. See *MDR-Dashboard Wi-Fi Login Figure 44*. Using the dropdown menu, you must choose the **SERVER** option. By default, the **TLS** is enabled for client encryption communication login to server.

You may type the server IP directly into *MDR-Dashboard Wi-Fi Login Figure 44* or follow the steps below.



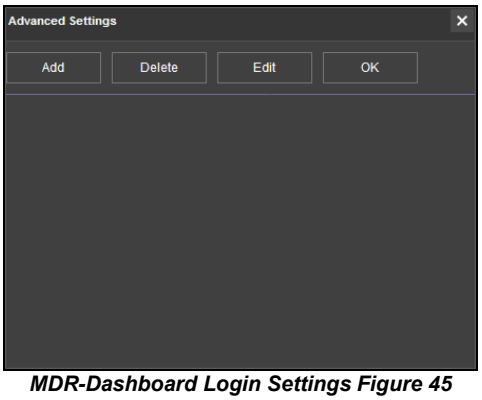
MDR-Dashboard Start Menu Figure 43



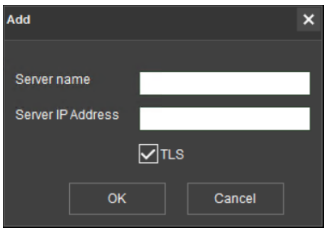
MDR-Dashboard Wi-Fi Login Figure 44

Click on **ASSIGN** which will bring up the window shown in *MDR-Dashboard Login Settings Figure 45*. This allows the user to save several server names and their associated IP addresses.

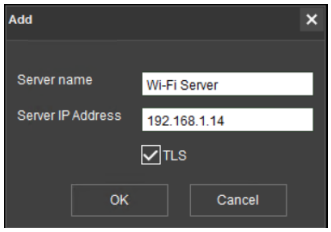
Click on **ADD** which will display *Adding a Server Figure 46*. The **SERVER NAME** can contain up to 21 alphanumerical characters. **SERVER IP** should contain numerical values and be in xxx.xxx.xxx.xxx format. The **TLS** is enabled by default.



MDR-Dashboard Login Settings Figure 45



Adding a Server Figure 46



Adding Wi-Fi Server Figure 47

Adding Wi-Fi Server Figure 47 indicates how the server has been named Wi-Fi Server and the IP has been entered as 192.168.1.14.

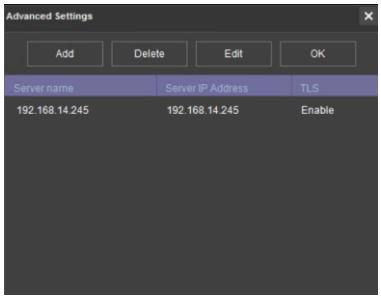
Once the details have been entered, click **OK** and the following window shown in *Wi-Fi Server Saved Figure 48* will be displayed.

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

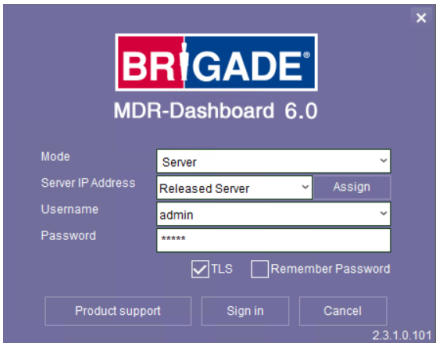
The **USER** by default is **admin** and the **PASSWORD** by default is **admin**. You may tick the **Remember Password** option if desired. Brigade recommends changing this password as sensitive data may be accessed within MDR-Dashboard.

Choose **WI-FI SERVER** and click **OK**. You will then be presented with *Wi-Fi Login Information Figure 49*.

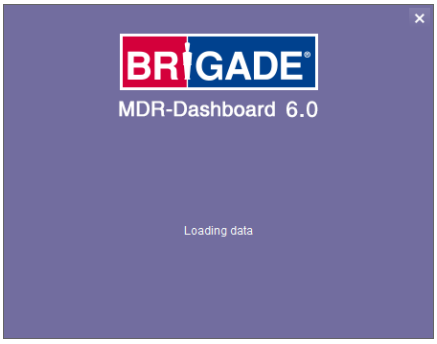
For further resources, please click on the **Product support** button. The software version number is found on the bottom right of the login window (2.3.1.XX.XX). Click **SIGN IN** to login. A loading screen will be displayed like *Wi-Fi Loading Screen Figure 50*.



Wi-Fi Server Saved Figure 48



Wi-Fi Login Information Figure 49

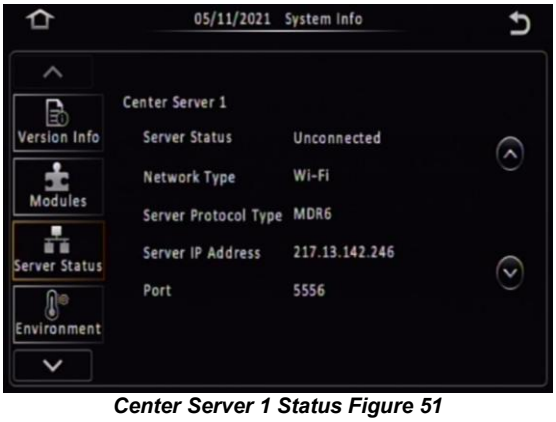


Wi-Fi Loading Screen Figure 50

4.2.2 Connecting an MDR to MDR-Dashboard 6.0 (Wi-Fi)

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

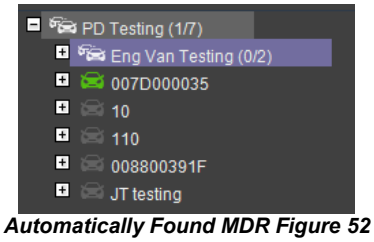
If the Chapter 4.1 Unit procedure has been followed correctly on the MDR, access **SYS INFO** → **SERVER STATUS** and confirm the Center Server 1 has successfully connected. See *Center Server 1 Status Figure 51*.



Center Server 1 Status Figure 51

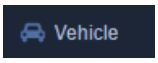
Once the above connection has been made, it may take a few minutes for the MDR unit to appear in MDR-Dashboard 6.0.

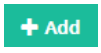
If the MDR automatically appeared, it will be found under a group labelled **TODAY'S DATE** and the MDR will be named using its **SERIAL NUM**. See *Automatically Found MDR Figure 52.*



Automatically Found MDR Figure 52

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

- In MDR-Dashboard 6.0, click **System Management**  found on the top right of the software. It will redirect you into a web page.
- Browse to 

as shown in *System Management Window Figure 55*
- Click 

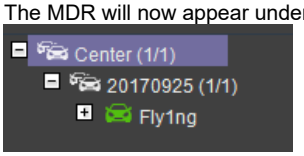
as shown in *Vehicle Window Figure 56*

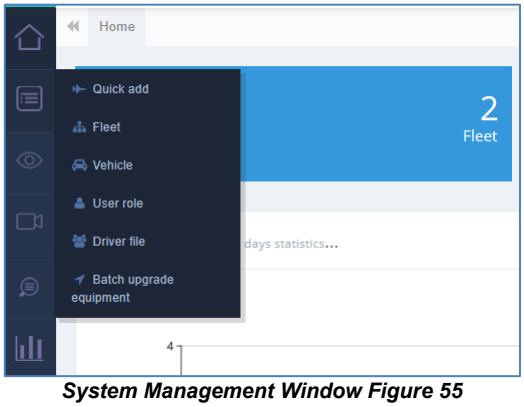
Version Information Figure 53

- 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 53*.
- **PROTOCOL** by default is **MDR6** which works for all MDR 600 Series and AI Dashcam products.

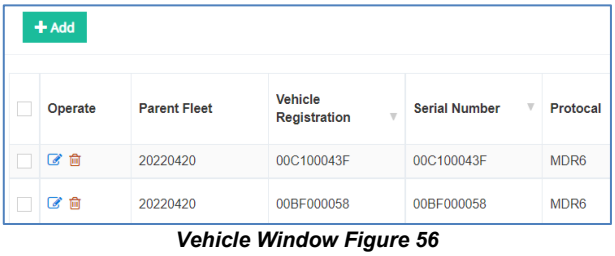
Note: **MDR5** is used for the 500 Series and the **MDR** is used for the 400 Series

- Make sure **Number of Channels** are put in correctly, this will determine how many channels are available in Live View on MDR-Dashboard client and web interface.
- **Transmit IP** and **Transmit port** are auto detected and filled in. Do not change it manually. Other information (**SIM card**, **Vehicle file** and **Equipment file**) is optional.
- Once completed, click **CONFIRM**.
- After all vehicles have been added, you will need to re-login to the MDR-Dashboard 6.0 for any changes to come into effect.
- The MDR will now appear under the group you assigned it to.





System Management Window Figure 55



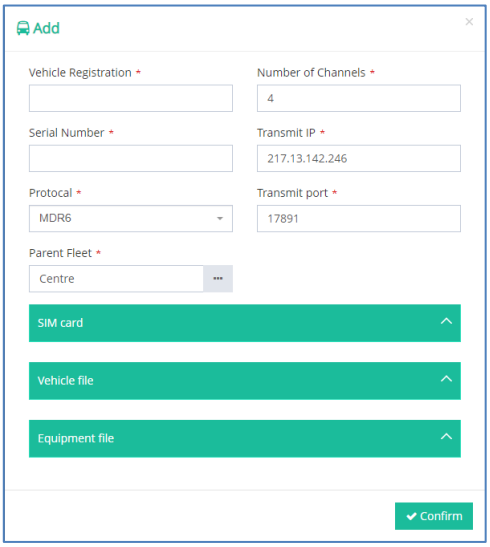
Vehicle Window Figure 56

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

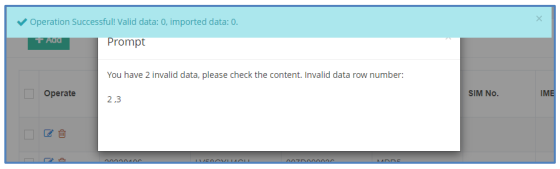
Alternative Method: Batch Import / Export Vehicles

- Apart from the above introduction of adding vehicles individually, the Web Dashboard also supports batch uploading of multiple vehicles in one go.
- In the **Vehicle** interface, find the  in the top right corner. Open the drop-down list to find **Import** or **Export** options. **Export** will download the current vehicle list in an Excel sheet. **Import** will allow the user to download a vehicle list template or choose to import the already filled-in vehicle template file.
- In the template file, please make sure all items with "*" have been filled in correctly. The Web Dashboard will check the data validity and feedback the result with a prompt window.

Note: Please be aware, every cell needs to have a value inputted. If no value is available or the user chooses not to add a value, please use "*" or "-" to replace the content, otherwise it will cause an import error.



Add a Vehicle Figure 57



Figures not Valid Figure 54

5 Mobile Network Configuration

MDR Server 6.0 and MDR-Dashboard 6.0 are compatible with various hardware models, such as the MDR 500 Series, MDR 600 Series and AI Dashcam Series. Their configuration follows the same rules and steps. The below steps will take use the MDR 600 Series as an example.

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. The SIM card must be tested prior to being installed in the MDR.

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

Brigade recommends changing the default unit password. This must be documented and controlled by the end user.

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

MTU is used to adjust MTU (Maximum Transmission Unit). The value for optimising your network transmission, by default, is set to 1500.

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.

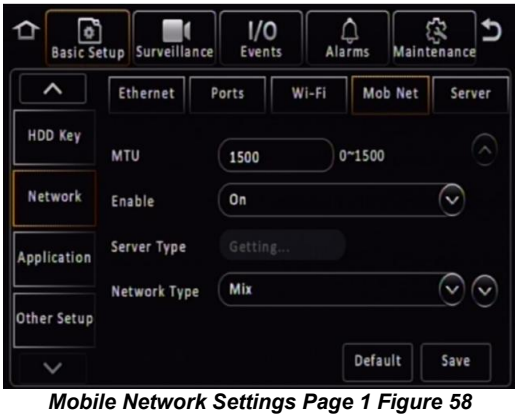
Network Type refers to the type of mobile network connection that is used by the MDR to connect to the internet. Currently, 4G is the fastest connection speed. Setting the network type to **3G** or **4G**. **MIX** can cause connectivity issues in low mobile network coverage areas.

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.

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#



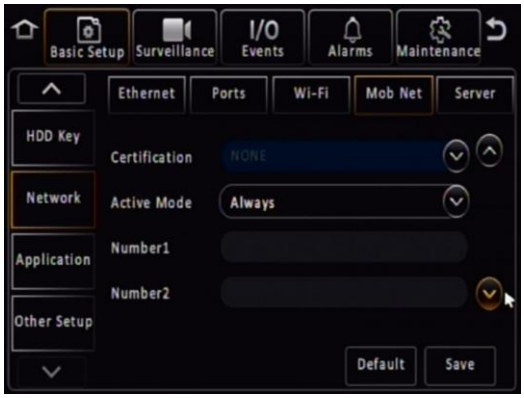
Mobile Network Settings Page 1 Figure 58

Certification refers to the authentication mode. This 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.

Mobile Network Settings Page 2 Figure 59

Active Mode provides a different type of Mob Net connection. By default, the connection mode is **Always** which means the MDR will immediately connect to a mobile network as long as this feature enabled. Another option is **Phone/SMS**, which will cause the MDR keep a 'not connected' state until certain phone call or message comes in.

Number1/2/3 link with above Active mode. If **Phone/SMS** is chosen in active mode, users can enter 3 different mobile numbers. When any of these numbers call or send a message to the MDR sim card, the Mob Net connection will be built up and MDR can start using mobile data for online features.



Mobile Network Settings Page 2 Figure 60

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 will either show module model names 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.

IMSI refers to International Mobile Subscriber Identity number. This is made up of 15 alphanumeric characters. This will display the correct number after a sim card is installed.

Mobile Network Status Figure 61

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 4 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.

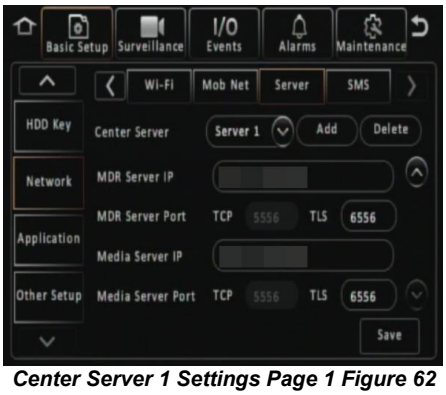
Delete removes the currently displayed center server.

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

TLS Enable encrypts communication between the MDR and the Server. This is recommended to enable if the server deployed with HTTPS.

Verify Certificate ensures the authenticity of the server's certificate during every TLS connection attempt once the server's root certificate and revocation list (CRL optional) are imported into the MDR. The connection is allowed only after successful verification. This feature is disabled by default.

Warning: If enable this feature, importing the server's root certificate is mandatory prior to use; otherwise, server connections will fail. For



Center Server 1 Settings Page 1 Figure 62

importing toot certificate and CRLs, please refer to *MDR-64XXX-X-XXX(XX) (Various) Installation & Operation Guide*

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 MDR6. Maintenance is not currently used.

Network Mode refers to the network communication modules used for communication with the MDR Server. The options are Ethernet, Mobile Network and Wi-Fi.

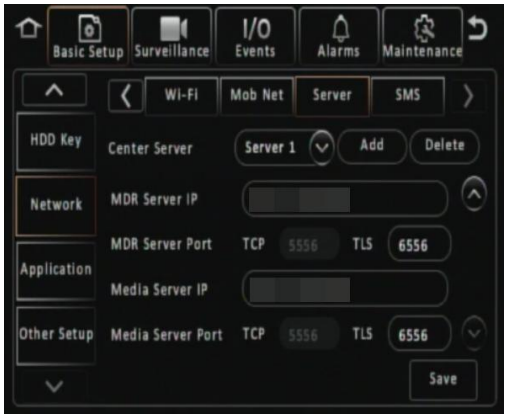
Browse to this Server page using **SETUP → BASIC SETUP → NETWORK → SERVER→ PAGE DOWN.**

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. When TLS function is enabled, it uses TLS port, by default, it is 6556. When TLS function is disabled, it uses TCP port, by default, it is 5556.

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

Media Server Port should be the same as the MDR Server Port. By default, this is set to 6556 or 5556.



Center Server 1 Settings Page 2 Figure 63

Browse to this System Info page using **SYSTEM INFO → SERVER STATUS.**

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

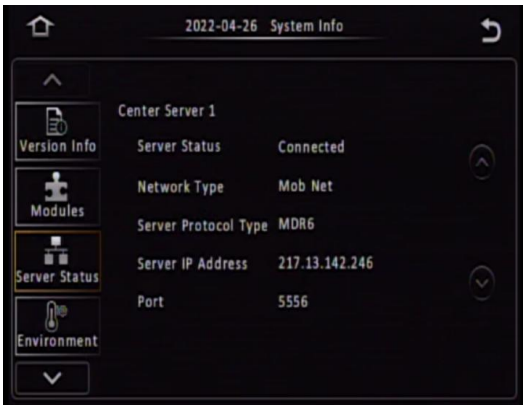
Server Status shows the current connection state of the chosen server. This can either be connected or unconnected.

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 MDR6 or maintenance. Ensure that this is set to MDR6.

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 64

5.2 MDR-Dashboard 6.0 Configuration (Mob. Net.)

5.2.1 Logging into Server Mode (Mob. Net.)

Mode refers to the MDR-Dashboard 6.0 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.

TLS is using TLS encryption to login to server.

You may type the server IP directly into *Mobile Network MDR-Dashboard Figure 65* 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 66*.
- This allows you to save several server names and their associated IP addresses.
- Click on **ADD** which will display *Adding Mobile Network Server Figure 67*. 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. The **TLS** is enabled by default.

If you are accessing the Mobile Network server externally (outside the firewall) then use the external IP address. *External Mobile Network Server Figure 68* indicates how the server has been named Mobile Network Server External and the IP has been entered as 12.345.6.78.

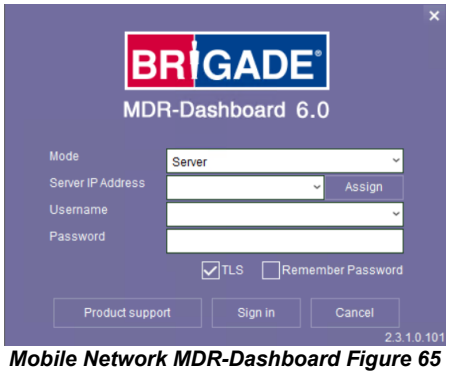
If you are accessing the Mobile Network server internally (behind the firewall) then use the IP address of the MDR Windows Server. *Internal Mobile Network Server Figure 69* indicates how the server has been named 'Mobile Network Server Internal' and the IP has been entered as '192.168.14.100'.

Choose the server which has been added and click **OK**. You will then be presented with *Mobile Network Login Figure 70*.

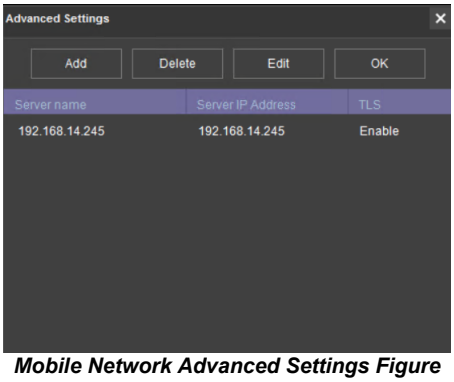
If the incorrect **USER**, **PASSWORD** **SERVER IP** is entered a "login failed" screen will be displayed.

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

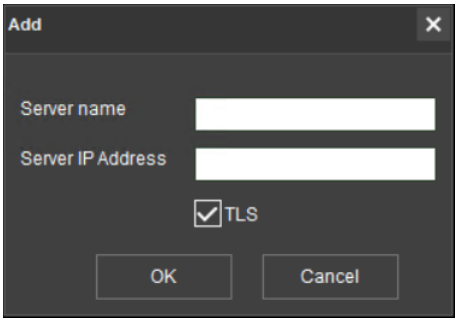
For further resources, please click on the **Product support** button. The software version number is found on the bottom right of the login window (2.3.1.XX.XX).



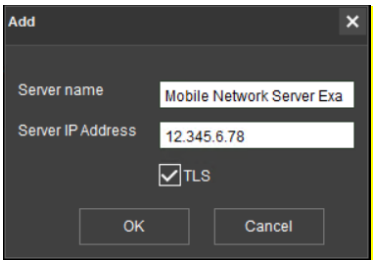
Mobile Network MDR-Dashboard Figure 65



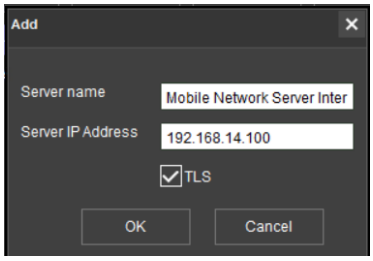
Mobile Network Advanced Settings Figure 66



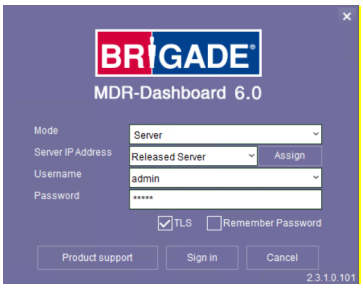
Adding Mobile Network Server Figure 67



External Mobile Network Server Figure 68



Internal Mobile Network Server Figure 69



Mobile Network Login Figure 70

5.2.2 Connecting an MDR to MDR-Dashboard 6.0 (Mobile Network)

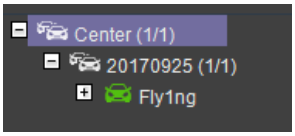
Center Servers indicates when the MDR unit has connected to a relevant MDR Server.

If the procedure in Chapter 4.1 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 71.*

Center Server 1 Status Figure 71

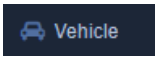
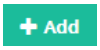
Once the above connection has been made, it may take a few minutes for the MDR unit to appear in MDR-Dashboard 6.0.

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** or **VEHICLE REGISTRATION** if populated.



Automatically Found MDR Figure 72

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

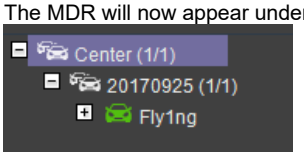
- In MDR-Dashboard 6.0, click **System Management**  found on the top right of the software. It will redirect you into a web page.
- Browse to  as shown in *System Management Window Figure 75.*
- Click  as shown in *Vehicle Window Figure 76.*

Version Information Figure 73

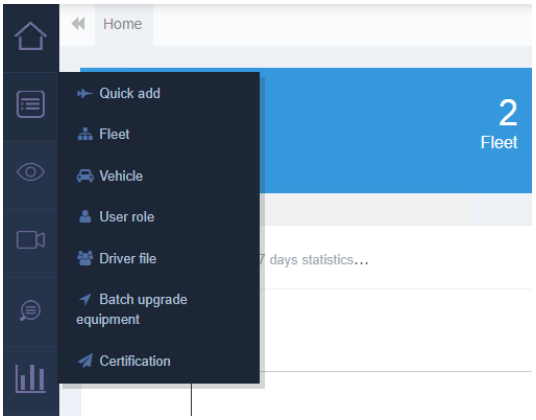
- It is recommended for the input registration details to match the vehicle registration. The maximum is 50 alphanumeric characters.
- Ensure your **SERIAL NUMBER** from the MDR firmware is entered correctly. An example is shown in *Version Information Figure 73.*
- **PROTOCOL** by default is **MDR6** which works for all MDR 600 Series and AI Dashcam products.

Note: **MDR5** is used for 500 Series and **MDR** is used for 400 Series.

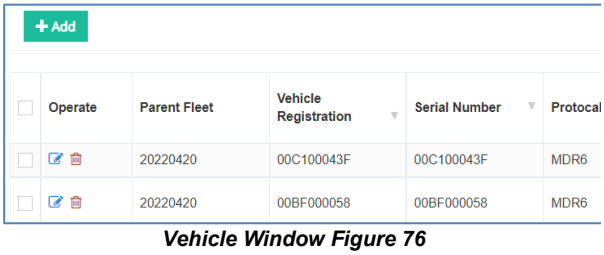
- Make sure **Number of Channels** are put in correctly, this will determine how many channels are available in Live View on the MDR-Dashboard client and web interface.
- **Transmit IP** and **Transmit port** are auto detected and filled in. Do not change it manually. Other information (**SIM card**, **Vehicle file** and **Equipment file**) is optional.
- Once completed click **CONFIRM**.
- After all vehicles have been added, you will need to re-login to the MDR-Dashboard 6.0 to allow the change to come into effect.
- 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.



System Management Window Figure 75



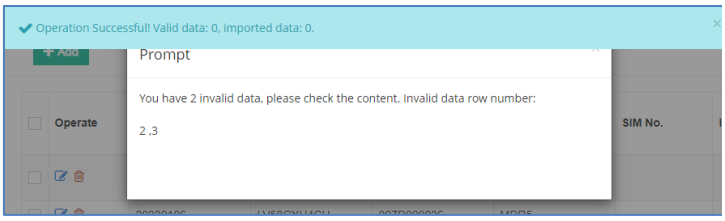
Vehicle Window Figure 76

Alternative Method: Batch Import / Export Vehicles

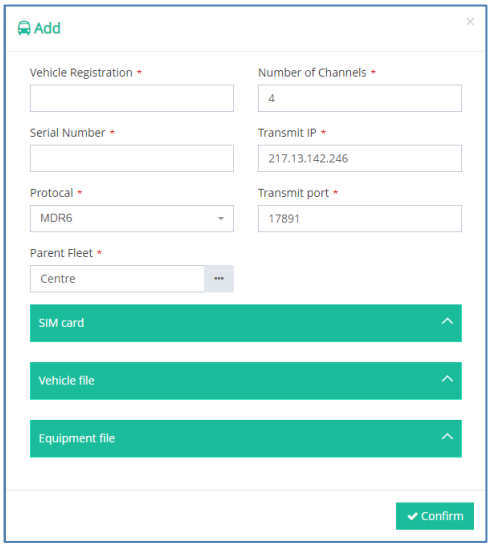
- Apart from the above introduction of adding vehicles individually, the Web Dashboard also supports batch upload of multiple vehicles in one go.

- In the **Vehicle** interface, find the  at the top right corner. Open the drop-down list to find **Import** or **Export** options. **Export** will download current vehicle list in an Excel sheet. **Import** will allow the user to download a vehicle list template or choose to import the already filled-in vehicle template file.
- In the template file, please make sure all items with "*" have been filled in correctly. The Web Dashboard will check the data validity and feedback the result with a prompt window.

Note: Please be aware, every cell needs to have a value input, if there is no information to input then please use "*" or "-" to replace the content, or an import error will be shown.



Figures not Valid Figure 74



Add a Vehicle Figure 77

6 MDR-Dashboard 6.0 Operation

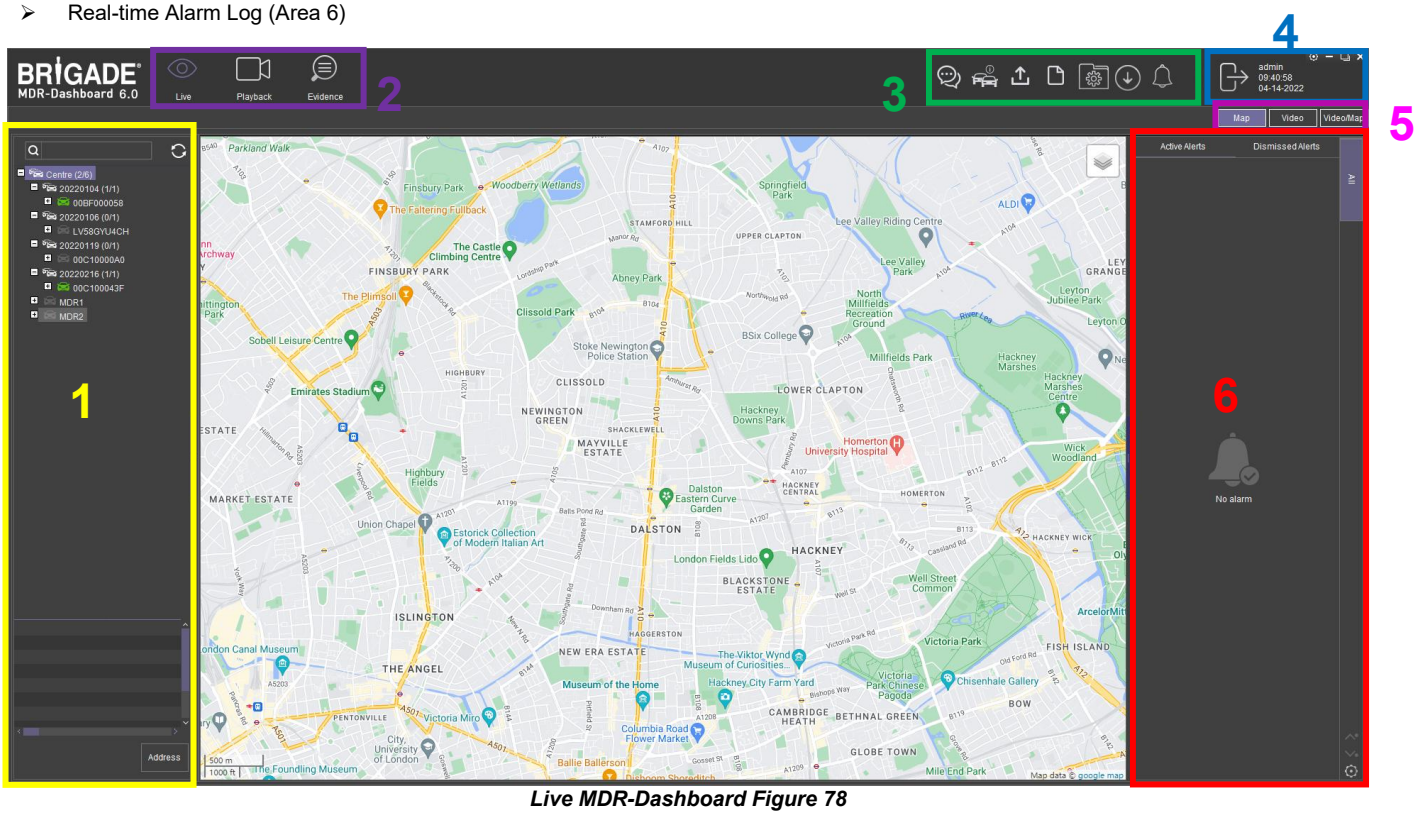
Usage scenarios must be clearly defined to meet and surpass your needs. Below is a comparison table showing the advantages of using either Mobile Network or Wi-Fi.

Table 12: Mobile Network vs Wi-Fi

MOBILE NETWORK	WI-FI
Can be accessed whilst vehicles are out	Vehicles must be in AP (access point) range and in an ON or shutdown delay (post-record) state
Remotely monitor vehicle operation (stream live devices video).	Wireless download and access data over Wi-Fi
Instant alerts of alarms for immediate action.	Automatic alerts of alarms when vehicle returns within Wi-Fi range.
Remote download of footage and view alarms.	Automatic download of footage and alarms when vehicle is 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)	No Real-time GPS tracking (beyond Wi-Fi range)

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 78*.
MDR-Dashboard 6.0 consists of several key areas such as:

- Vehicle State (Area 1)
- Type of operation (Area 2)
- **Message Centre**, **Fleet Status**, **MDR Upgrade**, **Fleet Statistics**, **System Management**, **Downloads and Alarm** (Area 3)
- User and System Settings (Area 4)
- View Settings (Area 5)
- Real-time Alarm Log (Area 6)

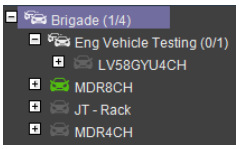


Live MDR-Dashboard Figure 78

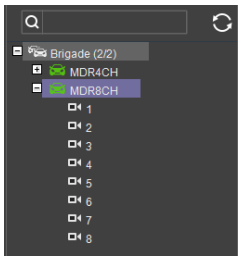
6.1 Vehicle State (Area 1)

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 79*. Camera channels may be expanded  to choose a camera to view.

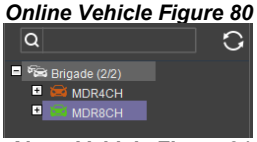
If a device is offline, camera channels cannot be accessed. Also, the vehicle icon is greyed out to indicate its offline state. An online vehicle example is shown in *Online Vehicle Figure 80*. The vehicle icon may display as a red icon if it is currently in an alarm state. See *Alarm Vehicle Figure 81*.



Offline Vehicle Figure 79



Online Vehicle Figure 80



Alarm Vehicle Figure 81

The fleet named **BRIGADE** (in this example) may be right clicked to show a sub-menu. See *Fleet Menu Figure 82*. This allows the list of vehicles in that fleet to be **EXPANDED** or **COLLAPSED**. The 'plus' and 'minus' symbols can also be used for the same purposes.

Use the **REFRESH** button  to update data for online vehicles. See *Fleet Menu Figure 82*.

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 82*. 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 Registration
- Device ID/SN
- Group
- Mode
- Longitude, Latitude
- Speed and Time/Date.
- Company Branch and Company Name
- ADAS & DFC

An example is shown in *Quick Information Figure 83*.

An advanced vehicle menu shown in *Vehicle Menu Figure 84* 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
- Network

MDR SETTINGS are used to access **ONLINE MDR** units' settings. Once **MDR SETTINGS** are accessed, *Brigade Loading Figure 85* is displayed.

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

If you get the error shown in Online *MDR Settings Error Figure 86*, this means that the setting page is still initialising, please re-try after 5 minutes.

If the setting window is not displayed but instead a prompt window asking users to re-login is displayed, it may suggest the password you previous saved for this device is incorrect.

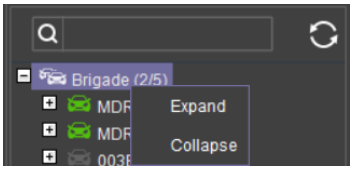
There are two ways to fix this problem. Method one is re-login as the software suggests, this is a temporary one-time access fix. Method two is to save the firmware password in the MDR-Dashboard **System Management** → **Vehicle** → **Equipment file** page, which is a permanent fix (unless the firmware login password is changed on the unit).

Method one:

- Click Confirm
- Enter Username and Password then click Login

Method two:

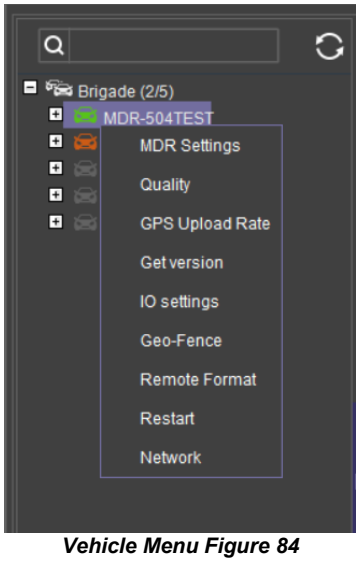
- Click X to close the error prompt
- Click System Management
- Click Vehicle
- Find the vehicle and click operate button
- Find Equipment file
- Enter Device username and Device password then click OK



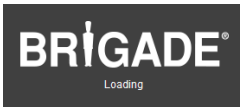
Fleet Menu Figure 82

Vehicle Registration	00BF0009D1
Device ID/SN	00BF0009D1
Group	Centre / 202407
Mode	MDR6
Longitude	0.220885
Latitude	51.432431
Speed	0 MPH
Time/Date	14:04:46 07-22-2
Company Branch	
Company Name	
ADAS	Not Calibrated
DFC	Not Calibrated

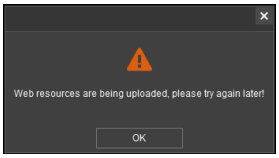
Quick Information Figure 83



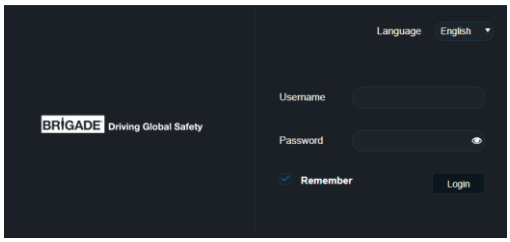
Vehicle Menu Figure 84



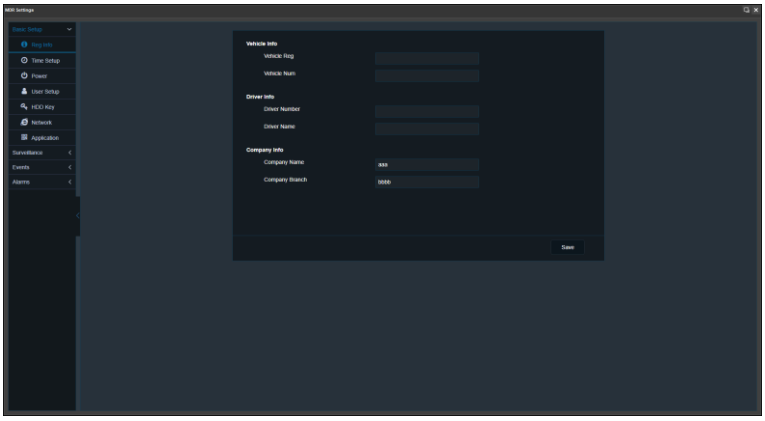
Brigade Loading Figure 85



Online MDR Settings Error Figure 86



Online MDR Settings Menu Setup Login Figure 87



Vehicle Settings Menu Setup Figure 88

See *Vehicle Settings Menu Setup Figure 88*, you can configure MDR settings related to: **Basic Setup**, **Surveillance**, **Events** and **Alarms**. This menu structure follows the device 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.

GPS Upload Rate is used to configure the interval in which the device uploads GPS information to the server. By default, it is 10 seconds. *As shown* in *Online MDR GPS Upload Rate Figure 90.*

GET VERSION is used to obtain the current firmware and MCU version installed on the device. See *Online MDR Get Version Figure 91*.

IO SETTINGS are used to remotely configure 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 92*.

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 6.0. Fence types are polygon, circle and line. Triggering conditions can be entry, exit and in or out.

Geo-Fence supports the setup of multiple zones with different trigger conditions. Every time any settings are changed (add/delete/edit a zone), please re-issue the Geo-Fence setting to the device, or it will not take into effect.

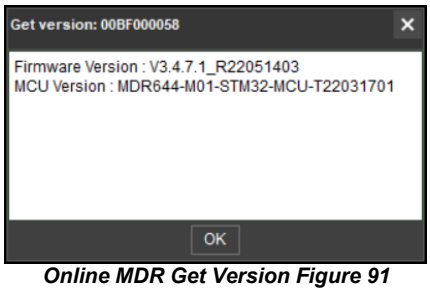
Under “in or out” condition, a Close Camera feature is available to stop camera live viewing or recording whilst inside the region set. All camera channels will display ‘Video Loss’ and no recordings will be generated or stored to the device. This feature was designed for some special security requirements. See *Geo-Fence Close Camera Feature Figure 94.*

Geo-fences can be batch issued if this needs to be applied to a fleet of vehicles. See *Online MDR Geo-Fence Figure 93.*

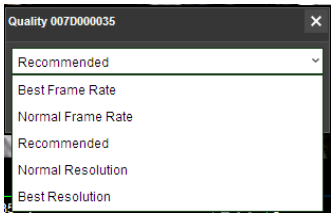
REMOTE FORMAT can be used to remotely format the main storage medium of a device. See *Online MDR Remote Format Figure 95.*

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

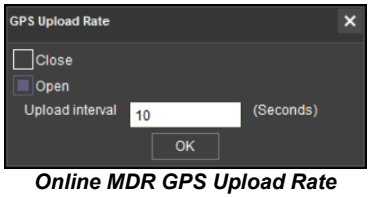
Network is used to display the current device connection method: Either via Wi-Fi, 3G/4G or Local (through Ethernet cable). See *Network Figure 97*



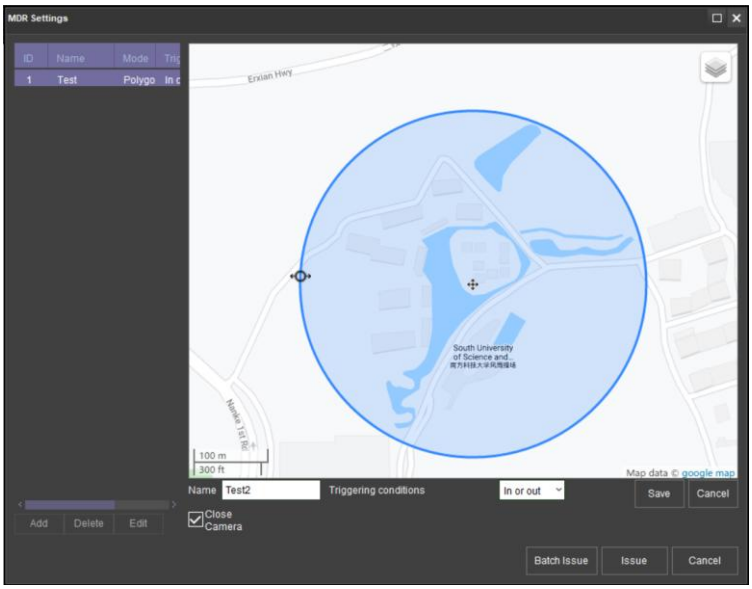
Online MDR Get Version Figure 91



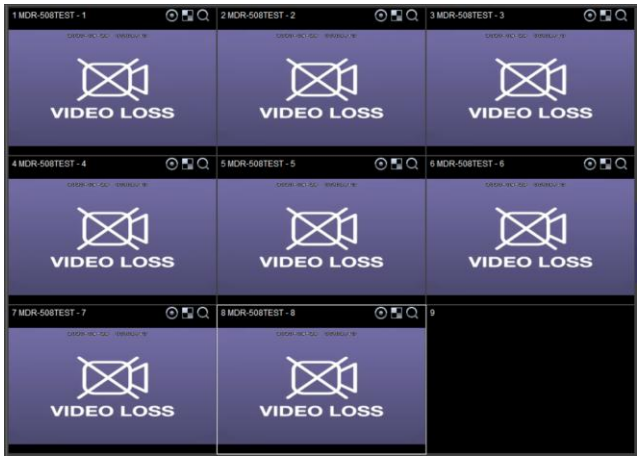
Online MDR Quality Setting Figure 89



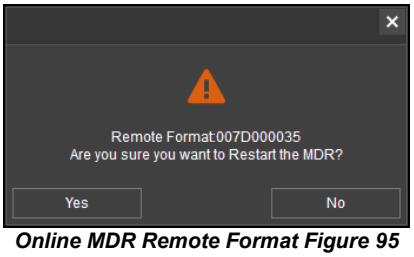
Online MDR GPS Upload Rate Figure 90



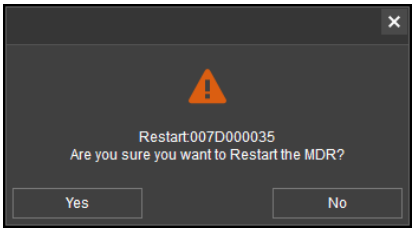
Online MDR Geo-Fence Figure 93



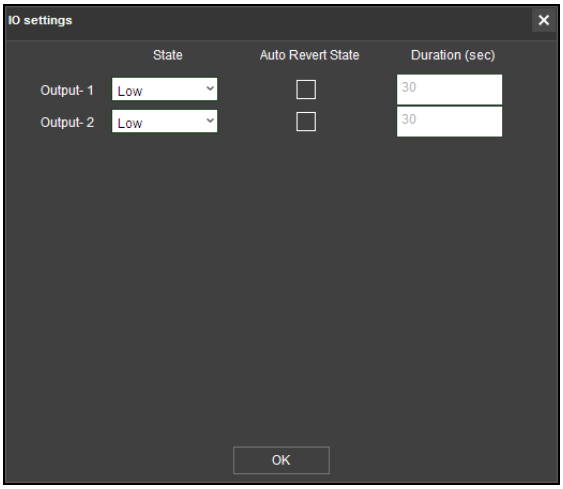
Geo-Fence Close Camera Feature Figure 94



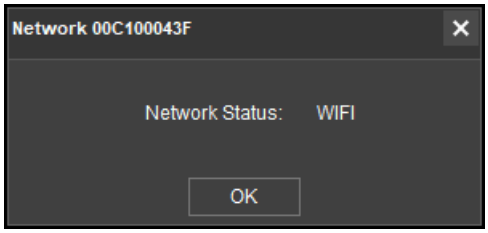
Online MDR Remote Format Figure 95



Online MDR Restart Figure 96



Online MDR IO Settings Figure 92



Network Figure 97

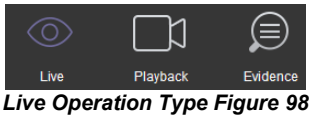
6.2 Type of operation (Area 2)

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 6.0 is in server mode. When the MDR-Dashboard 6.0 is in local mode, there is limited functionality. See **MDR 600 Series Installation&Operation Guide** for details on local mode.

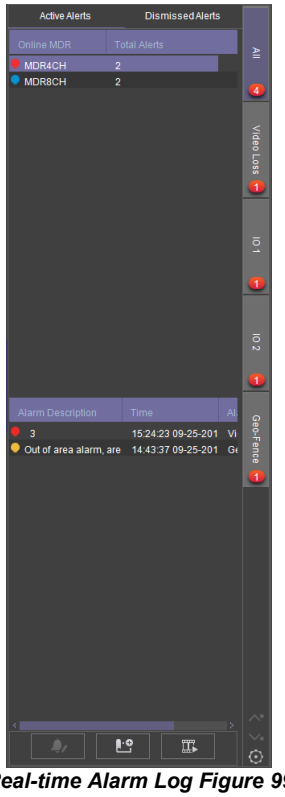
6.2.1 Live View

You access live operation by clicking on the **LIVE** icon. See *Live Operation Type Figure 98*.



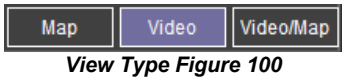
Live Operation Type Figure 98

A key feature of live operation is the real-time alarm log that shows currently occurring alarms on an online device. See *Real-time Alarm Log Figure 99*.



Real-time Alarm Log Figure 99

Choose a suitable view - **MAP**, **VIDEO** or **VIDEO/MAP**. See *View Type Figure 100*. The various views are discussed further in *View Settings (Area 5)*.

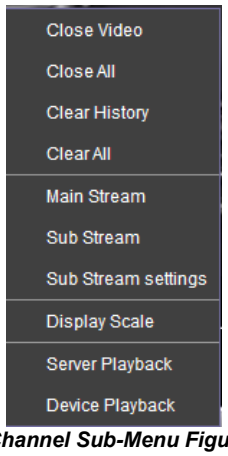


View Type Figure 100

The *Live Control Bar Figure 101* 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 101

When you right click a video channel, the sub menu shown in *Live Channel Sub-Menu Figure 102* will be displayed.



Live Channel Sub-Menu Figure 102

OPEN VIDEO is used to display all channel information and live video. See *Live Channel Sub-Menu Figure 102*.

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 102*. 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 102*.

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

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

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

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 device from the start of the current day. If there is no content, a prompt will state "Operation Failed".

DEVICE PLAYBACK will automatically playback the device's main storage media content from the start of the current day.

Note:
- A maximum of 32 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 on the available bandwidth.

Each camera channel has three additional features, **Live Recording**, **BLUR** and **ZOOM**.

Note: **LIVE RECORDING** is available in **LIVE** mode only; **ZOOM** is available in both **LIVE** and **PLAYBACK** mode. **BLUR** is available in **PLAYBACK** mode only.

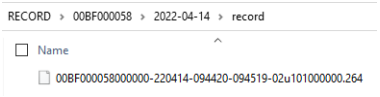
Live Recording is used to record the current live view footage and save it in a local folder. Clicking the button once will turn the icon red, indicating that recording has started, click it again to end the recording. The saved path can be set on the MDR-Dashboard 6.0 Setting page. The folder structure is "C:/RECORD/Vehicle Registration/Date/record". Only a H.264 file format will be used and saved. Regardless of what video format a device is using. See *Live Recording Figure 103*

Note: The minimum recording file size can be no less then 500kb, approximately 30s of footage, otherwise the footage will not be saved.

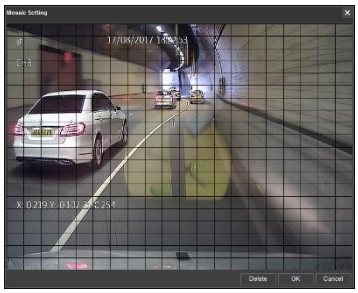
You can use **BLUR** to create a mosaic setting of an area which will be blurred throughout video playback. See Creating Mosaic for Blur Figure 104, *Setting the Blur Area Figure 106* and *Blur Activated Figure 107.*

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 108* and *Zoom area Figure 109*.

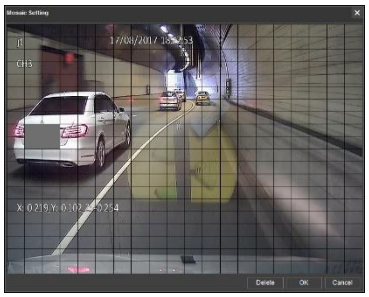
Live Recording Figure 103



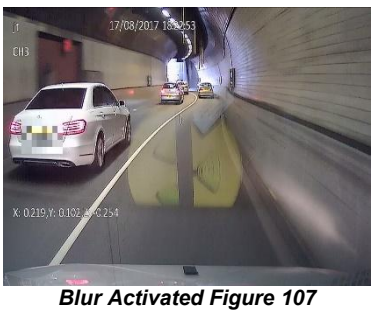
Live View Recording Saved Path Figure 105



Creating Mosaic for Blur Figure 104



Setting the Blur Area Figure 106



Blur Activated Figure 107

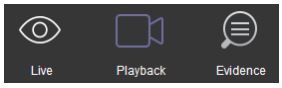
Choosing Zoom Area Figure 108

Zoom area Figure 109

is used to **ZOOM** in or out of the time scale. Maximum **ZOOM** in is 5 seconds and maximum **ZOOM** out is 24 hours. Refer to *Clipping Markers Figure 119.*

6.2.2 Playback

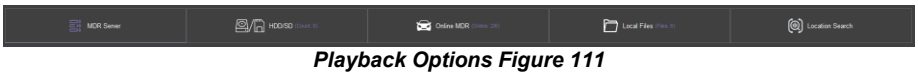
You access playback operation by clicking on the **PLAYBACK** icon. See *Playback Operation Figure 110*.



Playback Operation Figure 110

Playback Options Figure 111 will then be presented to you. There are 5 playback options:

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



Playback Options Figure 111

When using any of the **PLAYBACK** modes, you can download recordings. During playback, click on the clipping icon , shown in *Playback Bar Figure 112*. You are then presented with the toolbar shown in *Clipping Toolbar Figure 113*.

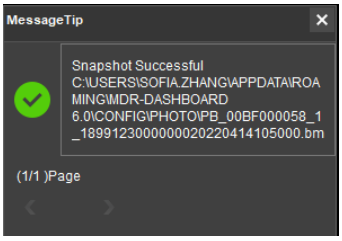
Playback Bar Figure 112

Clipping Toolbar Figure 113

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

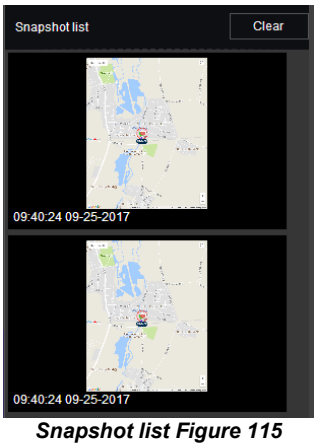
The **PLAY** function is used to play the video during clipping mode.

Once the **SCREENSHOT** button is clicked, a screenshot of the video image is stored locally under C:\USERS*username*\AppData\Roaming\MDR-Dashboard 6.0\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 114.

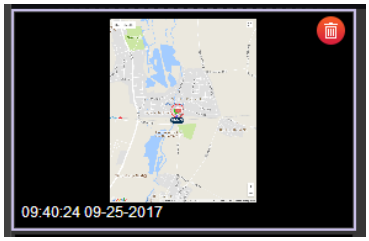


Screenshot pop-up Figure 114

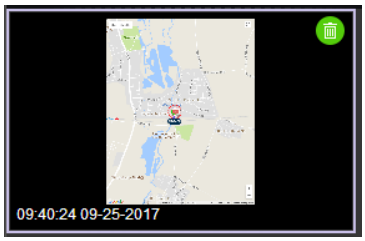
MAP SCREENSHOT is used to take screenshot of the current map position being displayed. Once this is clicked, the data will appear in the **SNAPSHOT LIST** as shown in *Snapshot list Figure 115*. Items can easily be deleted from the snapshot list by using the delete icon. See *Snapshot list Delete Icon Figure 116*. The delete icon turns green when the mouse hovers over it. See *Snapshot list Active Delete Icon Figure 117*.



Snapshot list Figure 115



Snapshot list Delete Icon Figure 116

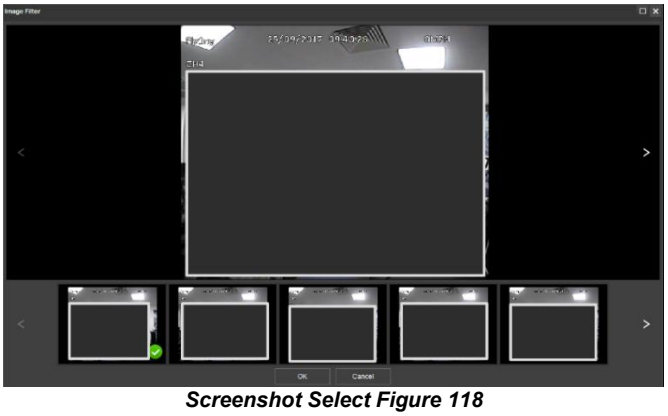


Snapshot list Active Delete Icon Figure 117

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 115*.

SCREENSHOT ALL CHANNELS is used to screenshot all channels which then appear in the Snapshot list as shown in *Snapshot list Figure 115*.

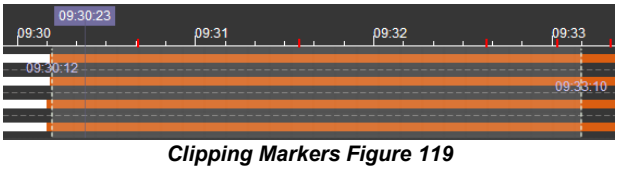
SCREENSHOT SELECT is used to give you the option to choose from several automatically generated video screenshots based on the current time marker (15:17:08 shown in *Screenshot Select Figure 118*.



Screenshot Select Figure 118

Once a screenshot is chosen, it will appear in the Snapshot list as shown in *Snapshot list Figure 115*.

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 119*.



Clipping Markers Figure 119

The clip settings window will now be shown. See *Clip Settings Figure 120*. 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 / H.265 files are opened manually by MDR-Dashboard 6.0 / MDR-Player 6.0 and are stored locally. Standard downloads can also be uploaded as evidence.
- **EXPORT** – The file size cannot be exceed 1.5GB otherwise it will become unusable. You must set the desired **PATH** and **FOLDER**

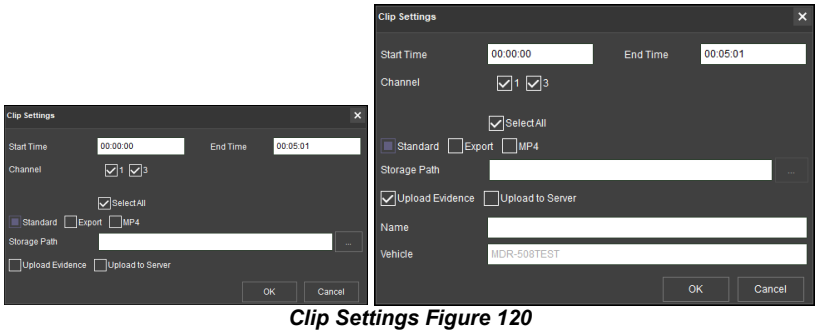
name before clicking **OK**. This option creates an executable (.exe) file including the MDR-Player 6.0 with the embedded video. These files may be password protected. If the password field is left blank then no password is set. These files are stored locally.

- **MP4** - You must set the desired **PATH** before clicking **OK**. These files can be played using standard media players. These files are stored locally.

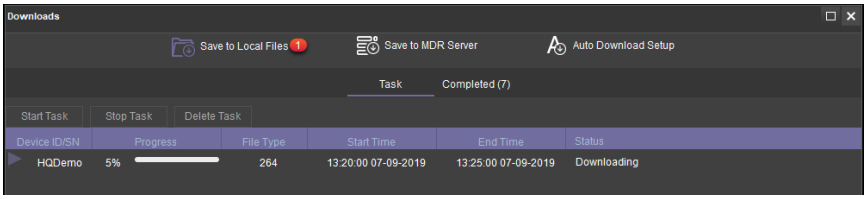
Note: If the **EVIDENCE** feature is used, the downloaded video will be uploaded to the server. The data is found in the Evidence tab. See section 6.2.6 for more information.

You can check the progress of clippings under **DOWNLOAD** → **TASK** (Area 3). See *Standard Clipping Figure 121*.

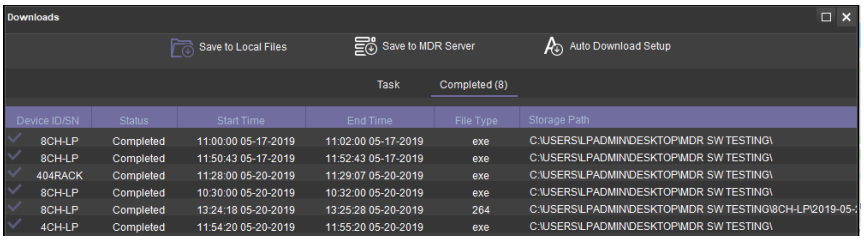
Once the task is completed, you can view the status and storage path under **DOWNLOAD** → **COMPLETED**. See *Completed Clippings Figure 122*.



Clip Settings Figure 120



Standard Clipping Figure 121



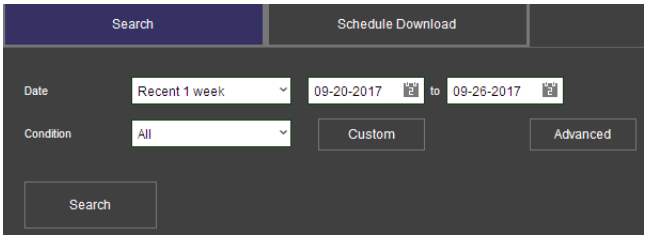
Completed Clippings Figure 122

6.2.3 MDR Server

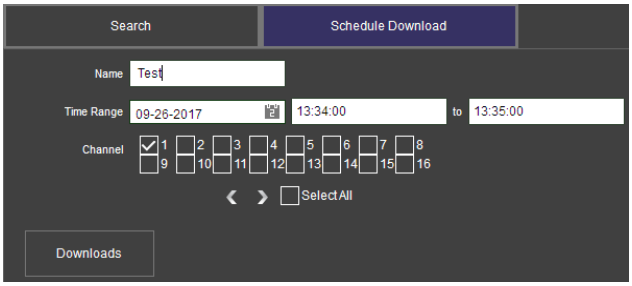
You can search the server for device downloads. These searches can be based on dates, speed and events. See *Server Search Figure 123*.

You can schedule downloads from the device to the server based on time, dates and video channels. See *Server Download Figure 124*.

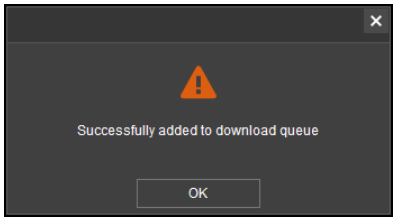
Once a user creates a scheduled download, a window pops up to indicate this has been added successfully. See *Server Download Pop-up Figure 125*.



Server Search Figure 123



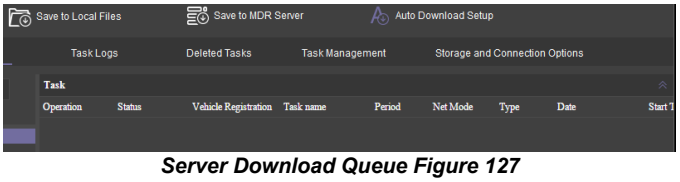
Server Download Figure 124



Server Download Pop-up Figure 125

Server Download Notification Figure 126

This scheduled download appears under auto downloads. You click on **DOWNLOAD** as shown in *Server Download Notification Figure 126*.



Server Download Queue Figure 127

Table 13 of Scheduled Downloads vs Auto Downloads

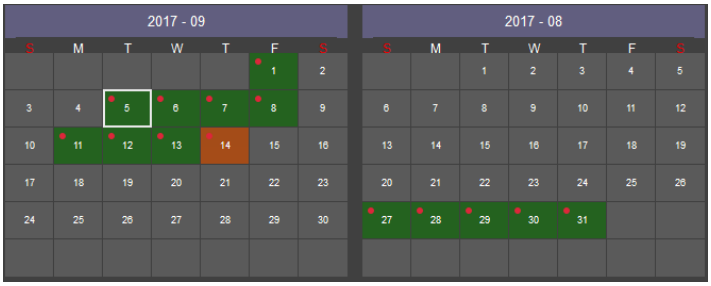
SCHEDULED DOWNLOAD	AUTO DOWNLOAD
Is a one-off download	Can be set as a recurring download
Setup based on time and channel	Setup based on time, channel, alarms and events
Will download over any available network	Can be configured to either wi-fi, mobile network or both
-	Configurable to download metadata and/or video

6.2.4 Online MDR

This is used to remotely access a unit's main storage media content.

Double-click the online vehicle icon 

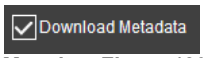
to open the calendar view as shown in *Online MDR Calendar View Figure* 128.



Online MDR Calendar View Figure 128

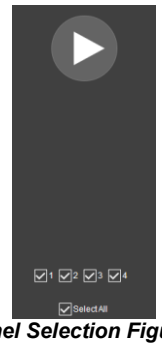
Ensure that the **DOWNLOAD METADATA** option is ticked as shown in *Metadata Figure 129*. This is found bottom left of the calendar view.

- 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)



Metadata Figure 129

Double-click the desired date and choose which camera channels to view. See *Channel Selection Figure 130*.



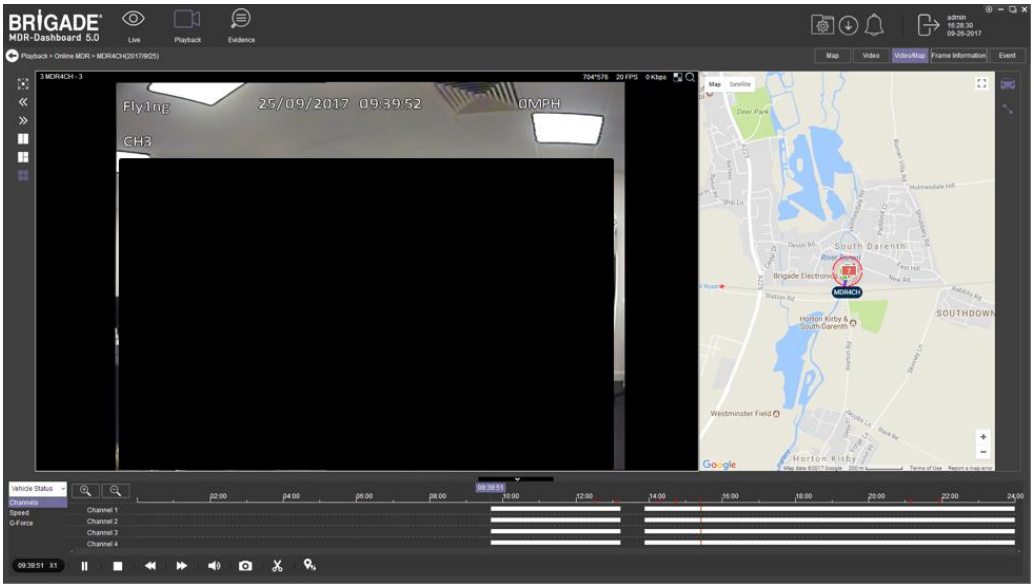
Channel Selection Figure 130

Then click the **PLAY** button located above the channel selection. See *Channel Selection Figure 130*.

Once you click play, the video will be displayed as shown in *Playing a Video Figure 131*.

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 device voltage.
- CAN data – 14x different CAN categories.



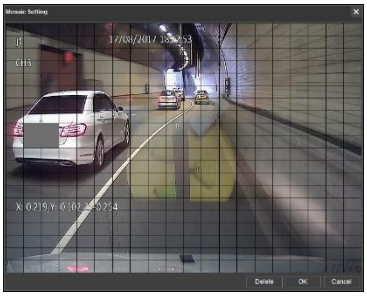
Playing a Video Figure 131

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 132*, *Setting the Blur Area Figure 133* and *Blur Activated Figure 134*.

Creating Mosaic for Blur Figure 132



Setting the Blur Area Figure 133

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 135* and *Zoom area Figure 136*.

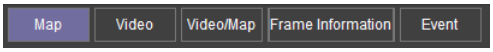
Blur Activated Figure 134

Choosing Zoom Area Figure 135

Zoom area Figure 136

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

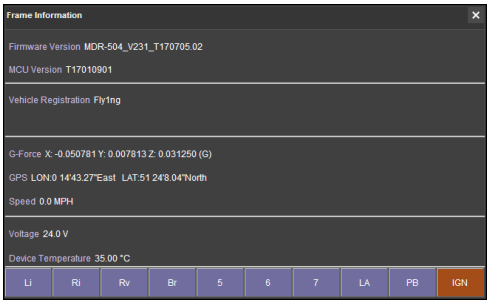
To view further information regarding the recording you can access **FRAME INFORMATION** and **EVENT** as shown in *Extended View Settings Figure 137*.



Extended View Settings Figure 137

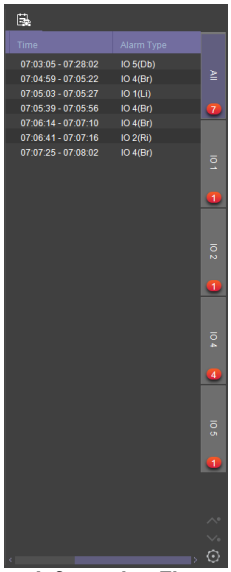
See *Frame Information Figure 138*. **FRAME INFORMATION** consists of:

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



Frame Information Figure 138

See *Event Information Figure 139*. Event information consists of device alarms which have event names and times.



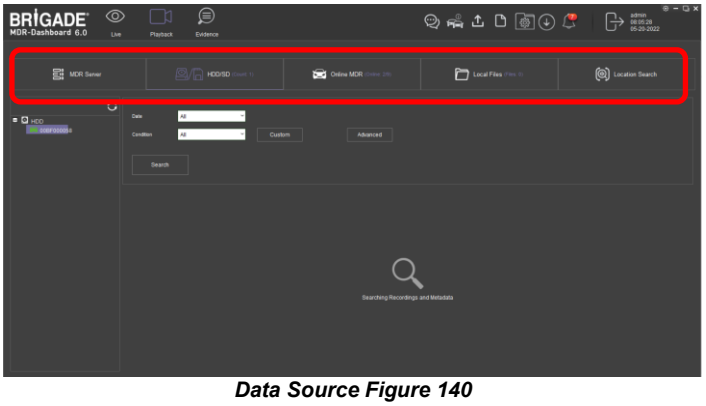
Event Information Figure 139

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 device and saved onto a USB flash drive or recordings saved onto a PC.

To view downloaded files, click on the **LOCAL FILES** tab found on the Data Source Access (area 1). See *Data Source Figure 140*.



Data Source Figure 140

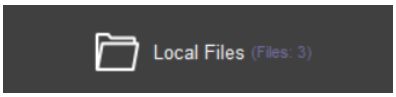
Click on the **LOCAL FILES** tab as shown in *Local Files Tab Figure* 141.

Click the **ADD** button as shown in *Local Files Add Figure* 142. Browse to the relevant folder and click **SELECT FOLDER**.

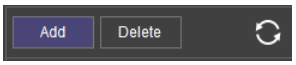
This brings up a Windows™ Explorer dialogue box (*Windows Explorer Folder Figure 143*) which allows you to select the folder that contains the recordings. Select the Vehicle name, in this example 3-3.

Once the folder has been successfully loaded, it will appear as shown in *Device Directory Figure 144*.

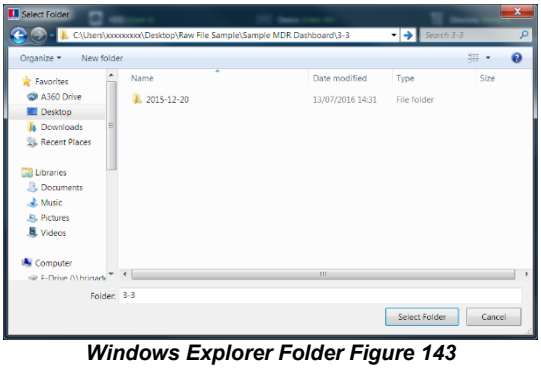
If there was a local file specified previously, click the refresh icon  to get the local file to appear. This will be a green icon to indicate it is available for browsing.



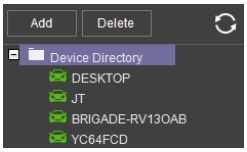
Local Files Tab Figure 141



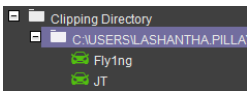
Local Files Add Figure 142



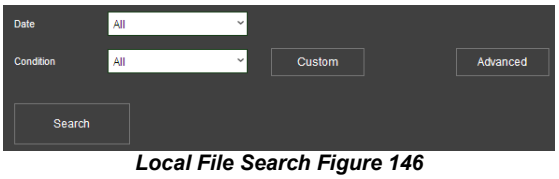
Windows Explorer Folder Figure 143



Device Directory Figure 144



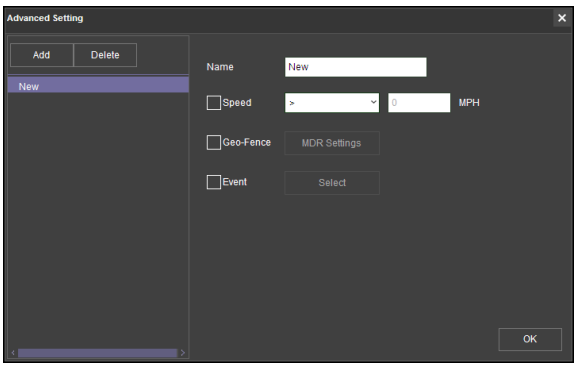
Clipping Directory Figure 145



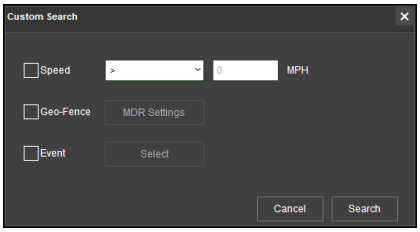
Local File Search Figure 146

The local file will now appear in the left pane as shown in *Device Directory Figure 144*. **DEVICE DIRECTORIES** show when a specific vehicle folder is chosen, these are added individually. If you would like to add multiple vehicles simultaneously, choose the folder level 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* 146. Custom and Advanced searches can be configured. See *Custom Search Figure 147, Windows Explorer Folder Figure 143* and *Advanced Search Settings Figure 148*.



Advanced Search Settings Figure 148



Custom Search Figure 147

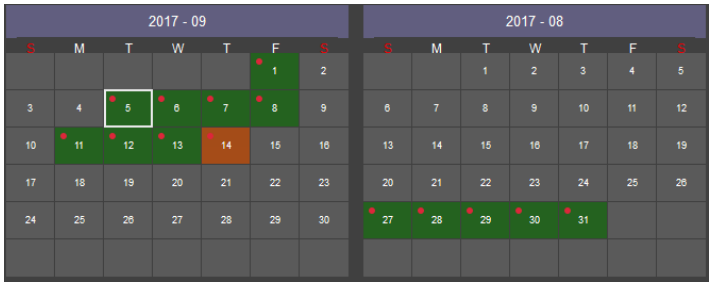
6.2.5.2 HDD/SD Playback

Double-click the vehicle icon 

. This will display **ALL** calendar events. A typical example of a calendar is shown in *HDD Calendar Figure 149.*

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).

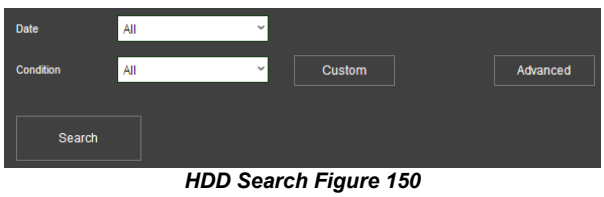


HDD Calendar Figure 149

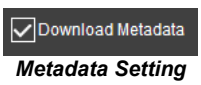
To refine the data displayed, you need to setup a search criteria. Custom and Advanced searches can be created. *HDD Search Figure 150*.

Ensure that the **DOWNLOAD METADATA** is always ticked. See *Metadata Setting Figure 151*. This will ensure that all metadata is shown with playback video.

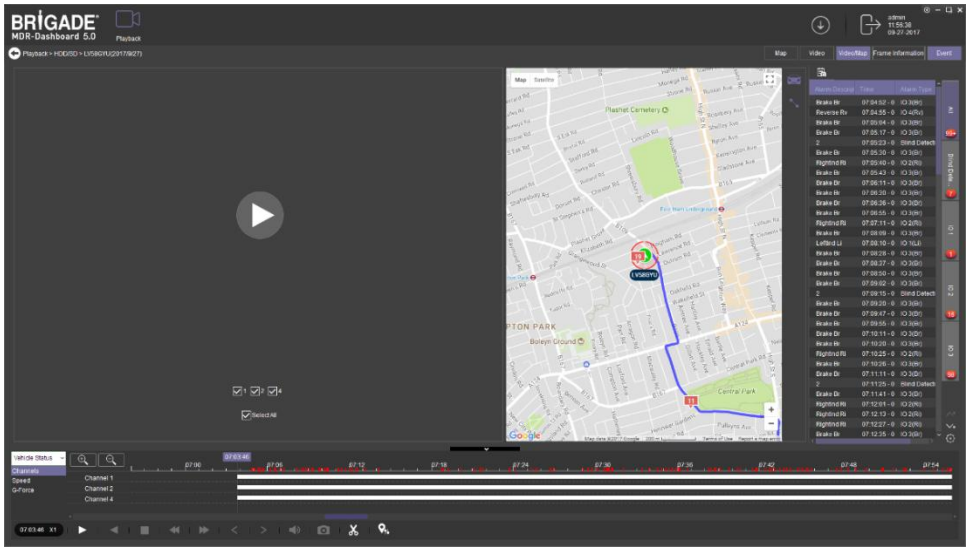
Double-click on the relevant calendar date, this will display the pre-playback screen. See *Pre-playback Figure 152.* You can choose which channels to view during playback.



HDD Search Figure 150

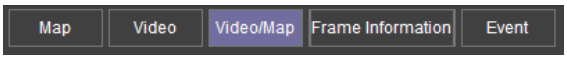


Metadata Setting Figure 151



Pre-playback Figure 152

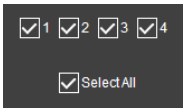
You can access different view settings such as, **MAP**, **VIDEO** and **VIDEO/MAP**. See *View Options Figure 153*.



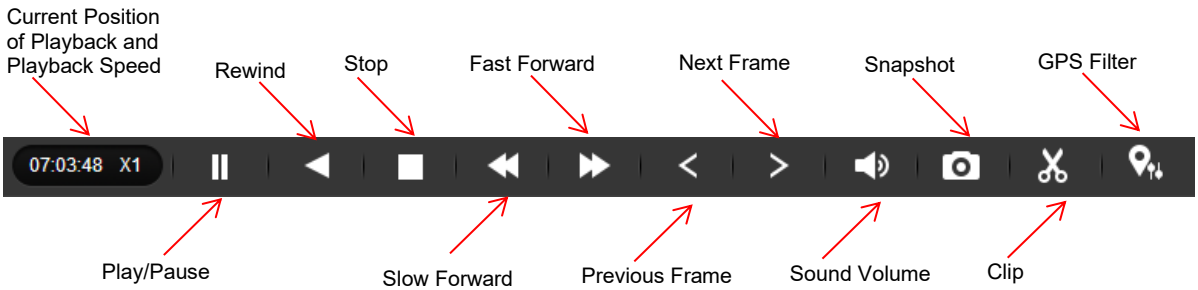
View Options Figure 153

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 154*.

Return to Calendar Figure 154

Choose which channels to playback. 

Click the Play button  to display the data.



MDR-Dashboard 6.0 Controls Panel Figure 155

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

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

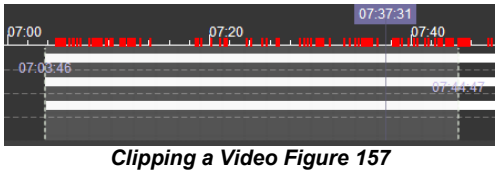
Video View Options Figure 156, such as:

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

Video View Options Figure 156

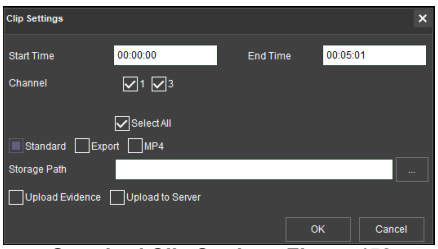
6.2.5.2.1 Downloading Videos

Click on the **CLIP** button  .
Clip markers appear (dashed vertical lines). See *Clipping a Video Figure 157*.
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 158*.
Choose the number of channels you wish to download.
Choose the type of download, there are three types of downloads:



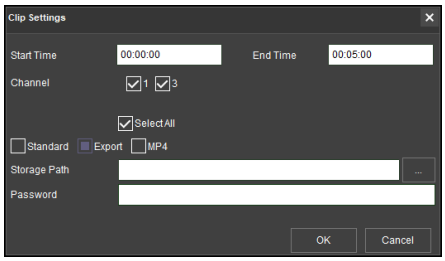
Clipping a Video Figure 157

- **STANDARD** creates a folder structure containing the video files in original proprietary format (H264 or H265 depending on the device setting) 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.



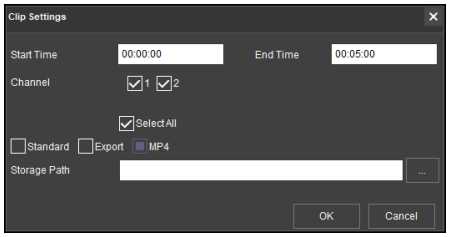
Standard Clip Settings Figure 158

- **EXPORT** allows you to export clips into a single .exe file with an embedded MDR-Player 6.0. This option is the recommended solution as it contains metadata and video. It can also be password protected and played without the need for any additional player software. This does not require any installation. Note, this file should not be larger than 1.5GB.



Export Clip Settings Figure 159

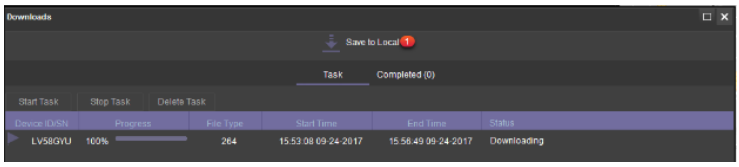
- **MP4** creates .MP4 files playable by common players such as Windows Media Player (WMP™) and Video Lan Client (VLC). This method provides an easily viewable format across various platforms. However, the protection is limited and the format does not allow for metadata. These files can be played and 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.



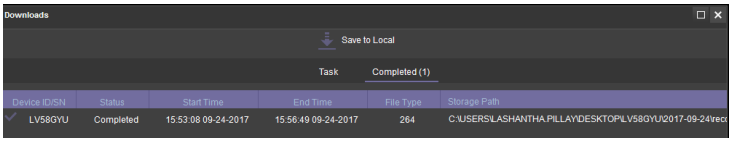
MP4 Clip Settings Figure 160

Choose the Storage Path using  . Brigade recommends choosing your C: drive or desktop.

Once selected, click on the **OK** button  .

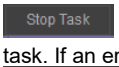
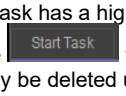
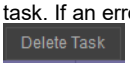


Current Download Tasks Figure 161



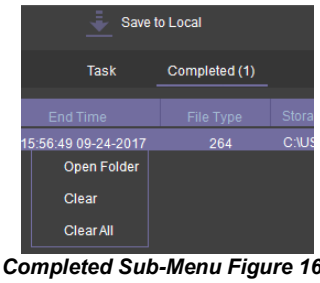
Completed Download Tasks Figure 162

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

See *Current Download Tasks Figure 161*. 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 162*.

Right-click a completed task to access a sub-menu as shown in *Completed Sub-Menu Figure 163*.



Completed Sub-Menu Figure 163

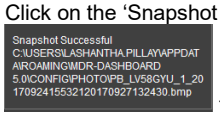
6.2.5.2.2 Saving Snapshots

Click the desired channel; this will be highlighted by a **WHITE OUTLINE**. See *Choosing a Channel Figure 165*.

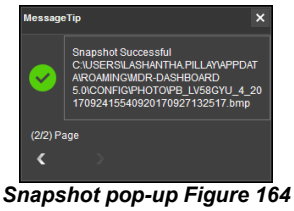
Click on the **SNAPSHOT** button  in the Controls Panel.

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 164*).

Click on the 'Snapshot Successful' information



to access the **IMAGE FILTER**, this shows all locally stored snapshots. See *Snapshot Image Filter Figure 166*.



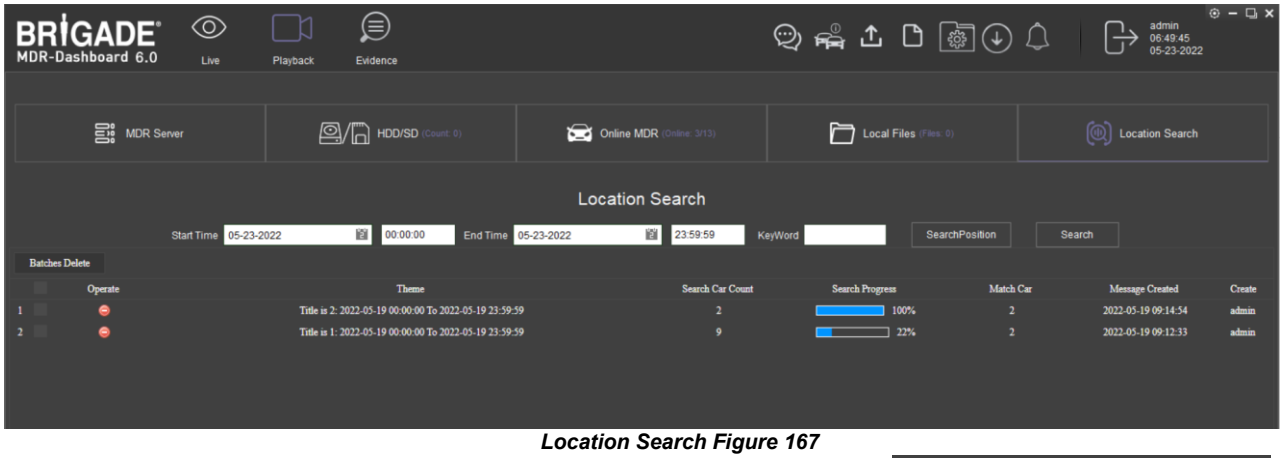
Snapshot pop-up Figure 164

Choosing a Channel Figure 165

Snapshot Image Filter Figure 166

6.2.6 Location Search

This feature allows users to search and extract recordings from online devices based on geographic requirements. Users can setup a dedicated zone on the Map, then decide a fleet scope to search for. After a few minutes, the MDR-Dashboard will give out a list of recordings which match with these requirements.



Location Search Figure 167

To create a location search task, please firstly decide the **Start Time** and **End Time** of the search. This can be decided down to seconds.

KeyWord used for assigning a task name.

SearchPosition will open a separate map window for users to draw the geographic searching zone. The map window looks identical to Geo-Fence window and has similar tools. Regions can be drawn as a **Polygon, Circle** or **Rectangle** and multiple separate zones can be supported via the **Add** button as shown in *Search Position Figure 170*.

The **SearchPosition** is a one-time operation. After saving and closing the map window, the next search will be based on zone(s) selected. If the user opens the **SearchPosition** window creates another zone, once saved it will overwrite the previous zone(s) set.

After setting up the time and region, when clicking the **Search** button, it will pull up the fleet list for defining the vehicle scope. The user can choose from different vehicles or fleets to operate the search, as shown in *Search Figure 171.*

After the search begins, it will show up on the list with details of:

Operate: Click  to delete this task.

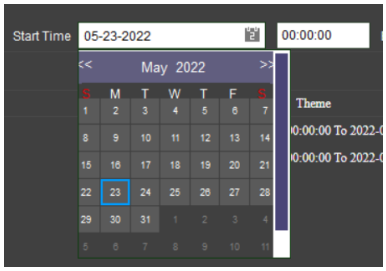
Theme: compose with task name and pre-set time range.

Search Car Count: total quantity of vehicles to be searched.

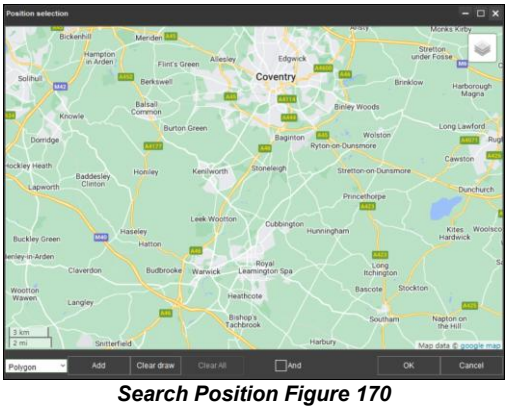
Search Progress: process bars to indicate the status of searches.

Match Car: how many vehicles fulfil the search condition.

Message Created: when this task has been created.

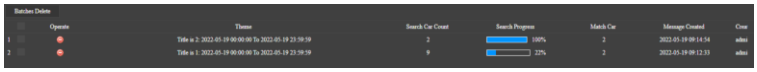


Start Time and End Time Figure 169



Search Position Figure 170

Creator: which user created this task.

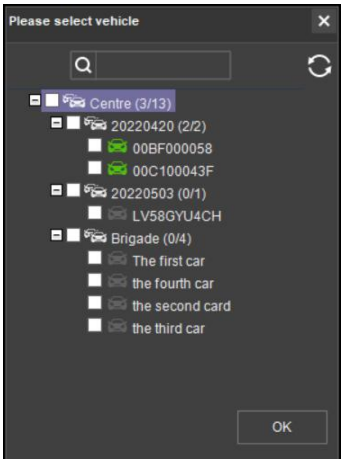


Location Search Task Details Position Figure 168

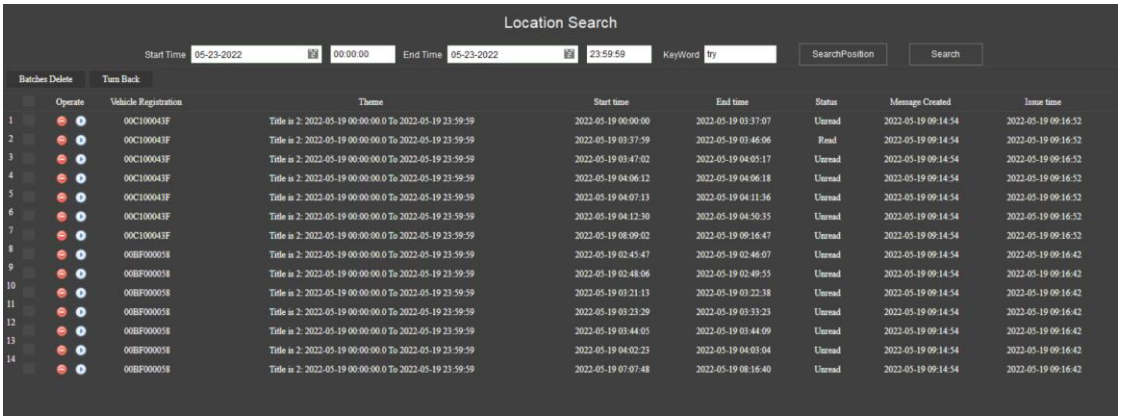
The **Location Search** is based on online devices. Therefore, if some of the chosen devices are not online, the task will suspend and wait until they come back online. The task will remain on the list with an unfinished progress bar whilst vehicles are still being scanned and searched.

This interface refreshes every 30 seconds. If manual refresh is required, click the manual refresh button at the bottom left of the window can be used.

After the search is complete, it will show how many vehicles match the set condition. The user can click on the **Match Car** number 2 to view detailed recordings.



Search Figure 171



Location Search Results Figure 172

Each displayed item represents a recording clip which matches the search condition. They can all be viewed by the operate button .

Operate: to delete the search entry or view it.

Vehicle Registration: which vehicle this recording is from.

Theme: The initial task title and search condition.

Start time: the actual start time of this footage.

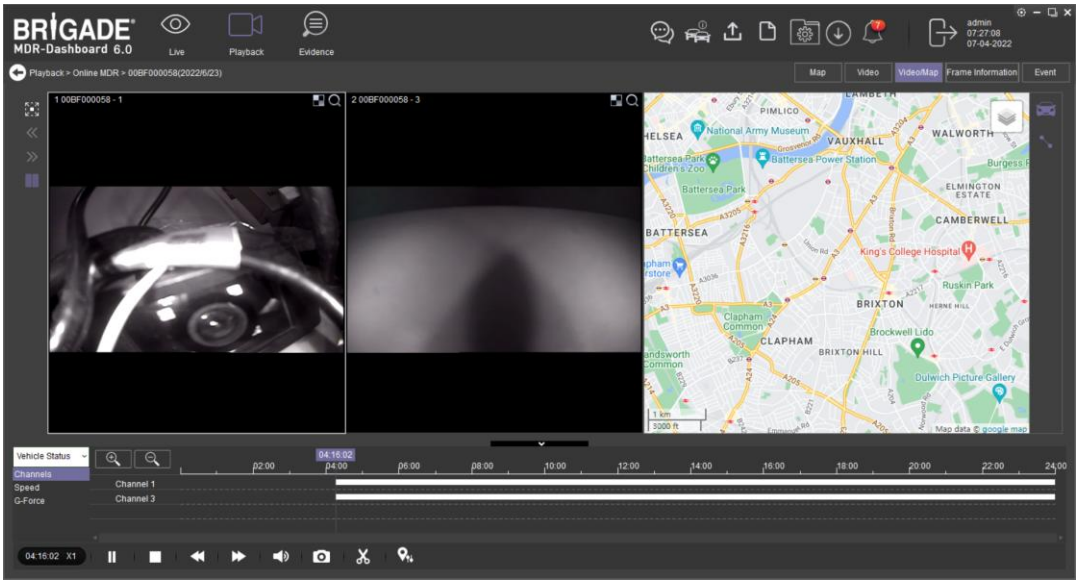
End time: the actual end time of this footage.

Status: shows whether the results have been viewed or not, for indication purpose only.

Message Created: when the task was created.

Issue Time: when the entry was searched.

The viewing window is the same as any recording playback window. It supports video and map views and multiple process operations. Details for each operation please refer to *Chapter 6.2.5.2 HDD/SD Playback*.



Playback Location Search Results Figure 173

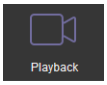
6.2.7 Evidence

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

Note: Evidence upload is only available when MDR-Dashboard 6.0 is logged into **SERVER** mode.

6.2.7.1 Evidence Upload

To create evidence packages please follow the steps described below. These files are accessible via MDR-Dashboard 6.0. 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.

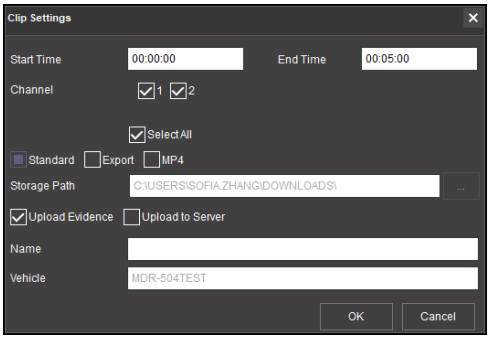
Create the desired snapshot list using the evidence buttons 

which will be associated with this video clip.

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

The Clip Settings window will now be displayed. See *Clipping Markers Figure 119*.

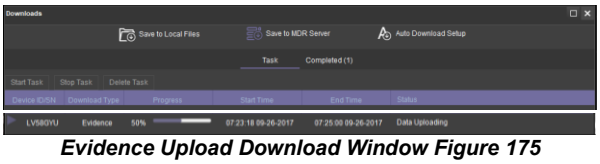
Ensure **STANDARD** is ticked then tick **UPLOAD EVIDENCE**. This means that the path specified under **PATH** is now void. See *Evidence Upload Figure 174*.



Evidence Upload Figure 174

Fill in all details shown in *Evidence Upload Figure 174*. The following details can be completed: Name and Vehicle (automatically populated). Click **OK** once all details are filled in. **Name** is a required field.

To confirm that this evidence upload task has been created, click **DOWNLOAD → SAVE TO SERVER**. See *Evidence Upload Download Window Figure 175*.



Evidence Upload Download Window Figure 175

This task will appear under **COMPLETED** once it has finished. See *Evidence Upload Download Window Figure 175*.

6.2.7.2 Evidence Centre

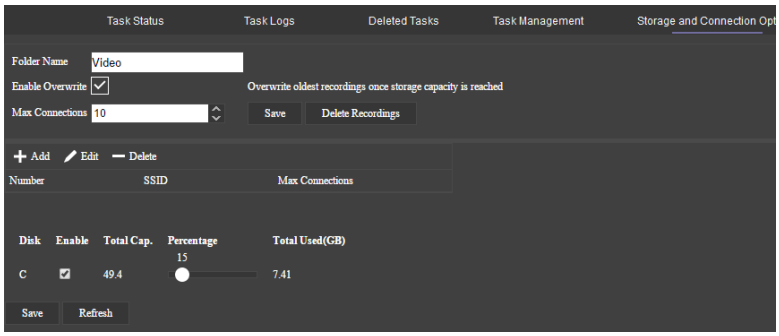
Due to the nature of evidence (contains sensitive information), it can **NEVER** be clipped or copied locally. Evidence is stored on the server and can only be accessed via MDR-Dashboard 6.0.

You access playback by clicking on the **EVIDENCE** icon. See *Evidence Icon Figure 177*.

Server directory for evidence video file storage: C:\evidencedata.

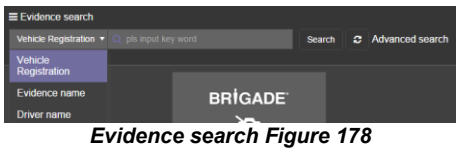
Use the search feature to navigate to the desired vehicle/company name (fleet) as shown in *Evidence search Figure 178*.

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



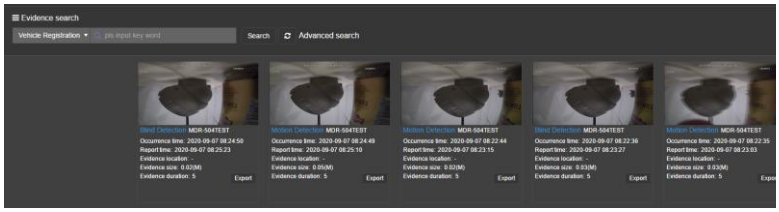
Storage and Connection Options Figure 176

Evidence Icon Figure 177



Evidence search Figure 178

A full list of evidence is now displayed as shown in *Evidence List Figure 179*. This list shows each evidence as information cards and has a snapshot as a thumbnail (at the top)



Evidence List Figure 179

Alarm type is shown in blue and followed with **vehicle registration**

Occurrence time: when the alarm happened, the timestamp is obtained from the device.

Report time: evidence upload time, the timestamp is obtained from the server.

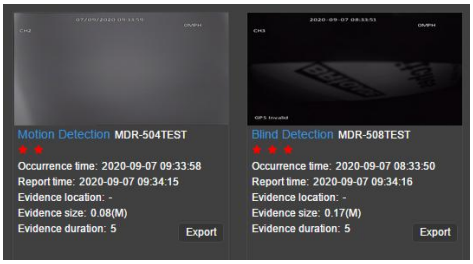
Evidence location: click the button to show the location, if the button is unavailable then it either means no

GPS info was ticked on the alarm setting page or the vehicle did not have any GPS data at that time.

Evidence size including H.264 / H.265 video, snapshot (if available) and a PDF report.

Evidence duration represents the video time in seconds.

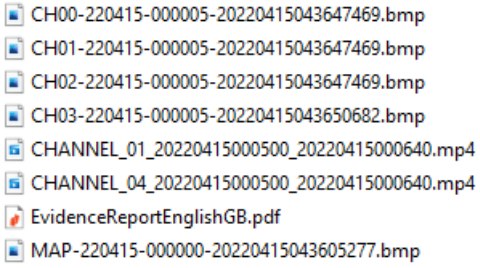
Importance displays as ★ which can be setup in web Dashboard->Setting->Alarm level setting. There are 4 available levels in total. By default, all alarms have no importance level assigned.



Evidence Importance Marker Figure 180

Click on **Export** button Export which will begin to download the evidence pack in .rar format. The package contains snapshots, .mp4 video and evidence report in excel format. See *Evidence Export Content Figure 181*

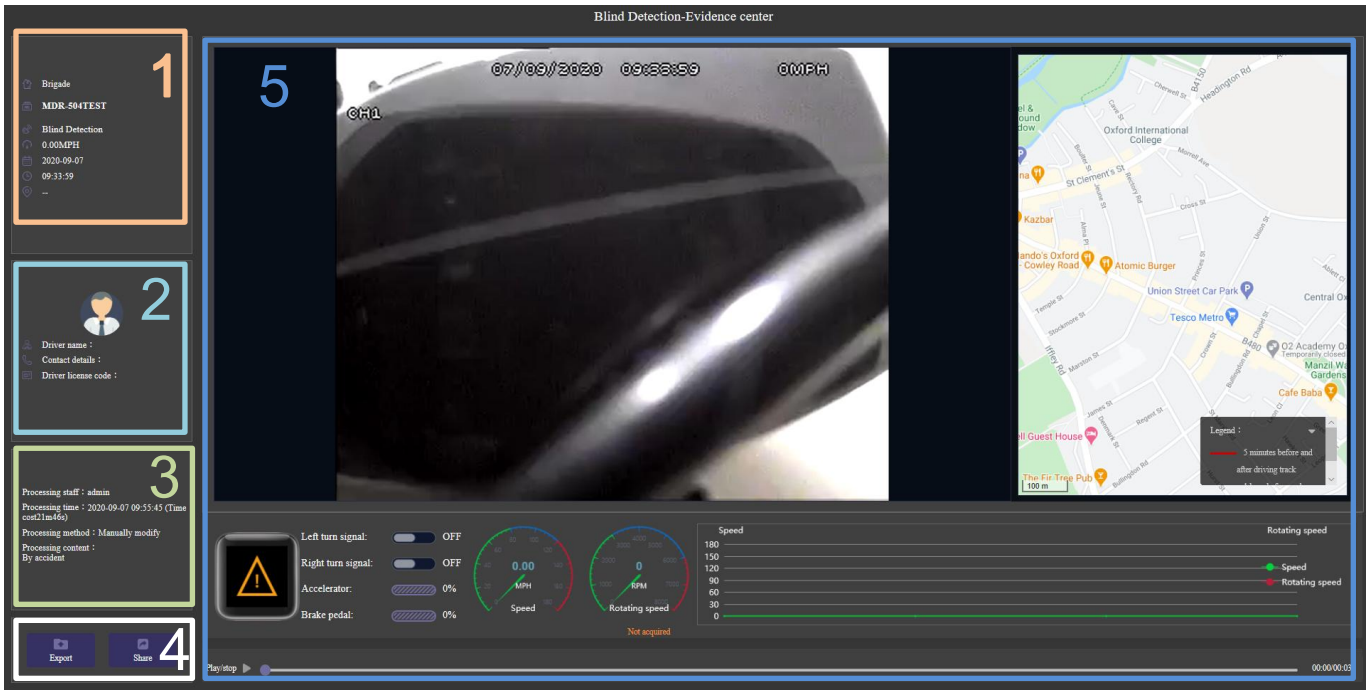
Note: The snapshot requires 1) Tick the snap button in MDR-Dashboard -> **Alarm**; 2) enable **Alarm Snap** in **Alarm Linkage Setup** in device OSD.



Evidence Export Content Figure 181

6.2.7.3 Browse Evidence

Clicking on each evidence card will redirect to a web page that displays the evidence information fully. See *Evidence Detail Page Figure 182*



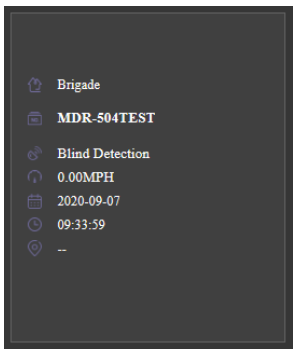
Evidence Detail Page Figure 182

The Evidence detail web page is sub-divided into several numbered areas as illustrated in *Evidence Detail Page Figure 182:*

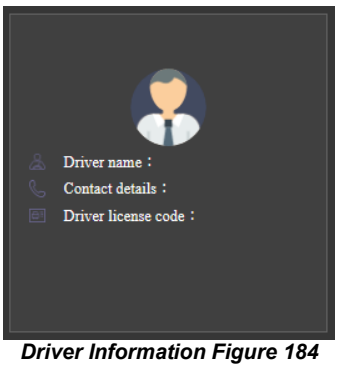
1. Vehicle Information
2. Driver Information
3. Alarm Process Status
4. Evidence Operations
5. Playback Panel

Vehicle Information detail see *Vehicle Information Figure 183.* From top to bottom is: Fleet, Vehicle Registration, Alarm Type, Speed, Evidence Date and Time and Location.

Driver Information as shown in *Driver Information Figure 184.* **Driver name**, **Contact details** (phone numbers) and **Driver license code** can be set in System Management -> Vehicle. It will be explained in detail in Chapter *0*



Vehicle Information Figure 183



Driver Information Figure 184

Driver File

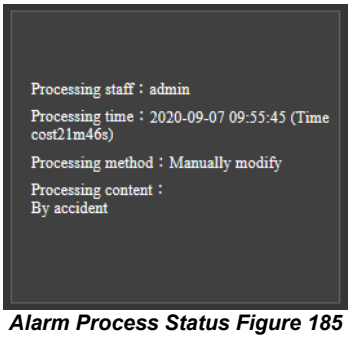
Alarm Process Status as shown in *Alarm Process Status Figure 185*.

Process staff logs operator's login name.

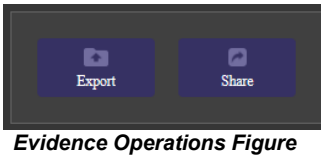
Processing time indicates when the alarm has been processed, the information in brackets shows the time difference between Evidence time and process time.

Processing method represents how the operator handled the alarm.

Processing content displays the description the operator inserted when they processed the alarm.



Alarm Process Status Figure 185



Evidence Operations Figure 186

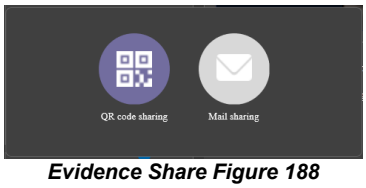
Evidence Operations contains two methods, Export and Share as shown in *Evidence Operations Figure 186*.

Export allows the evidence pack to be saved to the local computer. The evidence packs contains snapshots, .mp4 video and an evidence report in excel format.

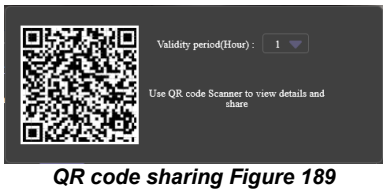
Evidence Pack Export Figure 187

Share contains **QR code sharing** and **Mail sharing**.

QR code sharing generates a new QR code when the web page is refreshed. The user can define its validity period, 1, 6, 12 or 24 hours. If the code expires, the user will be unable to open the web page when scanning the QR code. See *QR code sharing Figure 189*.



Evidence Share Figure 188

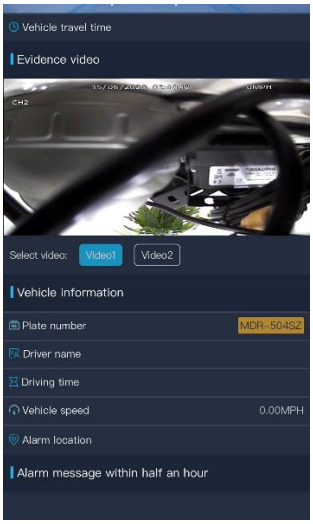


QR code sharing Figure 189

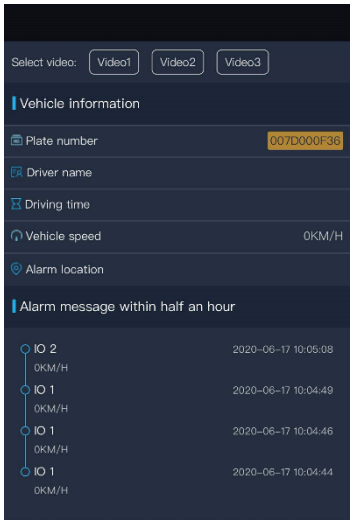
After scanning the QR code with a mobile phone or tablet, it opens a web page see QR Code Share-1 Figure 190.

The information displayed in the mobile web page is different to the computer web page. It includes Video Playback (without control panel); Certain vehicle information such as Vehicle registration and driver name etc.

At the bottom, is a list that shows all alarms that have occurred within half an hour, to give the user a general impression.



QR Code Share-1 Figure 190



QR Code Share-2 Figure 191

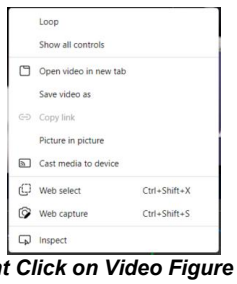
Mail Sharing allows the user to send a current Evidence web page link to specified email accounts. For multiple recipients use ";" to separate each account. The link will be effective for 1, 6, 12, 24 hours as set here. See *Mail sharing Figure 192*.

Note: To enable Mail Sharing you need to setup the mail setting in System Management first. For details see *Chapter 6.7.7.5*

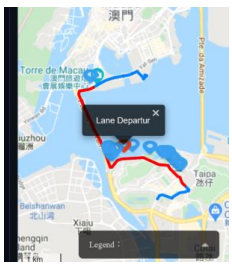
Mail sharing Figure 192

Playback Panel consists of **Loop** and **Save video as**, which allows users to save the current playing video into local computer as .mp4.

On the Map, the tracking will show in 2 colours:
Red represents 5 minutes before and after the alarm happens.
Blue represents an hour before and after the alarm happens.
See *Map Tracking Figure 194*.

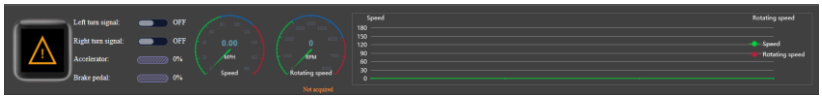


Right Click on Video Figure 193



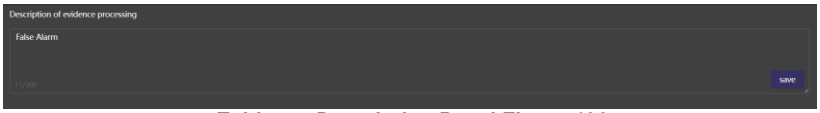
Map Tracking Figure 194

Information Panel reserved for future feature integration, currently not in use (except for Speed).



Information Panel Figure 195

At the bottom of the **Evidence** page, there's an editable block for inputting remarks for this evidence. The remark will be saved for each individual evidence item and available to view when a user opens it.



Evidence Description Panel Figure 196

6.3 Message Centre (Area 3)

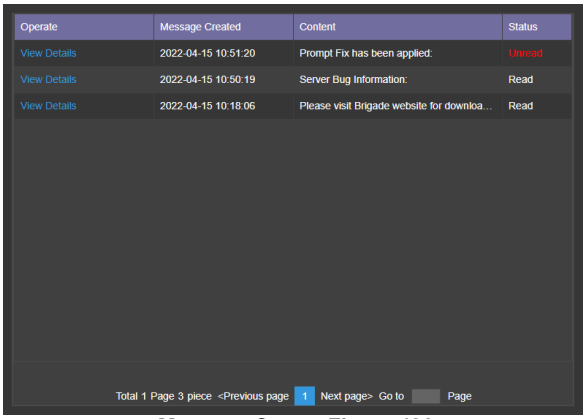
Message Centre is an interface for users to view Sever operators distributed messages. This feature usually is used for notifying server emergency issues or announcing software news to end users. This is a Server / Client feature, not related to device operations.

MDR-Dashboard users can receive broadcast messages from a server operator (who has admin rights), usually those messages are instant and a red dot with number of messages will appear on the icon when it comes in.

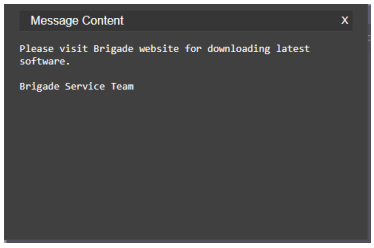
Opening the **Message Centre** window will allow users to see the message list with more details of when this has been distributed and whether it has been read or not.

Click on the **View Details** to open a sub-window to display the full content of that message. Once read, the status will switch from **Unread** to **Read**.

Usually, messages have a validity period and will be automatically deleted after a certain period of time. As shown in Chapter 6.7.7.9 Message Broadcast Setup.



Message Centre Figure 198



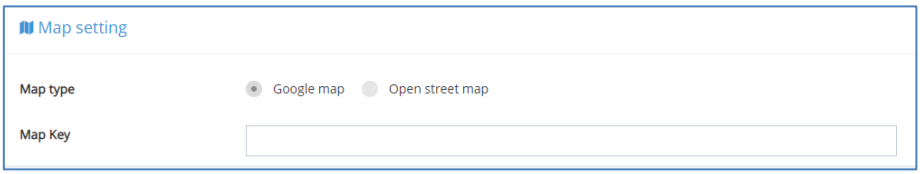
Message Content Figure 197

6.4 Fleet Status

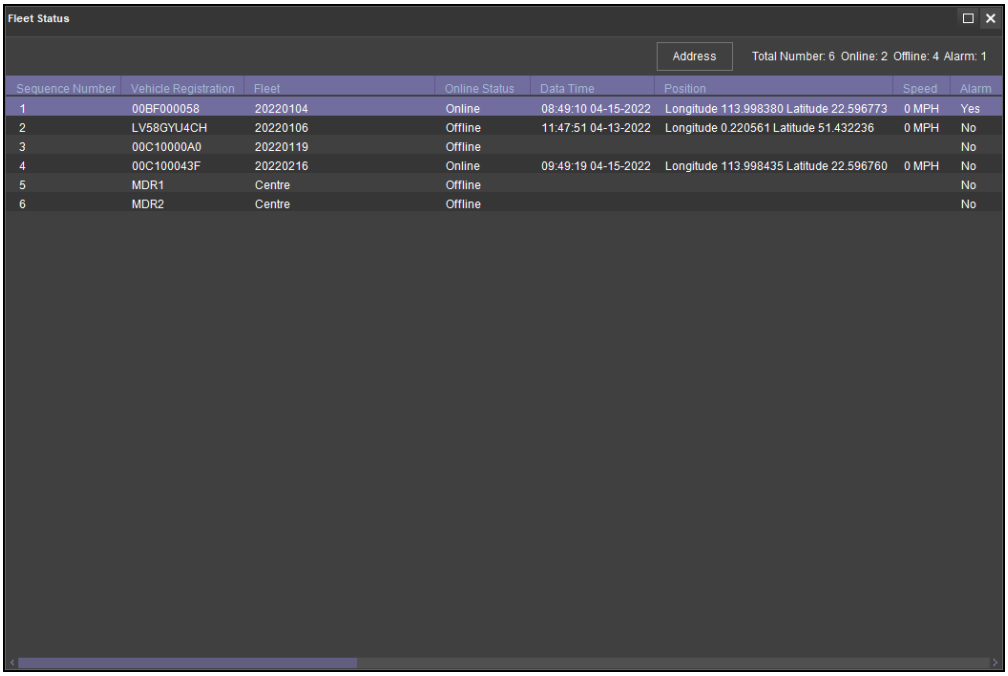
Fleet Status displays all vehicles in the server with direct information for online status, GPS position, speed and alarm. This feature is different from a traditional vehicle fleet, which mainly works for users that are trying to find information for a specific vehicle with confirmed registration details or serial number. **Fleet Status** gives a rough image of all vehicles, it benefits fleet management to spot or find abnormal cases. For example, Vehicles showing offline during working hours, vehicles traveling at high speeds, vehicles with no GPS location, etc.

There is a summary at the top right corner. This gives a general impression and an **Address** button to resolve GPS data into actual address info.

Note: If the Address button gives the error "The query fails", then please make sure a valid Google Map Key is inputted in Web Dashboard Config page.



Google Map Key Figure 199

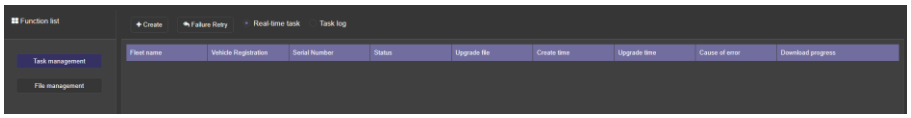


Fleet Status Window Figure 200

6.5 MDR Upgrade

This area is used to setup **UPGRADES** for devices.

Click on the button opens a web page for detailed configuration.



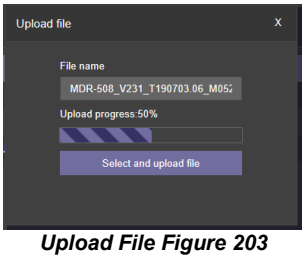
Catalogue Management Figure 201

Click File management to upload upgraded firmware. See *File Management Figure 202*. Previously uploaded files can be searched by their name or MD5 value. It supports upgrade of MDR firmware and the config file.

File Management Figure 202

Note: The capability to upgrade firmware versions and config files depends on the model and firmware version of the device. Currently only MDR 600 series support this feature.

Click Upload file which will open the window displayed in *Upload File Figure 203*. The upgrade file must be located on the local PC. Choose your firmware / Config file, once completed, the file shows up in the file list.



Upload File Figure 203

For managing uploaded files, they can be deleted by singularly or multi-select files first then click at the top right corner to perform batch delete.

Click Task management goes to manage upgrade tasks. This will display the *Batch Upgrade Equipment Figure 205* window.

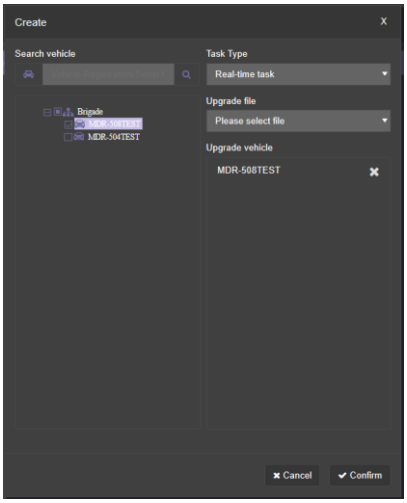
Click + Create to create a new upgrade task. Select the wanted vehicle/s from the list on the left by ticking the corresponding box. Make sure selected vehicles are applicable for the same upgrade file.

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

Choose the **Upgrade file** from the drop-down list.

To begin the task, highlight the task and then click ✔ Confirm. The task will begin automatically. **Real-time task** will execute immediately after issuing the task. **Shutdown task** will send the command to the device and wait until it enters Shutdown Delay period to execute the upgrade. **Reservation task** will be executed on the exact set time.

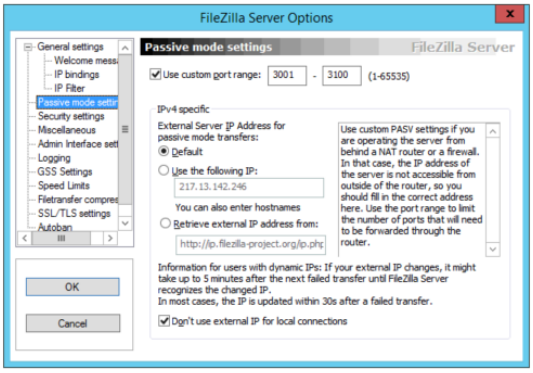
If a task(s) fails due to a bad network connection, once a connection has been re-established, click Failure Retry to retry all failed tasks.



Batch Upgrade Equipment Figure 205

When a task begins, the device will download the upgrade file in the background. Once it completes, the hardware upgrade process will execute automatically.

Note: if the upgrade cannot be completed successfully, make sure all FTP service ports have been mapped correctly. If re-mapping does not rectify the issue then this may be caused by the local network firewall strategy. Please follow the steps below for troubleshooting. Please follow steps below to troubleshoot.
1. Go to MDR Server Control Software to stop the FTP Service first.
2. Go to C:\Program Files (x86)\MDR Server 6.0\FtpServer and click the application named “FileZilla Server Interface”
3. Go to Edit->Settings->Passive mode setting, choose the mode as default, click OK to save the setting, then restart the FTP service and the remote upgrade feature should work.



FileZilla Server Setting Figure 204

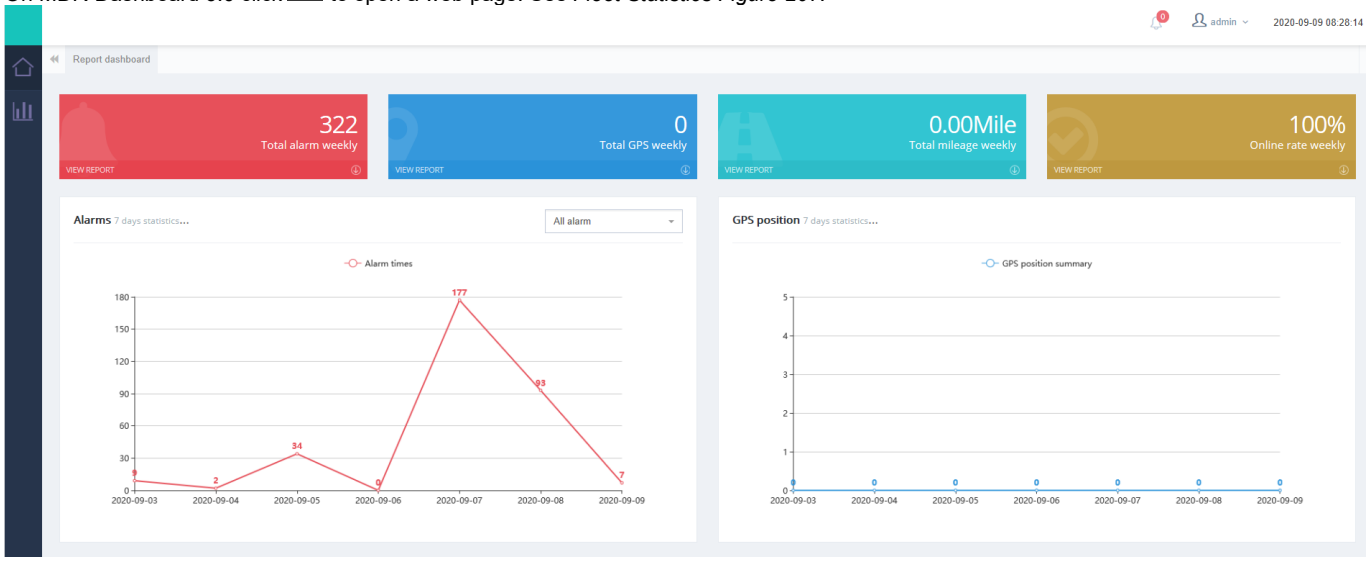
Fleet name	Vehicle Registration	Serial Number	Status	Upgrade file	Message Created	Upgrade time	Cause of error	Download progress
20220104	00BF000058	00BF000058	Downloading file	MDR644~1.2_R	2022-04-18 04:15:21	-	-	31%
20220216	00C100043F	00C100043F	Downloading file	MDR641_M04.52 6_V3.4.7.1_R220 11405	2022-04-18 04:15:21	-	-	32%

Upgrading Figure 206

6.6 Fleet Statistics

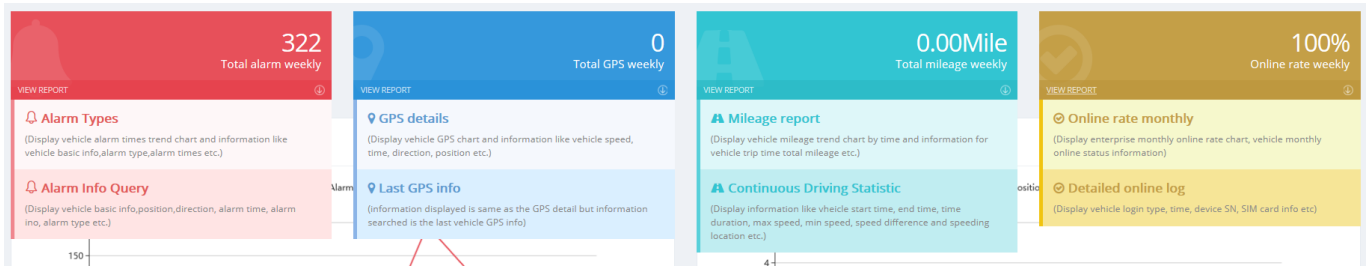
This feature provides multiple statistics for fleet management daily uses.

On MDR-Dashboard 6.0 click  to open a web page. See *Fleet Statistics Figure 207.*



Fleet Statistics Figure 207

The main dashboard shows the 4 most important figures including alarm, GPS info, Mileage and Online rate in the past 7 days. Each figure also has a graph to illustrate the trend. If you click the drop-down arrow on each figure, it will show 2 more sub-figures for quick access. These reports are also available from the left panel.



Fleet Statistics – Sub Menus Figure 208

Users can access all available reports/statistics from the left side menu, to show these, click the  button. Each alarm below can be searched by day/s, week/s or a user-defined period.

GPS position statistics includes 'GPS position Statistics report' and 'GPS details Report'. GPS position Statistics report provides the total number of GPS data collected in a period for a fleet and GPS details Report gives detailed speed, location, and direction information for each piece of GPS data.

Alarm statistics provide the total number of alarms, an alarm list for each vehicle and processing details for each alarm.

User operation log provides every operation for an account. Search result can be based on Web, Client and APP. Available operation including but not limited to live view, playback, alarm process, clip video, etc. Please refer to *User Operation Log Figure 213*.

Overspeed Report supports setting a speed limit value and searches all vehicles in the server database to find vehicles that have exceeded this limit. These search results include both real-time and historical information saved to the server.

User Online/Offline Report provides every account login and logout details, including login IP, Time, Source (login to web or client), etc.

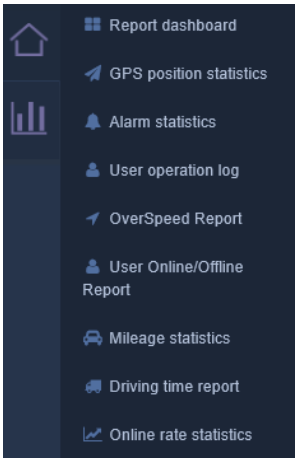
Mileage Statistics provides daily total mileage for each vehicle.

Driving time report will allow users to access driving information based on minimum driving time and minimum speed. The report will provide all matching vehicles with detailed information. See *Driving time report Figure 217.*

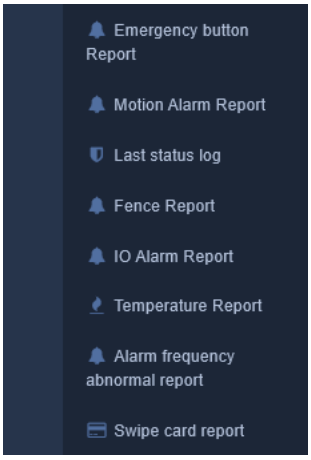
Online rate statistics gives a detailed online status log for each device, including how many days each device shows an online status and how long for.

Emergency button report, **Motion Alarm Report**, **Fence Report** (Geo-Fence), **IO Alarm Report** and **Alarm frequency abnormal report** are sub-reports of Alarm Statistics. Only user-defined alarms can be viewed.

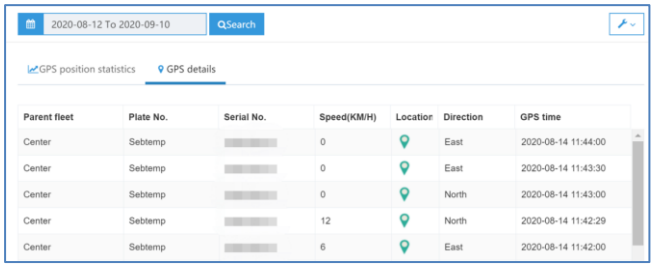
Last Status log shows the last known location of the vehicle from the latest GPS information uploaded before the device went offline, this includes related information such as registration number, speed, time, etc.
Temperature Report and **Swipe card report** are for future features, currently unused.



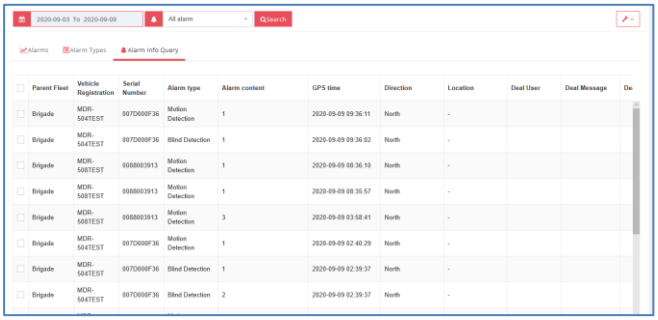
Reports-1Figure 209



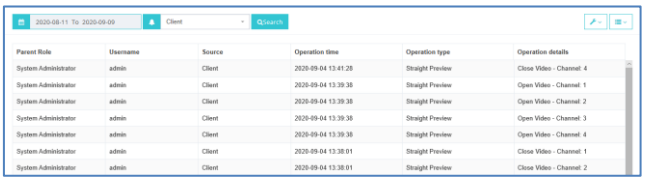
Reports-2 Figure 210



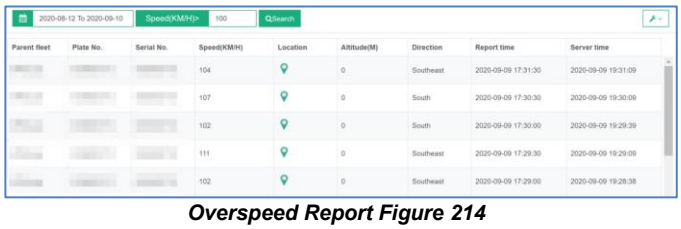
GPS Position Statistics Figure 211



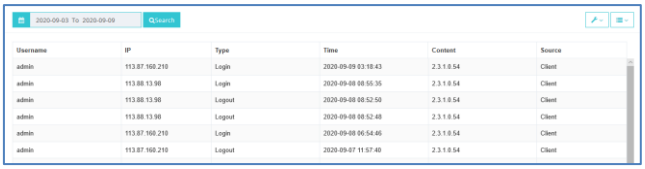
Alarm Statistics Figure 212



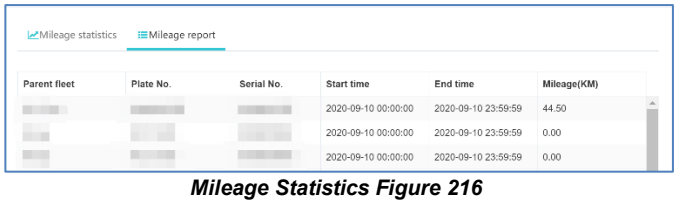
User Operation Log Figure 213



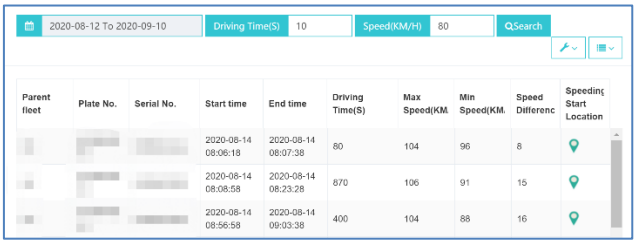
Overspeed Report Figure 214



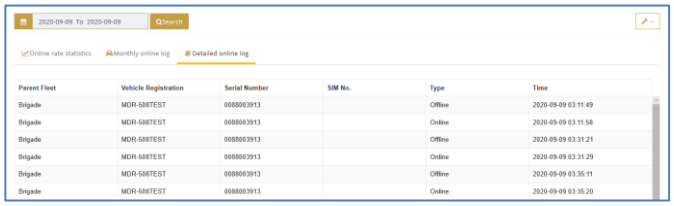
User Online/Offline Report Figure 215



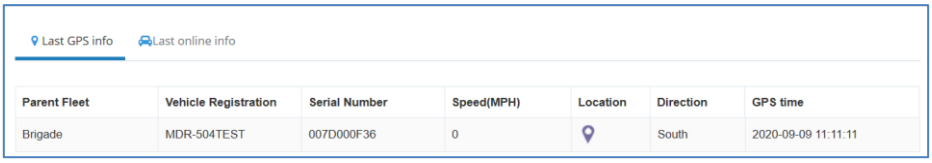
Mileage Statistics Figure 216



Driving time report Figure 217



Online Rate Statistics Figure 218



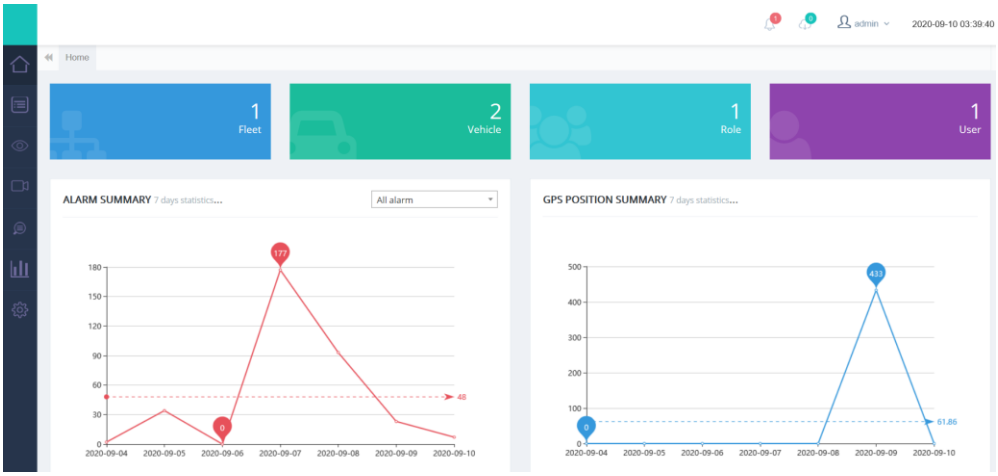
Last status log Figure 219

6.7 System Management

Browse to **SYSTEM MANAGEMENT** by clicking on the following icon  . See *System Manage Figure 220*.

System Management contains the following features:

- Home
- Fleet Management
- Live view (web)
- Playback (web)
- Evidence
- Reports
- System Configuration (web)

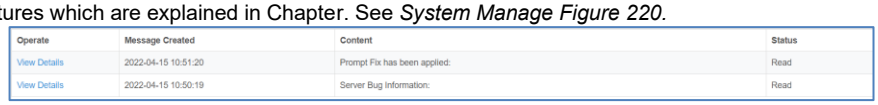


System Manage Figure 220

6.7.1 Home

Home is the start-up page when a user enters System Management. It contains 4 fields (Fleet, Vehicle, Role and User) and 2 graphs (Alarm Summary and GPS Data summary) to give an overview of the current fleet on the server. Refer to *System Manage Figure 220*.

The panel on the left allows navigation to other features which are explained in Chapter. See *System Manage Figure 220*.



Message Centre Figure 221

Click  to open **Message Centre**, which is a mirrored feature of the MDR-Dashboard client **Message Centre**, message content and status are aligned in both places, please refer to *Message Centre Figure 198* for more details.

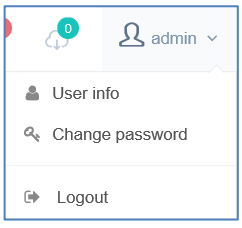
Click  to open the alarm notification window which displays previous alarms in chronological order. The time stamp corresponds to the device time, see

Alarm Notification Figure ***222*** shows an example of MDR-508TEST in a different time zone, even though the alarms occurred seconds ago, the window shows this as 1 hour ago.

Note: This list will be cleared after the web page is closed.

Click Details to open an alarm statistic report. Please refer to *Chapter 6.6 Fleet Statistics* for more details.

Alarm Notification Figure 222

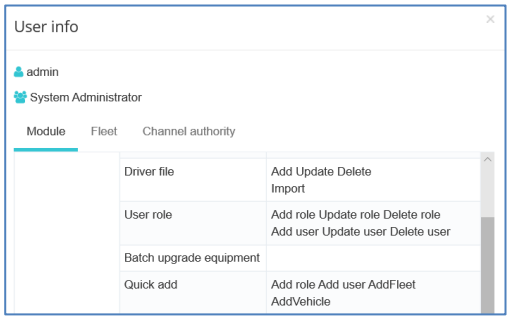


Login Details Figure 223

Click to open the footage download window. Please refer to *Chapter 0*

Playback (web-based browser) for more information.

admin allows account operations, such as change password and logout. It also supports opening the current user profile to view its authority information. See *User Info Figure 224.*



User Info Figure 224

6.7.2 Fleet Management

This area is used to configure fleet details. See Fleet Management Figure 226.

6.7.2.1 Quick Add

This feature especially benefits newly setup servers as it connects all necessary setups together in one go. Starting from adding a new fleet → adding a new vehicle → adding a role → adding new users. See *Quick Add Figure 227.*

Add fleet Create a new fleet by typing in the fleet name and chosing its parent Fleet, this works for multi-layer fleets.

Add vehicle To add a new vehicle by inputting **Vehicle Registration**, it supports up to 50 characters.

Serial number must match the serial number shown in firmware as it is the unique identifier for each device.

Number of Channel needs to input the correct numbers for each device. For e.g., MDR-641 supports 5 channels (4x analogue + 1x IP); MDR-644 supports 12 channels in total (4x analogue + 8x IP). If the correct number is not filled in, it will limit the number of channels to open in Live view.

Parent fleet to define which fleet to put this vehicle into. See *Add Vehicle Figure 228* for more details.

Under Quick Add, fleet and vehicle are mandatory to add, role and user are optional. After adding a vehicle, user can choose to continue setup of a new role by ticking this **Add Role** box. See *Add Vehicle Figure 228.*

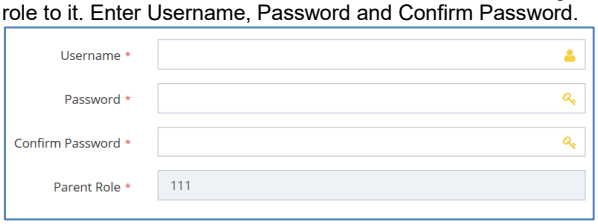
Add role allows for profiles to be assigned to one or more user accounts.

By adding a new role, user needs to create a **Role Name** and configure its **Authority** rights.

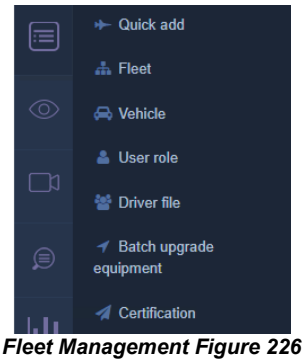
Parent Role defines what authorities can be assigned to roles under it.

Authority consists of two parts: Module and Fleet. **Module** includes feature authority such as Live view, Playback, Alarm Process, etc. **Fleet** defines which fleet is under control of this role.

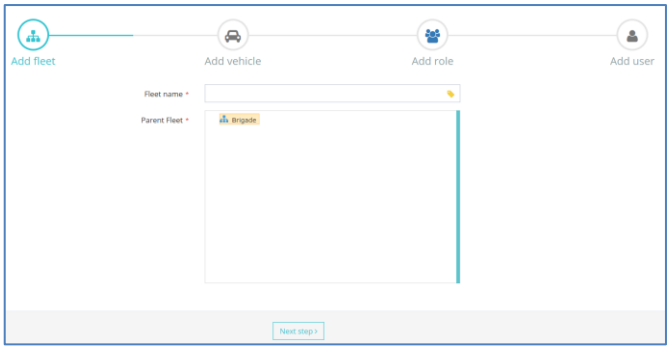
Add user Add User is used to create a new account and assign a role to it. Enter Username, Password and Confirm Password.



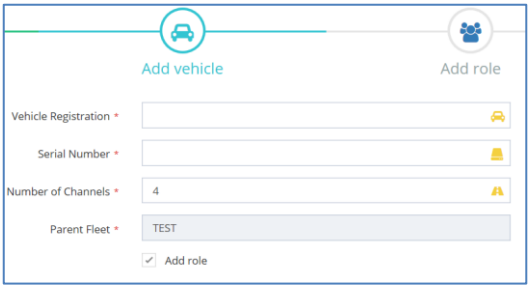
Add User Figure 225



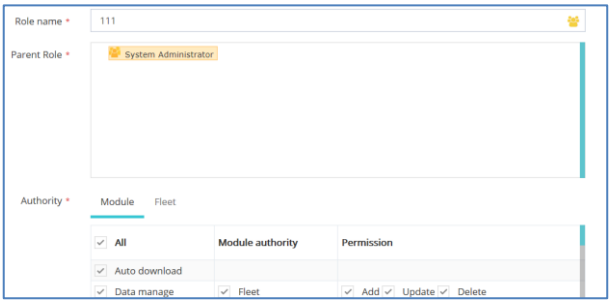
Fleet Management Figure 226



Quick Add Figure 227



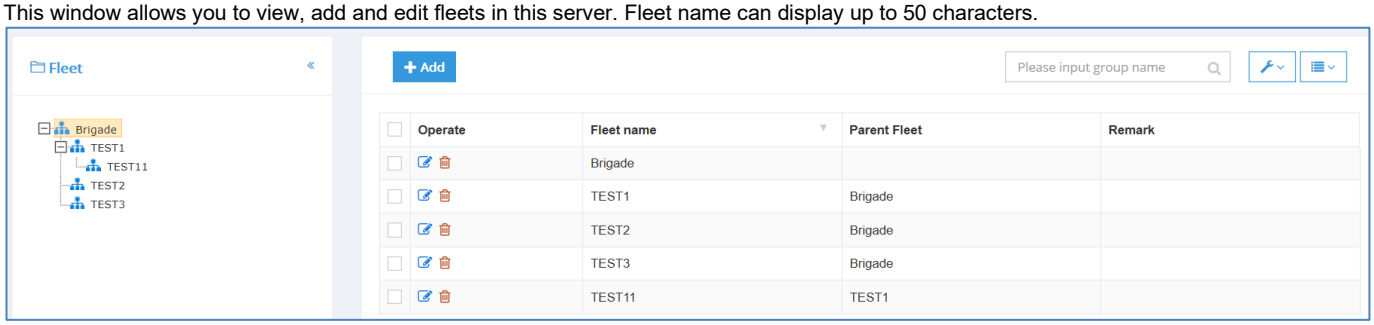
Add Vehicle Figure 228



Add Role Figure 229

6.7.2.2 Fleet

This window allows you to view, add and edit fleets in this server. Fleet name can display up to 50 characters.



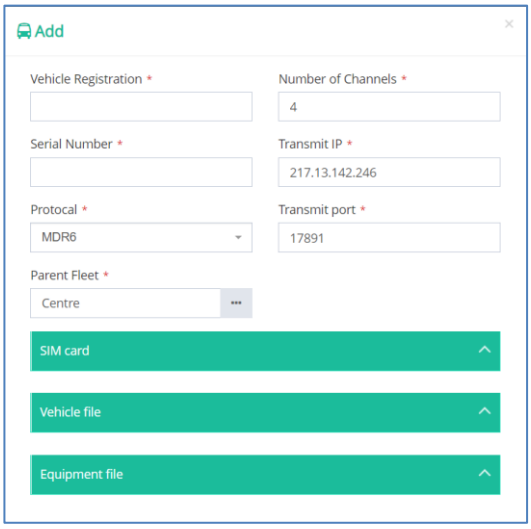
Add Fleet Figure 230

6.7.2.3 Vehicle

This area gives the vehicle information and provides operations such as adding and editing existing vehicles.

Click on different fleets to reveal the vehicle list associated with it.

A vehicle can be added by clicking + Add. The user can then input the **Vehicle Registration** number.



Add Vehicle Figure 231

Serial number must be the same as the serial number on the firmware.

Protocol is MDR6 by default, other options are MDR5 (for MDR 500 Series), MDR (for MDR 400 Series) and unknown (for future use).

Assign the vehicle to the right fleet and type in the correct **Number of Channels**, this will define the number of channels to open in Live view.

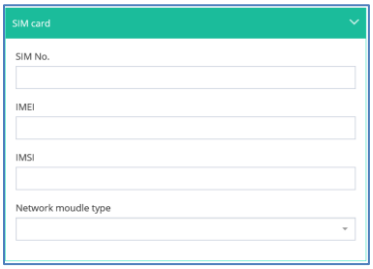
Transmit IP and **Transmit Port** are auto-detected, please do not change it manually.

After finishing the configuration explained above, the new device should be shown in the MDR-Dashboard 6.0 software.

There are some extra optional fields for vehicles, users can fill them in as needed.

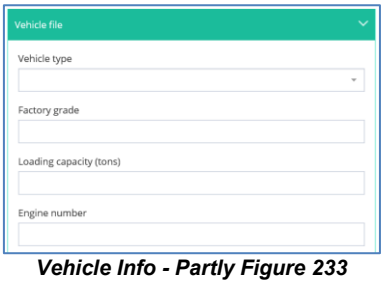
Note: These fields are to record information purpose only, they are not related to any operational features.

SIM Card section allows the input of details for SIM No., IMEI, IMSI and Network module type. See *SIM card Info Figure 232* for more details.



SIM card Info Figure 232

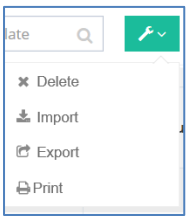
Vehicle file section includes additional fields for inputting additional vehicle information such as Vehicle type, Chassis number, Fuel type, Fuel consumption etc.



Vehicle Info - Partly Figure 233

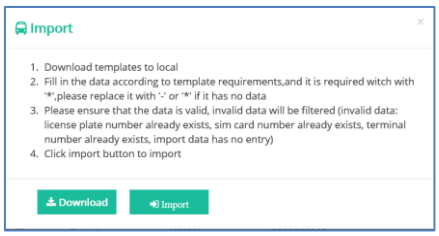
Equipment file consists of device information. Including Device name and password, installer and description etc.

Adding a vehicle is also supported by the batch import function from an excel spreadsheet. See *Import Vehicles Figure 234*.



Import Vehicles Figure 234

Click on **Import** to get instructions and download a template.



Import Vehicles Instruction Figure 235

Note:

1. Make sure to use "*" or "-" to fill in all cells if there is no actual data or it will cause import failure.

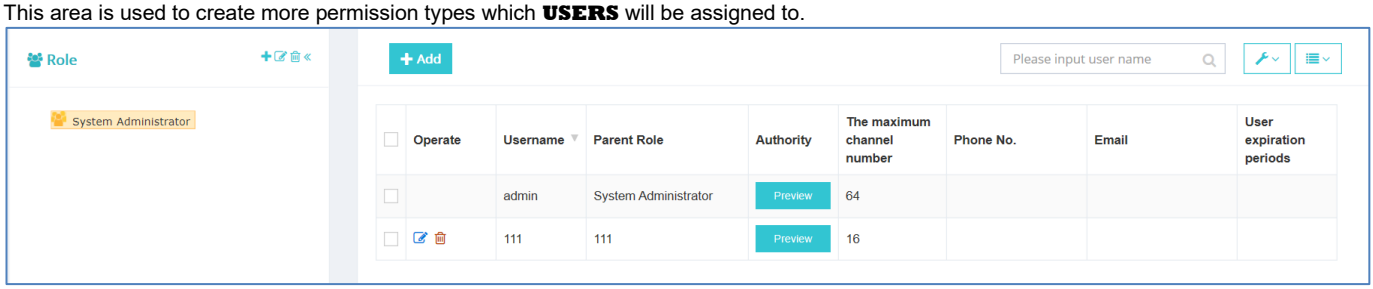
2. A fleet must already be set up on the server. See example below.

Parent fleet(*)	Plate No.(*)	Serial No.(*)	Protocal(*)[MDR5/MDR/unknown]	Channels(*)	Device username	Device password	Vehicle type	Factory grade
Brigade	WWW	0088003915	MDR5	8	admin	admin	-	-
Brigade	SSS	0088003916	MDR5	9	admin	admin	-	-
TEST1	FFF	0088003917	MDR5	10	admin	admin	-	-
TEST1	AAA	0088003918	MDR5	11	admin	admin	-	-

Import Vehicle Example Figure 236

6.7.2.4 User Role

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



User Role Figure 237

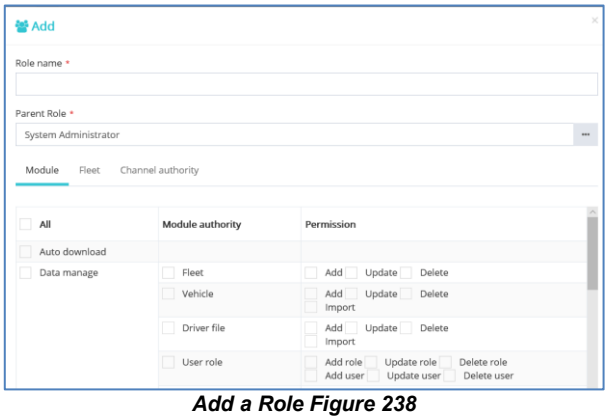
Click + ✎ 🗑 on the left to operate roles: Add, Edit and Delete.

For adding a new role, click on the + to open a configuration window. See *Add a Role Figure 238*.

Certain permissions are only accessible depending on your parent role. For example, if the parent role is the system administrator then all permissions will be available.

Each role has three aspects, **Module** includes feature authority such as Live view, Playback, Alarm Process, etc. **Fleet** defines which fleet is under control of this role, **Channel** specifies each channel of each vehicle for more precise control.

For a detailed authority list, see *Table 8 Role Permission List*.



Add a Role Figure 238

Click + Add to create a new user.

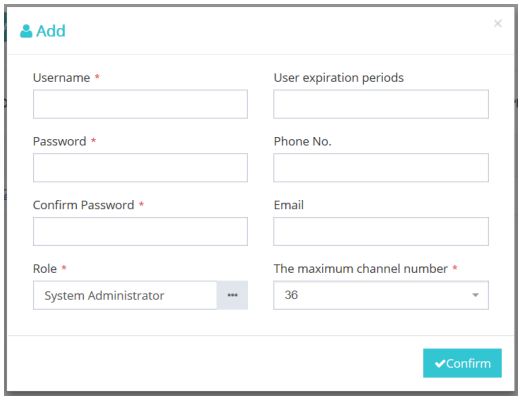
Input **Username** and **Password** accordingly, the assign the desired role on this user account.

User expiration periods can define when the account will become invalid and unable to login anymore. Leave it blank to make the account valid permanently.

Phone No. and **Email** can be filled in accordingly, these field are for information purpose only.

Maximum channel number defines how many channels will be able to be viewed simultaneously on the client MDR-Dashboard. Maximum support 64 channels.

After finishing setting up the user account, click Preview to check the account permissions.



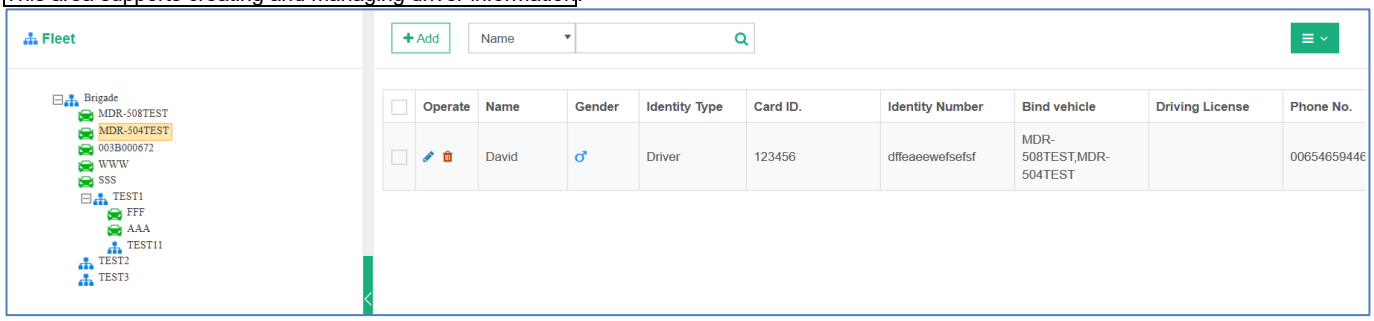
Add a User Figure 239

Table 8 Role Permission List

#	OPTIONS	OPERATING AUTHORITY	EXPLANATIONS
(1)	Automatic download	N/A	Auto download recording files
(2)	Fleet	(2.1) Add (2.2) Update (2.3) Delete	Allows the user to manage the vehicle group.
(3)	Vehicle	(3.1) Add (3.2) Update (3.3) Delete (3.4) Import	Allows the user to manage the vehicle.
(4)	Driver file	(4.1) Add (4.2) Update (4.3) Delete (4.4) Import	Allows the user to manage the driver information.
(5)	User role	(5.1) Add role (5.2) Update role (5.3) Delete role (5.4) Add user (5.5) Update user (5.6) Delete user	Allows the user to add/edit/delete Role permission and User accounts.
(6)	Batch upgrade equipment	N/A	Allows the user to manage and issue remote upgrade tasks for devices.
(7)	Quick add	N/A	Allows the user to get access to the Quick add page for operations.
(8)	System configuration (web)	Update	Allows the user to view and edit settings on web client.
(9)	Right click	(9.1) Remote Format (9.1) MDR Settings (9.3) GPS Upload Rate (9.4) Quality (9.5) Geo-Fence (9.6) Get Version (9.7) Restart (9.8) IO Settings	Allows user to manage vehicle settings by right click each vehicle on client MDR-Dashboard 6.0.
(10)	System settings	Real time preview automatically closes the video	Allows user to configure `auto-close video` option while live viewing on the client MDR-Dashboard.
(11)	Straight Preview	(11.1) Straight Video (11.2) Stream setting (11.3) Stream switch	(11.1) Allows user to be able get live view. (11.2) Allows user to right click live view channel and set up sub-stream settings (12.3) Allows user to right click live view channel to switch between main stream and sub-stream.
(12)	Alarm strategy	(12.1) MDR-Dashboard Strategy (12.2) Alarm push Strategy (12.3) Evidence download strategy	Allows user to issue different strategy for an alarm when it happens. There are 3 sections in total. They can be viewed and set in Alarm Centre in MDR-Dashboard.
(13)	Alarm query	Alarm handle	Permission to process alarms.
(14)	Intelligent retrieval	(14.1) Add (14.2) Delete (14.3) Play back	Allow users to add, delete or play back tasks for Location Search.
(15)	HDD playback	Clips	Allows user to playback video from connected HDD or SD card and make a clip of the video.
(16)	Device playback	Clips	Allows user to playback video from Online HDD and make a clip of the video.
(17)	Server playback	Clips	Allows user to playback video from MDR Server and make a clip of the video.
(18)	Local playback	Clips	Allows user to playback video from a local path and make a clip of the video.
(19)	Evidence playback	N/A	Allows user to view and playback each evidence recording.
(20)	GPS position statistics	N/A	Permission for users to open and view the report.
(21)	Alarm statistics	N/A	Permission for users to open and view the report.
(22)	User operation log	N/A	Permission for users to open and view the report.
(23)	Overspeed Report	N/A	Permission for users to open and view the report.
(24)	User Online/Offline Report	N/A	Permission for users to open and view the report.
(25)	Mileage statistics	N/A	Permission for users to open and view the report.
(26)	Driving time report	N/A	Permission for users to open and view the report.
(27)	Online rate statistics	N/A	Permission for users to open and view the report.
(28)	Emergency button Report	N/A	Permission for users to open and view the report.
(29)	Motion Alarm Report	N/A	Permission for users to open and view the report.
(30)	Last status log	N/A	Permission for users to open and view the report.
(31)	Fence Report	N/A	Permission for users to open and view the report.
(32)	IO Alarm Report	N/A	Permission for users to open and view the report.
(33)	Temperature Report	N/A	Permission for users to open and view the report.
(34)	Alarm frequency abnormal report	N/A	Permission for users to open and view the report.
(35)	Swipe card report	N/A	Permission for users to open and view the report.

6.7.2.5 Driver File

This area supports creating and managing driver information.



Driver File Figure 240

Click + Add to add a new driver.

Fill in driver information accordingly. **Identity Type** supports user definition. As shown in *Driver File Figure 240.*

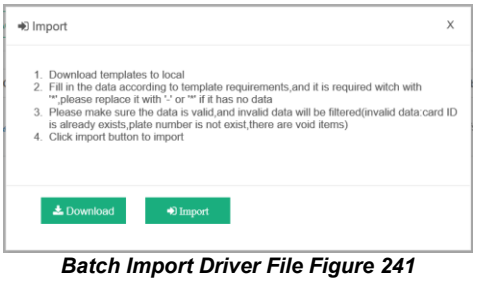
Verify and **Driver face recognition setup** currently not used, reserved for future use.

Bind vehicle assigns one or more vehicles to a driver.

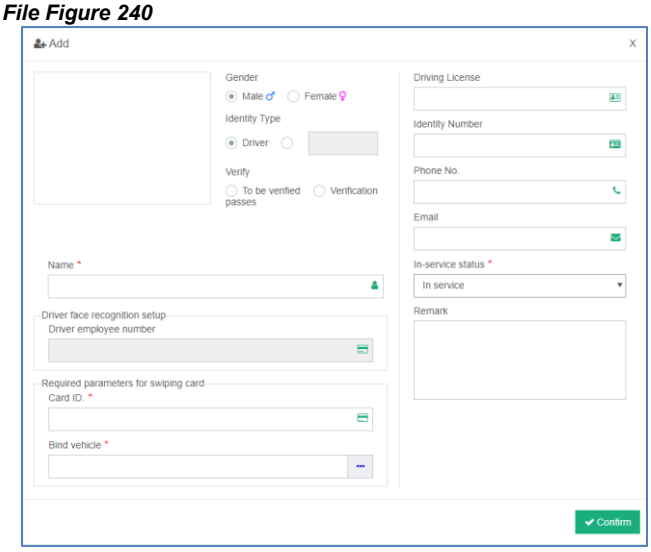
After finish the setup, click ✔ Confirm to save the driver information.

Driver file also supports batch imports, click the ≡ at the top right corner to get import instructions.

Note: Make sure to use "*" or "-" to fill in all cells if there is no actual data or it will cause import fails.



Batch Import Driver File Figure 241



Add a New Driver Figure 242

6.7.2.6 Batch upgrade equipment

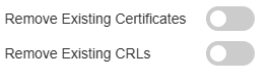
Please refer to section *6.5 MDR Upgrade.*

6.7.2.7 Certification

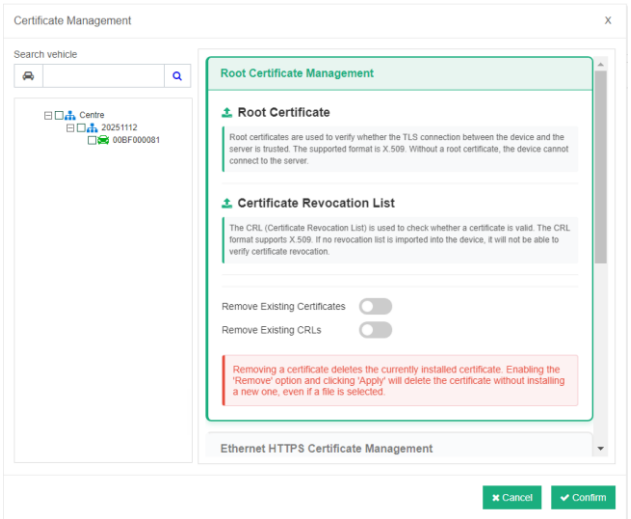
The certification enables the remote importation of the platform root certificate, revocation certificate (used for **Verify Certificate** functionality), Ethernet HTTPS certificate and its Key file, Smartcontroller TLS certificate and its key file from the platform to the device.Click + New Task and Certificate Management on the left to operate the device certificates: import or remove.

For adding a new **Root Certificate** and **Certificate Revocation List** for device, click Root Certificate and Certificate Revocation List , there will be pop-up window to ask user to import the corresponding certificates from local PC. Click the ✔ Confirm to finish the whole process.

For **Remove Existing Certificate** and **Remove Existing CRLs** on device, click the remove button to turn them as green. Click the ✔ Confirm to finish the whole process.



Remove Button Figure 243



Root Certificate Management Figure 245

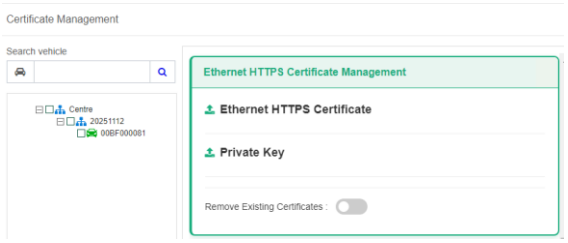
Remove Button Figure 244

For adding a new **HTTPS Certificate** and **Private Key** for device, click HTTPS Certificate and Private Key, there will be pop-up window to ask user to import the corresponding certificate and key file from local PC. Click the Confirm to finish the whole process.

For **Remove Existing Certificates** on device, click the remove button to turn them as green. Click the Confirm to finish the whole process.

Remove Button Figure 246

Remove Button Figure 247



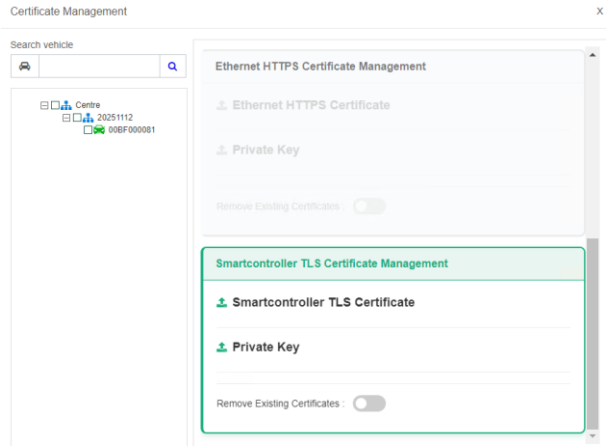
HTTPS Certificate Management Figure 248

For adding a new **HTTPS Certificate** and **Private Key** for device, click TLS Certificate and Private Key, there will be pop-up window to ask user to import the corresponding certificate and key file from local PC. Click the Confirm to finish the whole process.

For **Remove Existing Certificates** on device, click the remove button to turn them as green. Click the Confirm to finish the whole process.

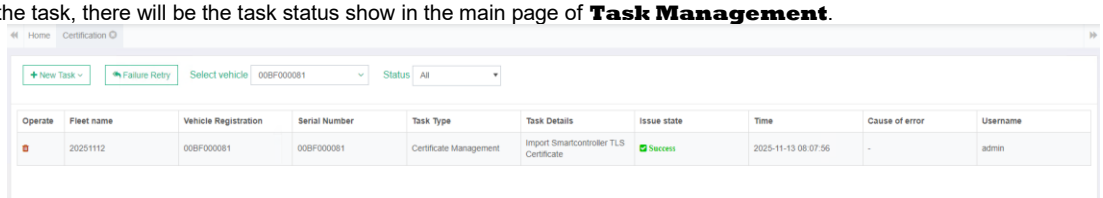
Remove Button Figure 249

Remove Button Figure 250



Smartcontroller TLS Management Figure 251

After finish the task, there will be the task status show in the main page of **Task Management**.



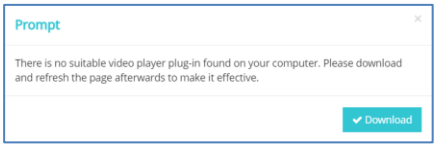
Smartcontroller TLS Management Figure 252

6.7.3 Live View (web)

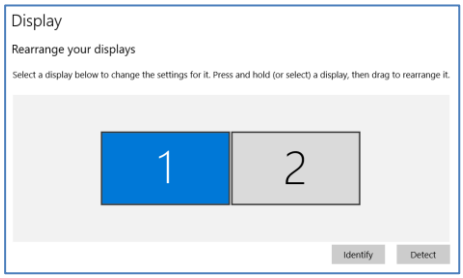
The web live view is a portable version for client MDR-Dashboard live view feature. It allows the user to have a quick view of vehicle videos when they are not using installed client software. The web live view has most of the features in the client software but is limited in certain areas.

When the web live view is opened for the first time, a prompt window will remind the user to download a proper video player plugin adapting H.264 / H.265 video formats. Once it is installed, please refresh the web page to make it effective. As shown in *No Available Player Figure 254.*

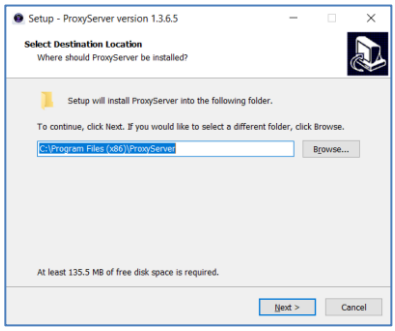
Note: if the user is using dual monitors, it may cause the live view window to display abnormally. Please make sure the computer display setup, for both monitors have the same resolution, scale and height level, as shown in *Computer Display Settings Figure 255.* Also, if the display does not work properly, please move the browser to another monitor, which may will fix the issue.



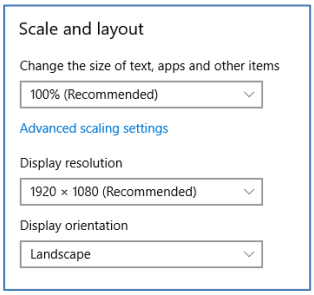
No Available Player Figure 254



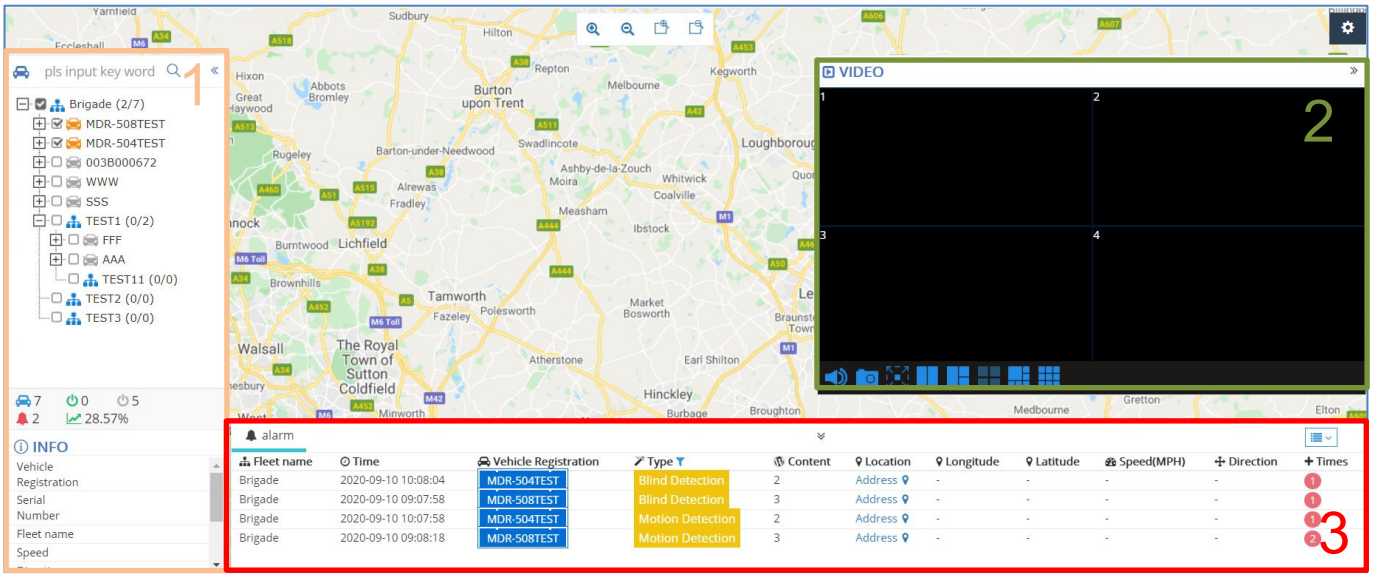
Computer Display Settings Figure 255



Install Player Plugin Figure 253



Computer Display Settings - continue Figure 256



Web Live View Figure 257

The live view interface divides into 4 parts in total:

1. **Fleet**
2. **Live view**
3. **Alarm Centre**
4. **Map**

Fleet displays all vehicles and uses icon colour to reflect its online or offline status: green for online; grey for offline and orange for alarm vehicles.

Ticking the box in front of the vehicle enables it to show up on the map. See section 1 in *Web Live View Figure 257*.

In the middle part there are 5 simple icons to reflect:

Total vehicle amount in the server.

Current online vehicles.

Current offline vehicle.

Current active alarms.

Current online rates.

Info tab includes quick information for selected vehicle, detail see *Vehicle Info Tab Figure 258*.

Live view is a floating window on the map, which can be dragged and dropped in different places. Double click the vehicle to turn on live view. While viewing the device channels using the mouse, click on one channel to hear its audio output.

Right clicking on a live view channel enables streaming setup, the same as the client MDR-Dashboard.

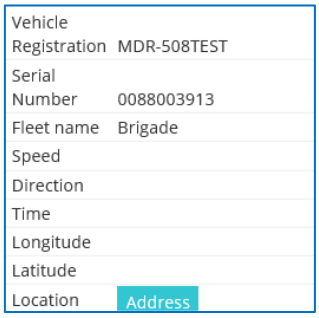
The live view control panel contains buttons such as:

For audio on/off

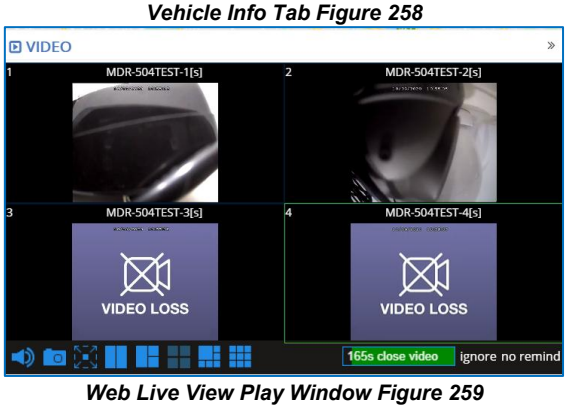
For taking snapshots of a single channel

For full screen mode

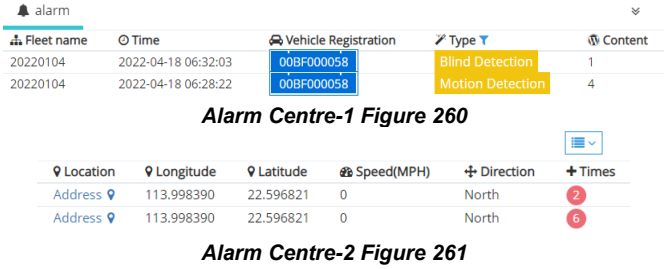
For changing channel layouts.



Vehicle Info Tab Figure 258



Web Live View Play Window Figure 259



Alarm Centre-1 Figure 260

Alarm Centre-2 Figure 261

Web live view only supports viewing a maximum of 9 channels simultaneously.

is a countdown for displaying how long the live view will continue. Click **Ignore** to re-fill the countdown bar, **no remind** is to remove the limitation and let the live view play infinitely. As shown in ***Web Live View Play Window Figure 259***.

Alarm used to display current active alarms for all online vehicles, this list will be cleared if you leave the web page. As shown in *Alarm Centre-1 Figure 260.*

Alarm list consists of multiple sub-parts. Basic information such as Fleet name, Time, Vehicle Registration, etc. Alarm related information like Alarm type and Alarm Content.

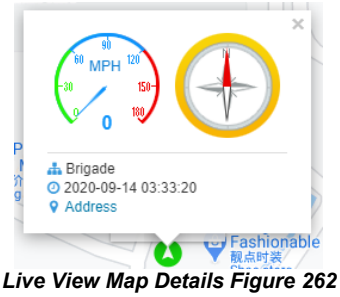
Map information like longitude, latitude and address (Click the Address to view address in text, click to display on map)

Note: Please input Google Map Key in Setting page to allow Google map convert longitude and latitude into address text, or it will show "**REQUEST_DENIED**" or "**208**" as the error code. See *Alarm Centre-2 Figure 261*. Setting sees *Chapter 6.7.7.1 Map setting.*

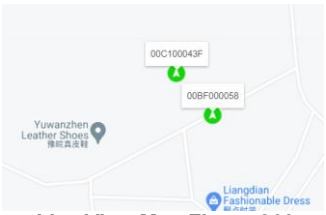
Alarm times window used to display concurrent alarms.

Map is shown in the background. By default, vehicles will have the icon and displays its vehicle registration on top, see *Live View Map Figure 263.*

If you click on the vehicle icon a floating window will show up to provide detailed vehicle driving information, such as speed, direction, GPS upload time, Address etc. See *Live View Map Details Figure 262*.



Live View Map Details Figure 262



Live View Map Figure 263

6.7.4 Playback (web-based browser)

The playback feature on a web-based browser basically is the same as Online Playback on MDR-Dashboard 6.0 client. The web feature is more flexible and benefits for a quick view.

Playback (web) Figure 264

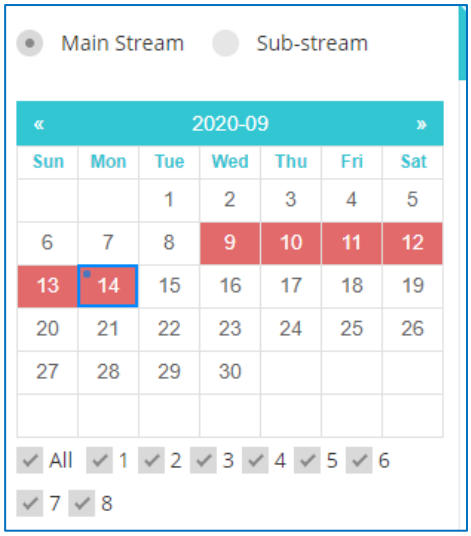
The Playback window is formed of 3 functional parts:

1. **Fleet and Calendar**
2. **Video Panel**
3. **Map**

Fleet and Calendar used to select which vehicle to playback.

User can choose to play mainstream or Sub-stream. **Main Stream** footage is saved on the main storage device and typically uses more storage capacity due to a higher resolution with a higher frame rate. **Sub-stream** footage will only be recorded if the main storage device has sub-stream recording enabled. The sub-stream footage with typically use less storage capacity due to a lower resolution and lower frame rate. Sub-stream is usually more suitable to view if the network bandwidth is limited.

Calendar view can define which date has the record. 6 A green block means that date only has normal recordings; 7 A red block means an alarm recording occurred on that date. 14 A blue dot represent metadata available on that date.



Playback (web) Calendar View Figure 265

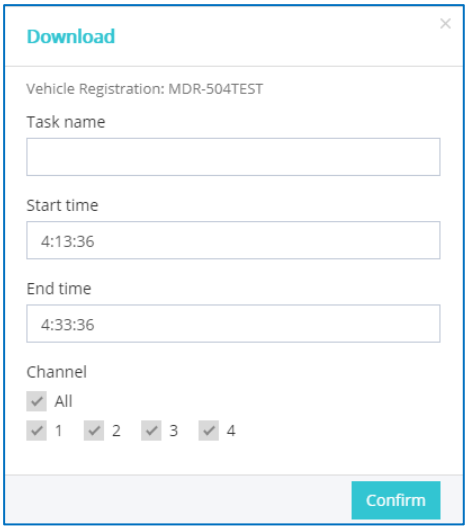
Web Playback supports a maximum of 9 channels be viewed at the same time. It is recommended that only the desired channels are selected in the bottom left of *Playback (web) Calendar View Figure 265* to minimise bandwidth usage. If more than 9 channels need to be selected for simultaneous viewing, then this will need to be done via the client software.

Video Panel displays a video window and playback controls. The video window can be double clicked to expand it to full screen.

Playing control only supports Time duration and Speed curve information. If the user wants more info about Temperature and Voltage while driving, please use the client software to view the desired information.


Play control has Play / Pause, Stop, Slow Forward, Fast Forward, Next Frame and Page Turner.

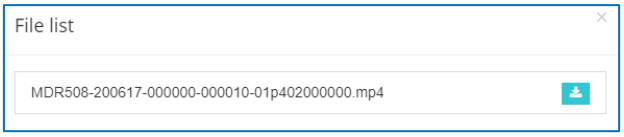
Clip used to download the footage as .mp4 format to the computer's local path. See *Playback (web) Clip Figure 267*. User can assign a task name and define the wanted period and channels to clip. After the task has been created, it will be displayed on the download centre, see *Clip Downloading Figure 268*.



Playback (web) Clip Figure 267

File List: The issued task will be downloaded and saved on the server initially. The user needs to click on 'File list' (*Clip File List Figure 266*) to view the recorded files and save them to a local computer. If the task is unable to finish and gives an error message such as "Insufficient disk space", please make sure the MDR server has enough space assigned. As shown in *Storage and Connection Options Figure 293.*

Map works the same as the client software, to show the tracking information while footage is being played back.



Clip File List Figure 266

Clip Downloading Figure 268

6.7.5 Evidence

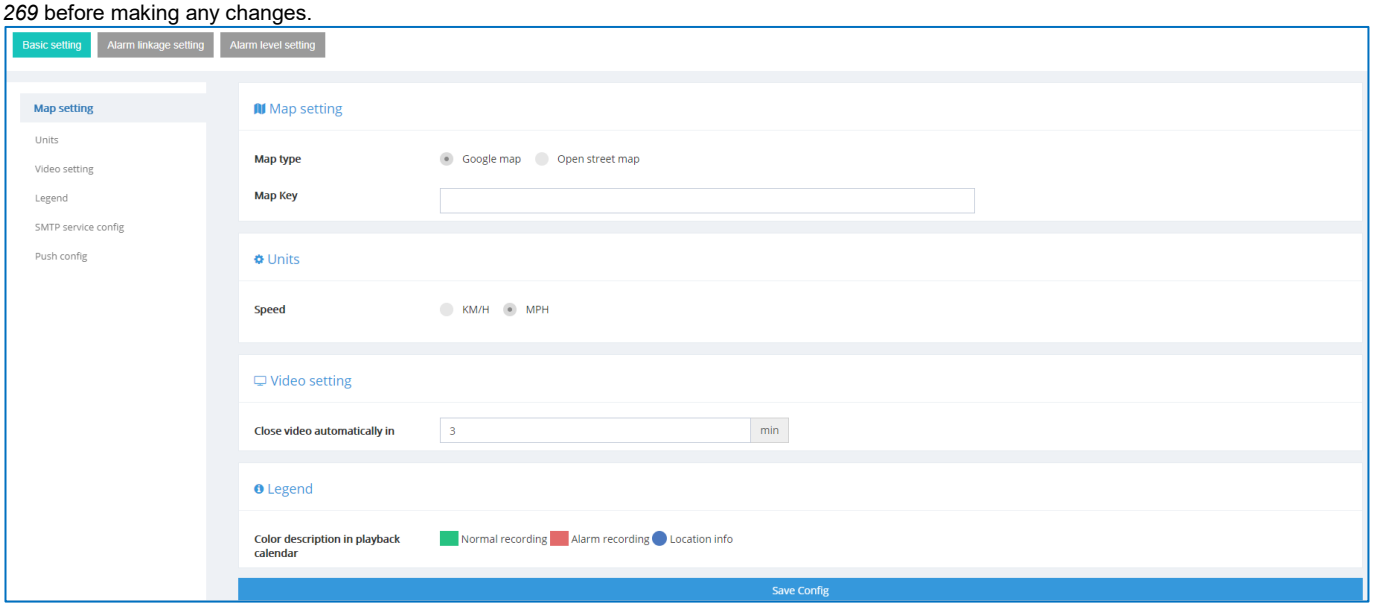
This section contains the same information as Chapter 6.2.6 Evidence. Please refer to the previous chapter for detailed information.

6.7.6 Fleet Statistics

This section contains the same information as Chapter 6.6 Fleet Statistics. Please refer to the previous chapter for detailed information.

6.7.7 System configuration (web-based browser)

This page includes various settings which have been used in the web interface. Please see the details in *System Configuration (web) Figure 269* before making any changes.



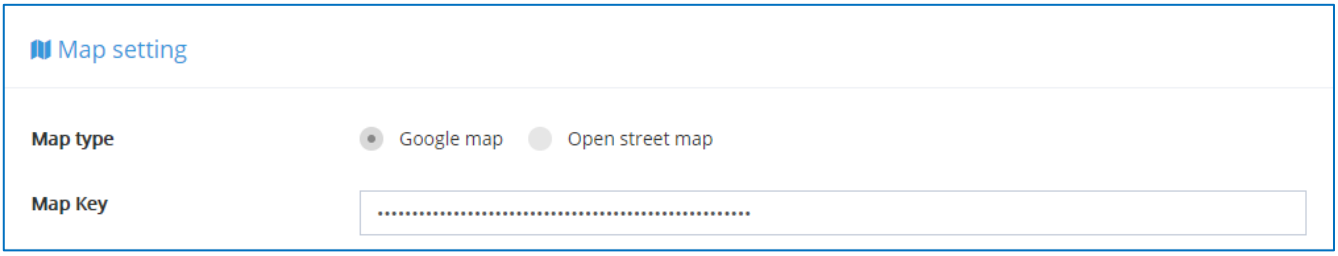
System Configuration (web) Figure 269

6.7.7.1 Map setting

This setting is only available for the web interface, not for the client MDR-Dashboard 6.0. Currently there are 2 types of maps available to display: Google Map and Open Street Map.

If user wants the address resolution feature: turning longitude and latitude to location address. Then please choose the Google Map. Also address resolution requires a Map Key, please input correct key value or it will cause address resolution to fail. Please refer to section *6.4 Fleet Status*.

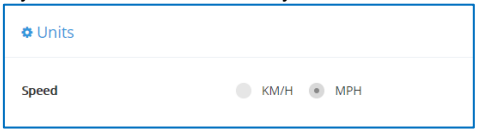
Note: Input key will display as " • " for security purposes.



Map setting Figure 270

6.7.7.2 Units

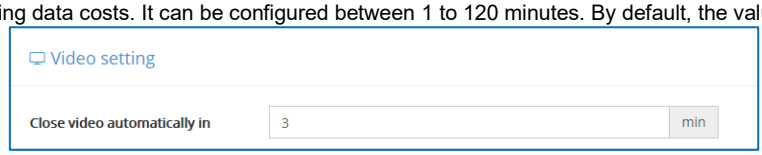
This is for setting up speed units. This setting only works for web interface. By default, it is set to "MPH".



Units Figure 271

6.7.7.3 Video setting

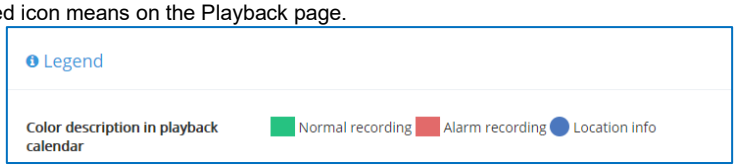
This setting will determine the length of time (in minutes) that the live view will display for before it automatically closes. This feature is designed to prevent unnecessary streaming data costs. It can be configured between 1 to 120 minutes. By default, the value is 3 minutes.



Close video automatically in Figure 272

6.7.7.4 Legend

For explaining what each coloured icon means on the Playback page.

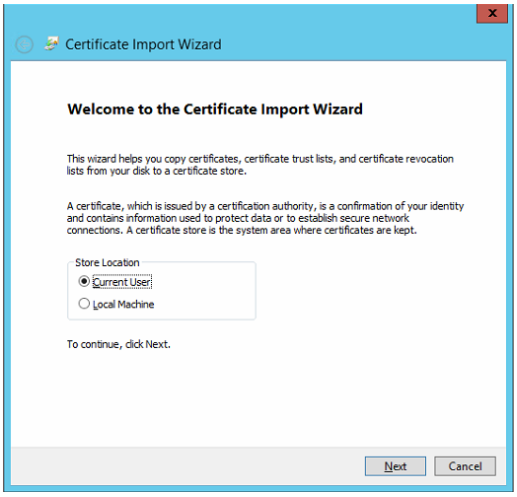


Legend Figure 273

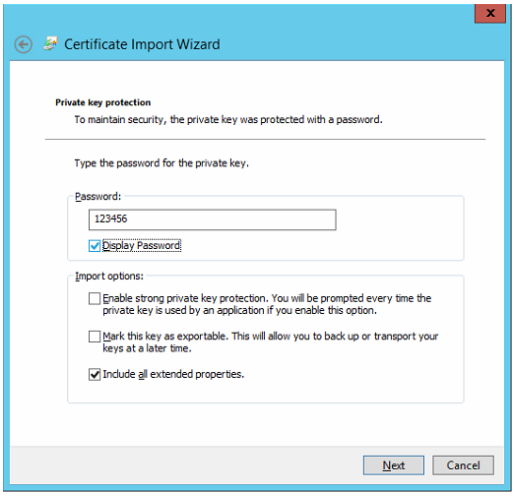
6.7.7.5 Push Config

The push config is used for the mobile app push function. When an alarm is activated, the mobile device will receive a push notification if it has been set up correctly. The push config setup is separate between iOS and Android devices.

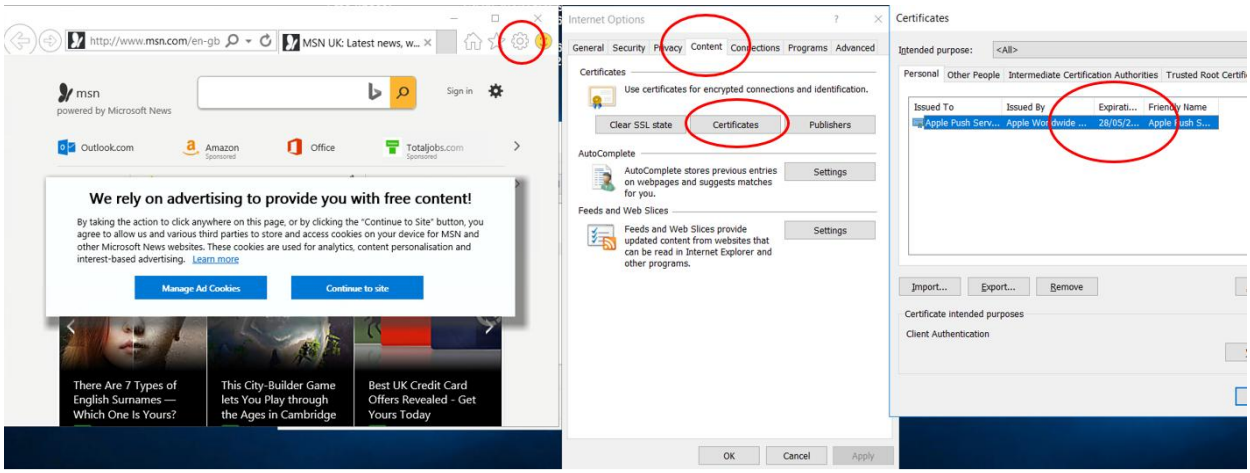
For iOS, it requires a push certificate which expires every year. Please contact your service provider if the certificate expires. To check an existing Push certificate expiration date, please locate the certificate under path: **MDR Server 6.0\WCMS5\root\system-file\config** on the Server. Double click the file and install it for the current user, as shown in *Install Push Certificate for Current User 274*. Input the password "123456" to complete the installation. After it is installed, the user can check the validity in any web browser.



Install Push Certificate for Current User 274



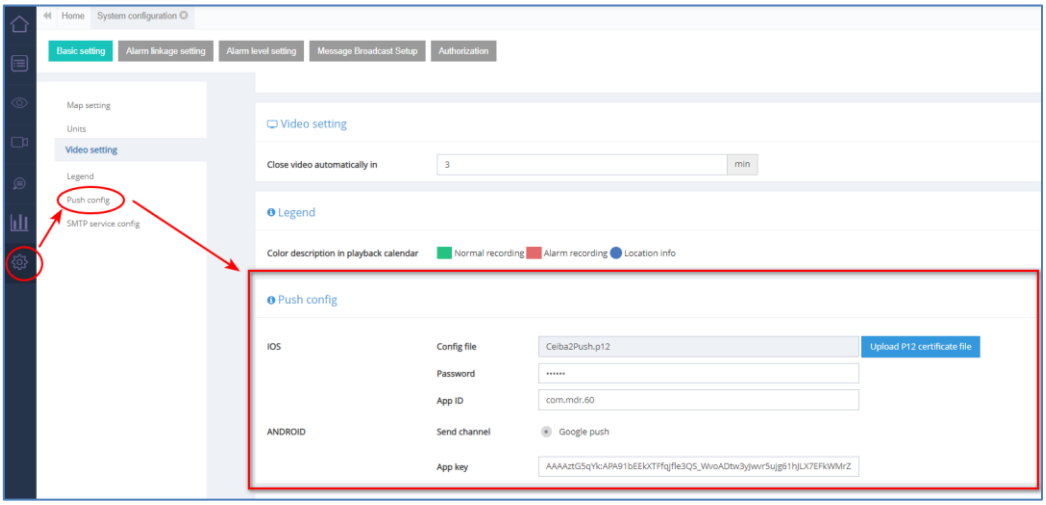
Certificate Password Figure 275



Checking Push Certificate Expiration Date through IE Figure 276

To renew the certificate, users can upload the certificate file to the Web Dashboard System configuration interface, see *Push config Figure 277****Push config Figure 277***. Please ensure the config is saved after uploading for it to come into effect.

Android uses a free Google Push key which works indefinitely. Do not change the key value manually without consulting your service provider.



Push config Figure 277

6.7.7.6 SMTP service

This section is to set up email configuration for MDR-Dashboard alarm email features.

Brigade recommends for an IT professional to setup a Microsoft Exchange account that can be used for this configuration. Ensure that this is named appropriately (MDR-Dashboard 6.0) to ensure that email alerts are clearly defined.

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:

- Sender
- Display name
- Username
- Password
- SMTP address (Simple Mail Transfer Protocol)
- SMTP port
- Subject
- Encrypt type

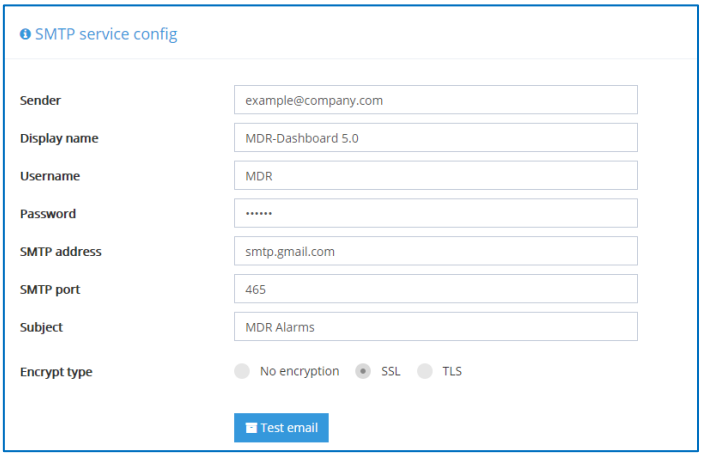
Encryption has the following: Not Encrypted, SSL (Secure Sockets Layer) and TLS (Transport Layer Security)
The configuration shown in *SMTP service config Figure 278* is for example purpose only. It may be used to send email alerts. Alternatively, you may create your own email address e.g. Company123@gmail.com.

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.

The email will contain a “Test Success” message. If the failure message (Test failed) appears, please double check the setup in *SMTP service config Figure 278*.



SMTP service config Figure 278

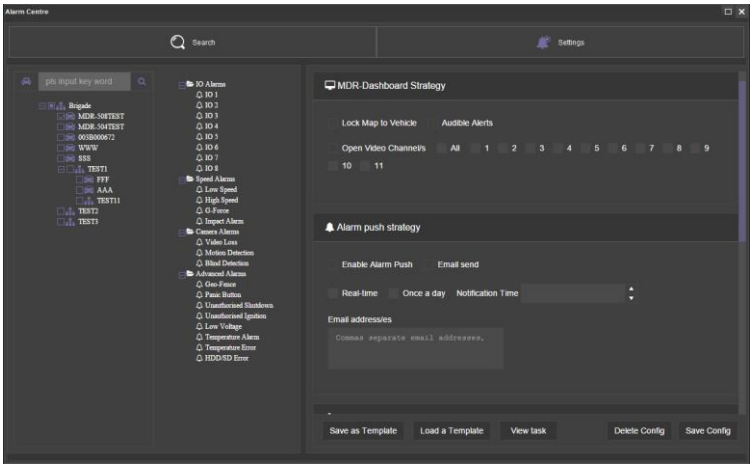
Email alerts can be set up by **ALARM QUERY** → Settings

Tick Real-time or Once a day as shown in *Alarm Notification Configuration Figure 279*

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 a once a day notification.

E-mail Address/s – enter multiple email addresses using a comma (,) to separate them

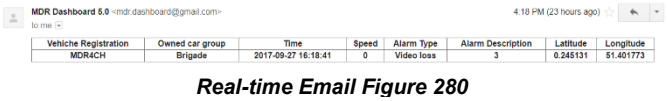


Alarm Notification Configuration Figure 279

Once the details have been correctly entered and saved via **Save Config**, the new alert will be added to the list shown in *Alarm Notification Configuration Figure 279*.

An example of the email received when using Send real-time is shown in *Real-time Email Figure 280*.

An example of the email received when using **Once a day** is shown in *Once a Day Email Figure 281*. Regularly send emails will contain alarm reports in excel spreadsheet format.



Real-time Email Figure 280

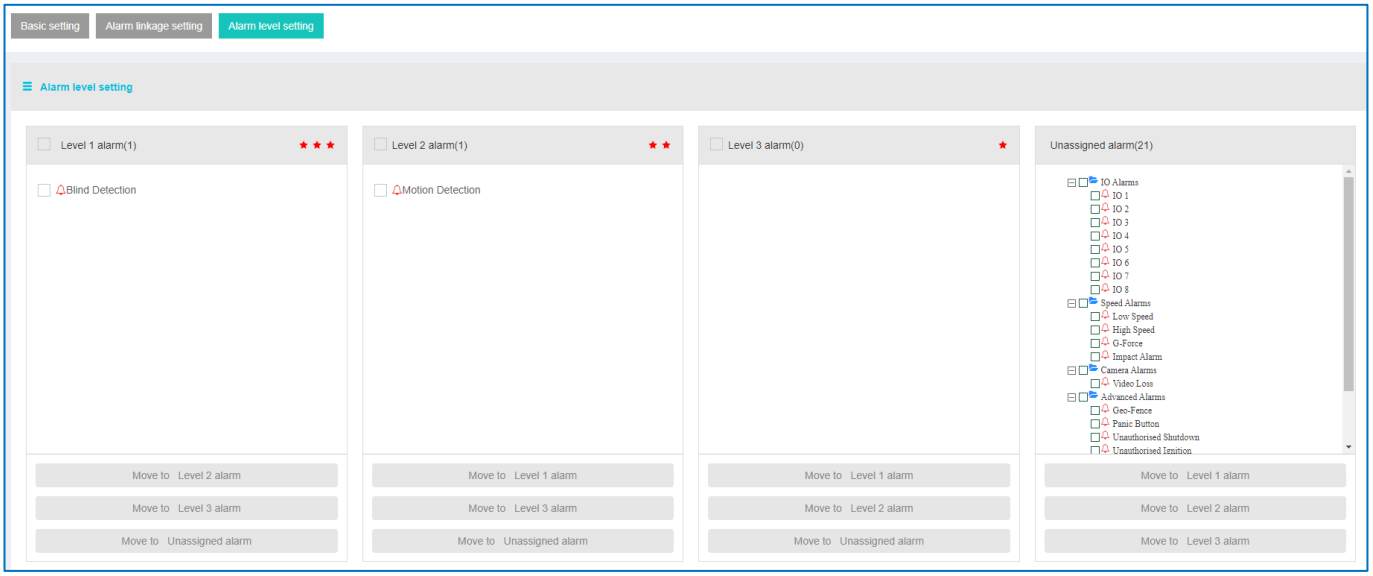
Once a Day Email Figure 281

6.7.7.7 Alarm linkage setting

This section has the same setup as 'Alarm centre' in the client MDR-Dashboard 6.0, please refer to section 6.8.2.2 for more detail.

6.7.7.8 Alarm level setting

This setting is for assigning an importance value for each alarm type. All alarms have no importance by default. Users can assign Level 1 (most important ★★★), Level 2 (Important ★★) and Level 3 (somewhat important ★) to different alarm types. This only works to show stars in Evidence centre.

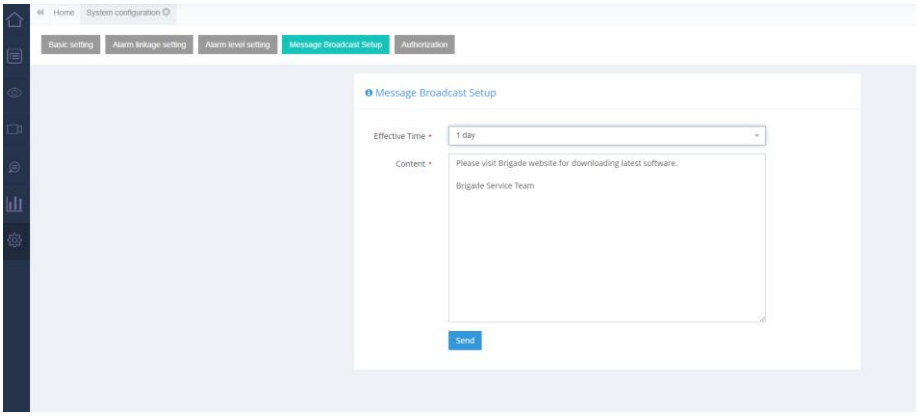


Alarm level setting Figure 282

6.7.7.9 Message Broadcast Setup

Only the **System Admin** account has message distribution authority. For achieving this, administrators need to go to the Message Broadcast Setup, as shown in *Message Broadcast Setup Figure 283*. Operators can compose a message and select a desired duration time from the drop-down list. Options are **1 day**, **7 days**, **30 days** and **90 days** (the longest). After the message has been sent, there is no method to recall or delete from MDR-Dashboard client.

After being sent, the message will be distributed to every MDR-Dashboard client and web interface users who login to the server. Previously sent messages can only be read, end users will be unable to delete message, they will expire once the desired time has lapsed.



Message Broadcast Setup Figure 283

6.7.7.10 Authorization

Only the **System Admin** accounts are able to view this setup page. For the detail usage and setup please refer to *2.4 Server Authorization.*

6.8 Downloads and Alarm

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**.

6.8.1 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 284*.

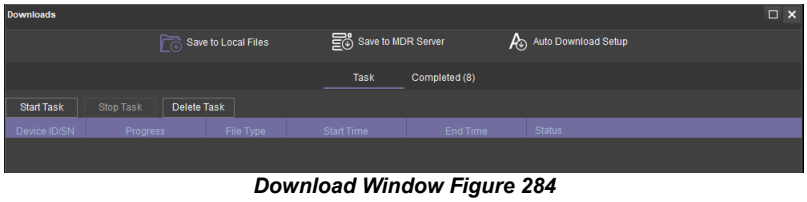
There are 3 download options: **SAVE TO LOCAL FILES**, **SAVE TO MDR SERVER** and **AUTO DOWNLOAD SETUP.**

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

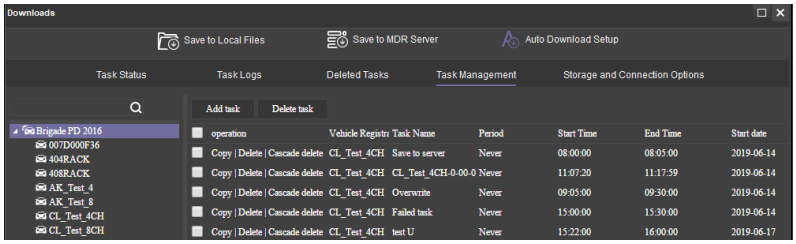
AUTO DOWNLOAD is more suited to a Mobile Network connection as the device can transfer data regardless of location. If **AUTO DOWNLOAD** is setup with a Wi-Fi connection, the device will only run the auto download schedule once it is powered on and connected to the Wi-Fi network.

Note: For users who have both 4G and Wi-Fi setup in their device and want to execute **Auto Download** only via Wi-Fi, it is recommended to change the settings to ‘**Auto-Adapt**’ in firmware when configuring the server connection. This will guarantee the device can automatically switch between different connection methods when either one is available. By default, the Wi-Fi has higher priority than 4G, the device prefers to use Wi-Fi for data transmission which can also save data consumption for SIM cards.

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



Download Window Figure 284



Auto Download Figure 285

Download priority is based on a first come, first served basis.

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

Auto Downloads are setup differently to Clippings and Appointments.

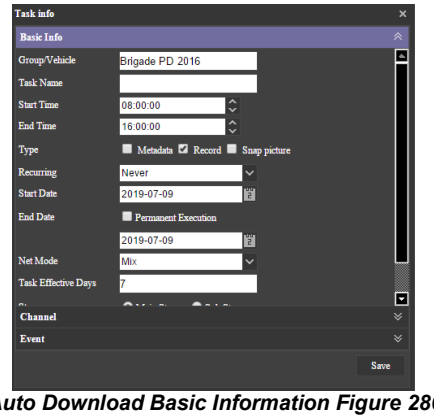
Select the vehicle and then click **TASK MANAGEMENT**. See *Auto Download Figure 285*.

- Click **ADD TASK**. You will now be presented with a **TASK INFO** window which is shown in *Auto Download Basic Information Figure 286*.
- You must now setup all details found under **BASIC INFO**, **CHANNEL** and **EVENT**. See the below figures, *Auto Download Basic Information Figure 286*, *Auto Download Channel Figure 287* and *Auto Download Event Figure 288*.
- **GROUP/VEHICLE** - this represents the vehicle name as shown in the group list in the left pane
- **TASK NAME** – assigned appropriately by the user.
- **START TIME** – this represents the start time of the clipping.
- **END TIME** - this represents the end time of the clipping.
- **TYPE** – choice of either metadata / record / snap picture or all.
- **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 be configured for a future date. The user must ensure that the date selected is when the device will be powered and online.
- **END DATE** – this refers to the end date of the clipping. Select `**Never**` for the task to run indefinitely.
- **NET MODE** – The options are Mob. Net, Wi-Fi and Mob. Net/Wi-Fi.
- Note: If the device has a post alarm set to 7 seconds with auto download set to on and the dashboard post alarm is set to 10 seconds then the auto download recording will have a post alarm record time of 7 seconds as there is no further alarm recording to be downloaded.
- **TASK EFFECTIVE DAYS** – defines how many days a recurring task should occur. If making a one-time clipping from one of the previous days, make sure the task effective days are set to cover the current date, or the task will fail immediately without execution.
- **STREAM** – The options are Main Stream or Sub Stream. Main Stream is higher quality.
- **VIDEO TYPE** – The options are All, Normal Video and Alarm Video.

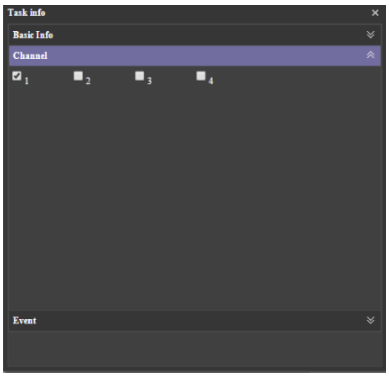
You can view the status of the **AUTO DOWNLOAD** tasks by clicking **TASK MONITOR**. See *Task Monitor Analysing Figure* 289.

Once a download list is created, the status will show 'waiting', then 'analysing', 'analysing finished' and then it begins to download.

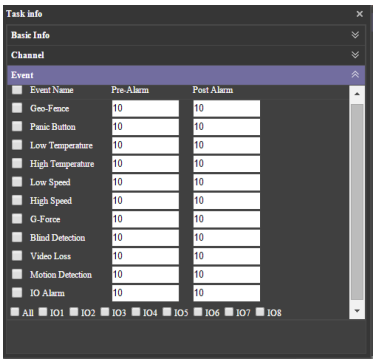
See *Task Monitor Analysing Figure* 289, **HIGH SPEED** will stop device recording to use maximum possible resource to download files at quicker speeds. **LOW SPEED**, device will download files at normal speed while other functions remain the same.



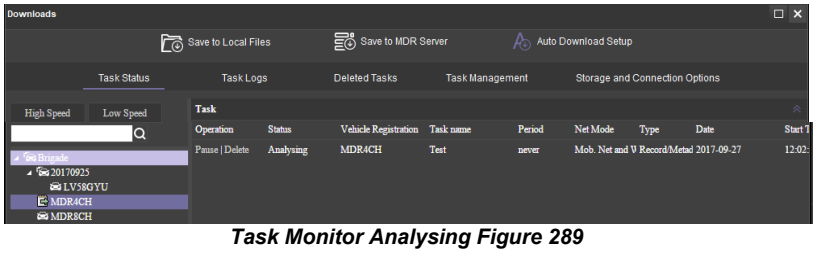
Auto Download Basic Information Figure 286



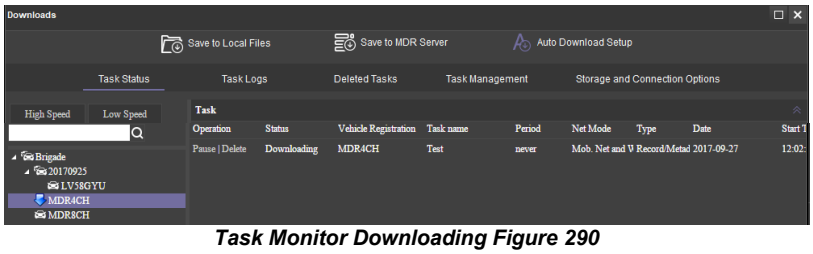
Auto Download Channel Figure 287



Auto Download Event Figure 288



Task Monitor Analysing Figure 289

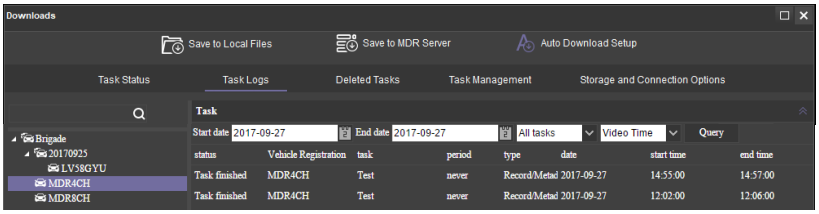


Task Monitor Downloading Figure 290

TASK LOGS are used to search all tasks based on dates and task status. See *Task Logs Figure 291*.

QUERY is used to update the list. See *Task Logs Figure 291*.

DELETED TASKS show tasks that have been deleted by the user. See *Deleted Tasks Figure 292.*



Task Logs Figure 291

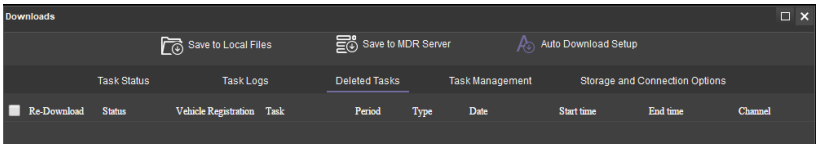
STORAGE AND CONNECTION OPTIONS is used to set the folder for the **AUTO DOWNLOAD** files. If auto-download task is set for Wi-Fi, then the **Max Connection** defines how many devices can download simultaneously. Other devices must wait until the previous one has completed the task. By default, the value is 20. Maximum value is 60. See *Storage and Connection Options Figure 293*.

If a device has multiple Wi-Fi connections available and the fleet manager wants to control each Wi-Fi connection limit, use the Wi-Fi list in the Storage and Connection Options page to define each Wi-Fi maximum connection number.

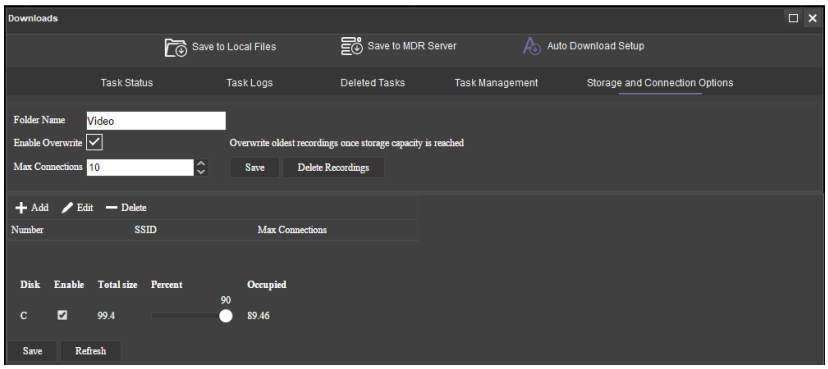
Note: The **Max Connection** in the Auto-Download section only controls the amount of devices able to upload video data. For other online usage such as remote liveview and GPS upload, no limitation is applied.

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*.



Deleted Tasks Figure 292



Storage and Connection Options Figure 293

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 device 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
Task timeout	The task expired (exceed effective date)

6.8.2 Alarm Centre

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

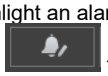
- Alarm Search
- Alarm Settings

6.8.2.1 Alarm Search

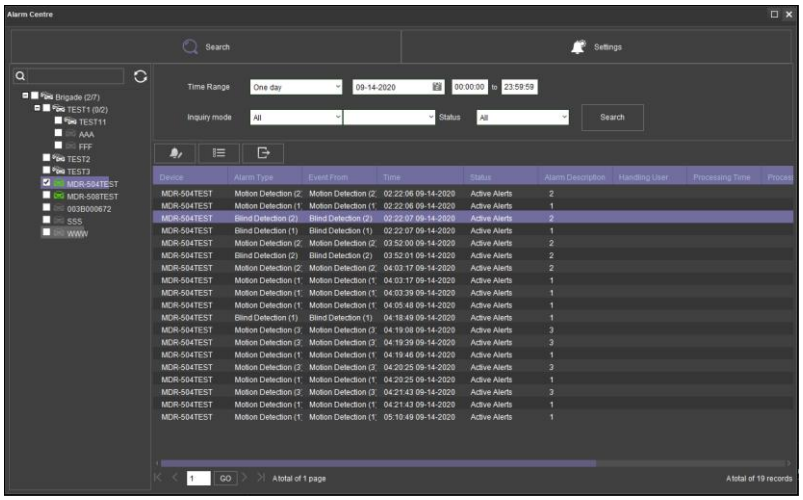
This area is used to search all alarms based on the vehicle, time range, date, event type and alarm status.

Search parameters will need to be set before clicking on the **SEARCH** button. Once clicked, the MDR Server will search and find the relevant information.

An example list is shown in *Alarm Centre Search Figure 294*. 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 Centre Search Figure 294*. **BATCH PROCESSING** is achieved by clicking the  icon. See *Alarm Centre Search Figure 294*.

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 Centre Search Figure 294*.



Alarm Centre Search Figure 294

6.8.2.2 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:

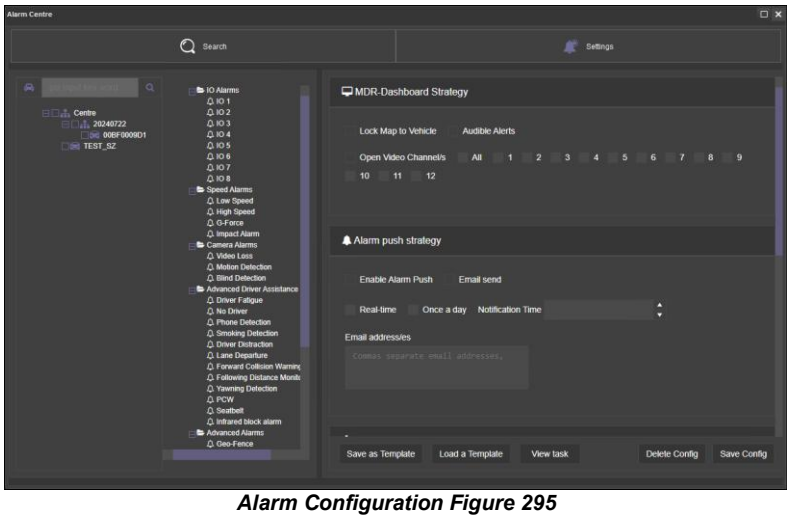
- **Lock Map to Vehicle**: When an alarm is triggered, maps will lock onto the specific vehicle on the map.
- **Audible Alerts**: An audible siren alarm will be played through your PC speakers to alert you of a triggered alarm. Note: Muted PC speakers will not be unmuted for this feature.
- **Open Video 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:

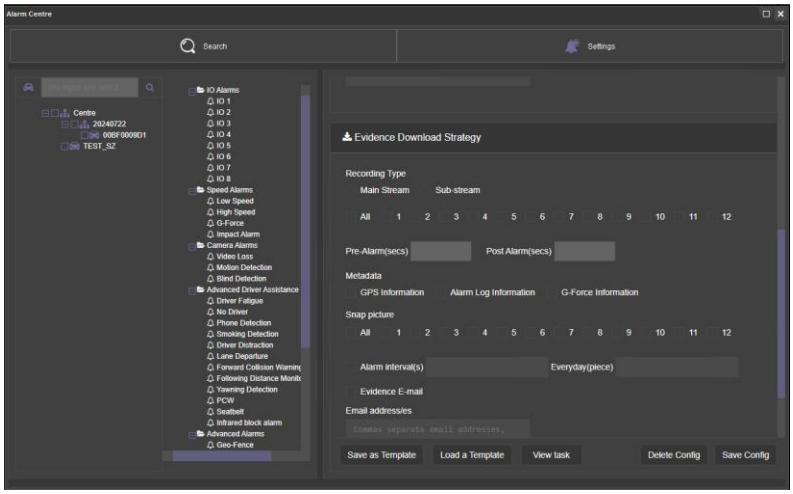
- **Enable Alarm Push**: When an alarm is triggered, notifications will be sent to your mobile apps. Note: Requires apps to be logged in and running as a background service.
- **Email send** to enable the sending of alarm emails to designated email account(s).
- **Real-time**: When an alarm is triggered, 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 295



Alarm Configuration (Continued) Figure 296

- **Snap picture** to capture snapshots when alarms are triggered and automatically uploads them to the evidence centre.
- **Alarm interval(s):** during the set period, no matter how many this alarm type has been triggered, it only forms the first set amount of evidence items.
- **Everyday (piece):** If daily alarms exceed this limit, there will be no more evidence items created. It will also trigger the 'Abnormal Frequent Alarm' in the Alarm Centre. Note: The alarm display is not affected but a new evidence item will not be created.
- **Evidence email:** When an evidence item has been created, it will send the notify the receiver via an email. For evidence email content see *Evidence Email Content Figure 297*.

License plate number	Time	Alarm Type	Alarm Description	Evience Video
MDR-5045Z	2020-06-12 07:26:25	IO 1	IO1	Open video

Evidence Email Content Figure 297

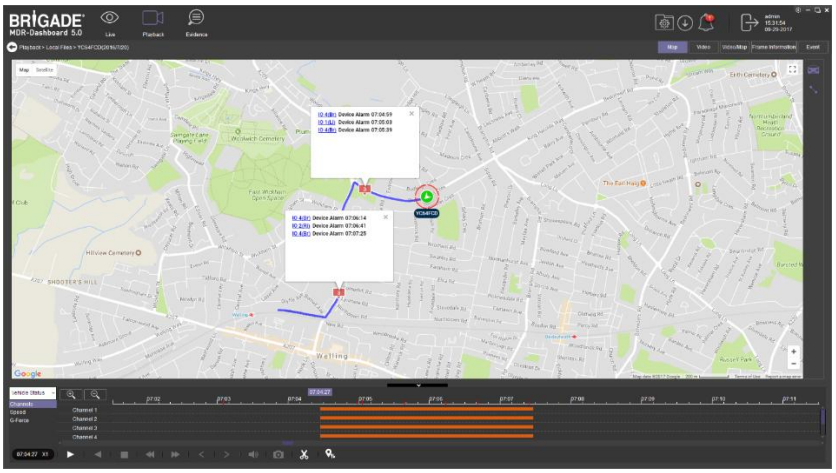
6.9 View Settings (Area 5)

This area contains the following view options:

- Map
- Video
- Video/Map

6.9.1 Map

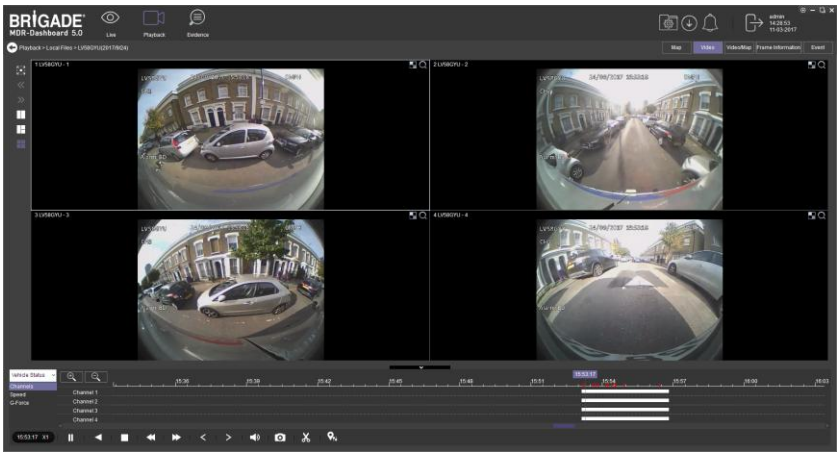
This view is accessed by clicking the **MAP** button. See *Map View Figure 298*. It will display the GPS tracking data. This can be used in both **LIVE** and **PLAYBACK** mode. A hazard symbol on the map will show points where an alarm was triggered. If there are multiple alarms in close succession, a box indicating the number of alarms will be shown on the map .



Map View Figure 298

6.9.2 Video

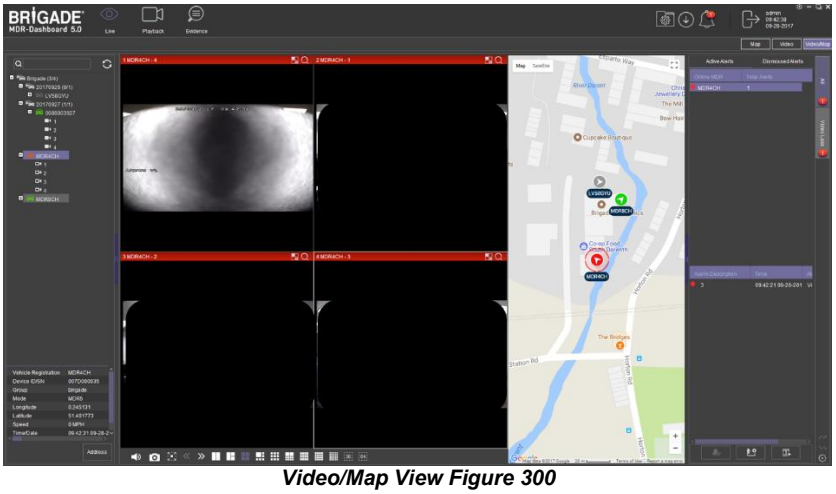
This mode is used to view video channels only. See *Video View Figure 299*. The order of the video channels may be changed by dragging the channel to another slot.



Video View Figure 299

6.9.3 Video/Map

This view is used to access both video and map data. See *Video/Map View* Figure 300 for an example.



Video/Map View Figure 300

6.10 Real-Time Alarm Log (Area 6)

Real-time Alarm Log Figure 301 shows alarms that are currently occurring on all online devices.

At the bottom of the Real-Time Alarm Log area is a menu as shown in *Alarm Menu Figure 302*.

Click on **LOCKING CAR** symbol  to access the Video/Map view with the vehicle locked in the centre 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 303*.

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+”.

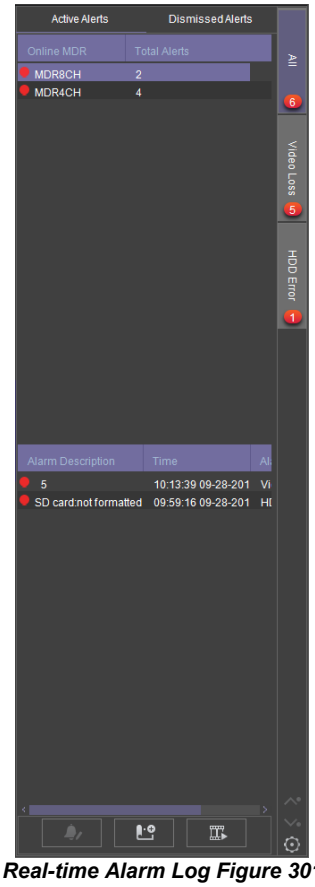
Processing alarms refers to when a user clears an alarm (marks an alarm as dismissed) once the alarm has been reviewed.

ACTIVE ALERTS show alarms that have not been processed by a user. See *Real-time Alarm Log Figure 301*.

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 304*. A description of the event can be applied for reference. For example, ‘False Alarm’.

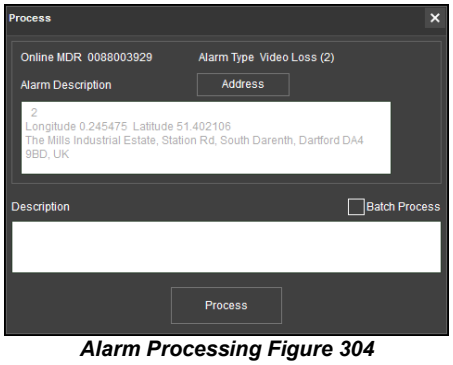
Click **PROCESS** to process an alarm event. Once processed, it will appear automatically under the **DISMISSED ALERTS** log.

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 304*.

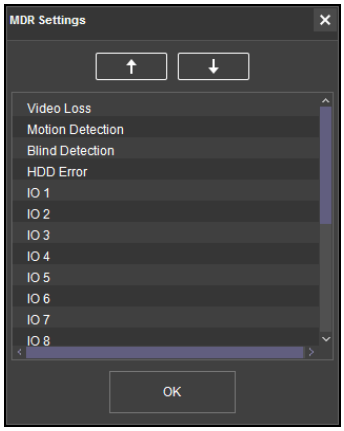


Real-time Alarm Log Figure 301

Alarm Menu Figure 302



Alarm Processing Figure 304



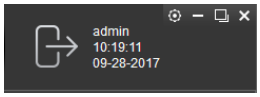
Alarm Settings Figure 303

6.11 User and System settings (Area 4)

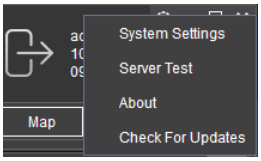
The current logged in username, date (Client PC) and time (Client PC) is displayed. See *User and System Area Figure 305*.

This area is used to **LOGOUT**. This is achieved by clicking on the door icon  . This brings up a confirmation window for logging out. See *Logout Screen Figure 309*.

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 306*.



User and System Area Figure 305



MDR-Dashboard Settings Menu Figure 306

SERVER TEST is used to aid troubleshooting server connections, the feature is used to determine which port is not functioning. See *Server Test Figure 307* and *Server Test Results Figure 308*.

ABOUT displays the window shown in *About Figure 310*. This will show the current MDR-Dashboard and MDR Server version.

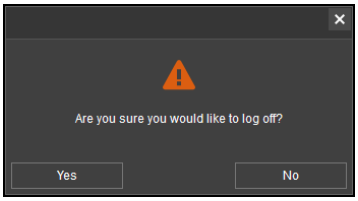
Additional information of which server ports are used will be shown in the **ABOUT** window when the MDR-Dashboard is logged in as server mode. Users can also check EULA and FOSS information as well. See *About Figure 310*.

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

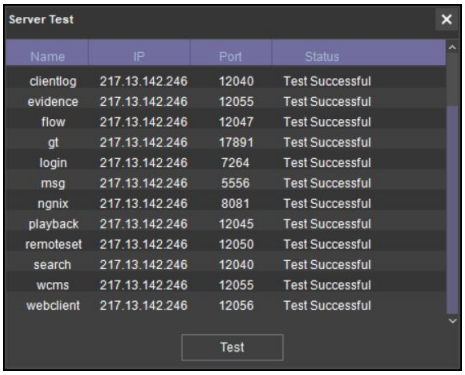
SYSTEM SETTINGS are shown in *System Settings Figure* 311.

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
- Skip Time Duration(seconds) – this enables users to use the keyboard left and right keys to skip forward and backward under Local Flies Playback. The value defines how many seconds to skip at one time.
- 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.
- Automatically Open Historic Live View Channels (Server Mode – Live View only)
- Set Path for Live View Recordings

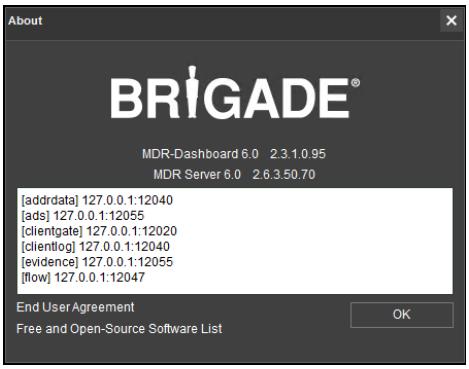


Logout Screen Figure 309

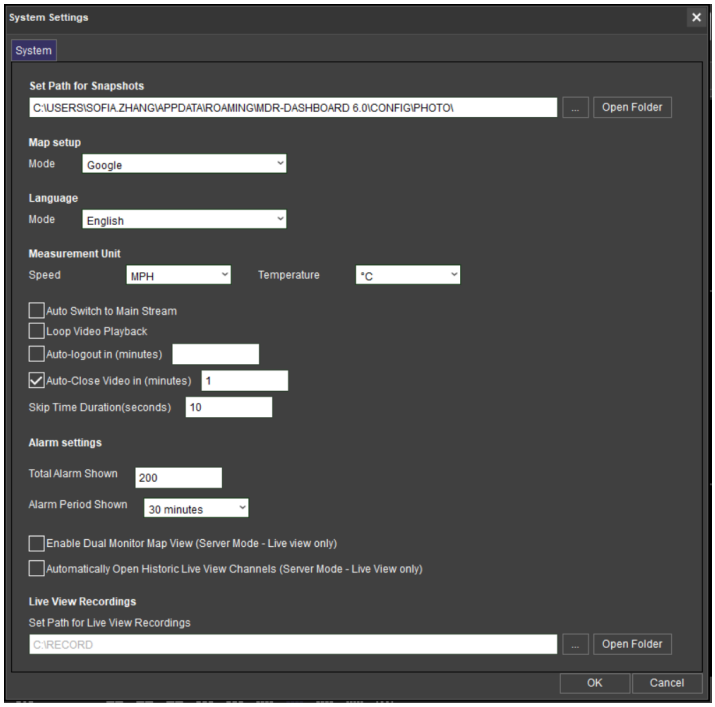


Server Test Figure 307

Server Test Results Figure 308



About Figure 310



System Settings Figure 311

7 Mobile Apps

BRIGADE MDR 6.0 is a free mobile application, available for both Android and iOS operating systems. The **BRIGADE MDR 6.0** application has the following features:

- Live View
- Map positions of devices (device must have GPS connected and locked signal)
- Remote Snapshot one channel at a time - saved to local device
- Playback
- Alarm supports processing alarms
- Statistics for GPS, Online Rate, Alarm and Milage
- Evidence Centre for viewing evidence footages

7.1 iOS App

7.1.1 iOS App Requirements

Table 16: Minimum requirements for BRIGADE MDR 6.0 to run on iOS

DEVICE	MINIMUM REQUIREMENTS
iPhone	iOS 11
iPad	iOS 11

7.1.2 iOS App Push Certificate

The iOS app utilises a **yearly Certificate** for Push functions. If the Push Certificate expires, an iOS device will be unable to get notification when an alarm is triggered, which would usually display a pop-up message on the iOS message centre and banner. When nearing the expiration date, Brigade will send out a notification email with a new certificate download link. Please download the certificate and upload the certificate to your current configured server as guided in *Chapter 6.7.7.5 Push Config*.

7.1.3 iOS App Installation

On your Apple device, go to the App Store.

Search for “Brigade Electronics” or “MDR 6.0”.

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 6.0 to send you notifications, this is a generic request.

The login window will be displayed, see *iOS App Login Figure 312*. These login details correspond to MDR-Dashboard 6.0 login details.

It is advised to create User accounts (in MDR-Dashboard 6.0 System Management Area) for MDR 6.0 app logins so this can be tracked in the MDR-Dashboard 6.0 Alarm processing area.

iOS App Login Figure 312

Login Advance Setting Figure 313

7.1.4 iOS App Operation

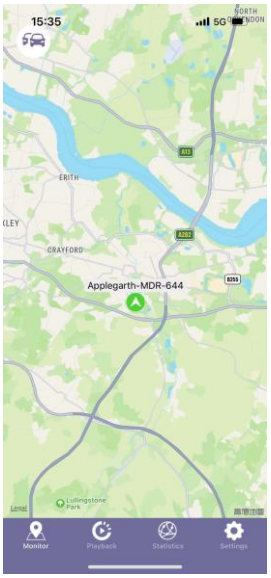
Depending on the device features and location, you can connect to an MDR Mobile Network Server or an MDR Wi-Fi Server.

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

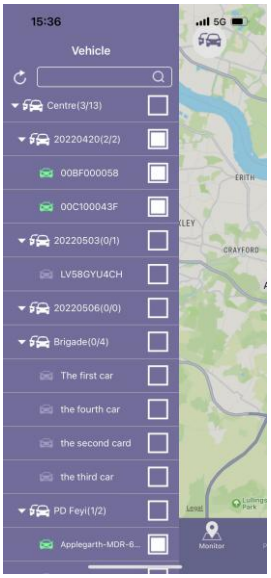
Tap the application icon as shown in *Application Icon Figure 314*.

The iPhone login screen is then displayed as shown.

Application Icon Figure 314



iOS Map View Figure 315



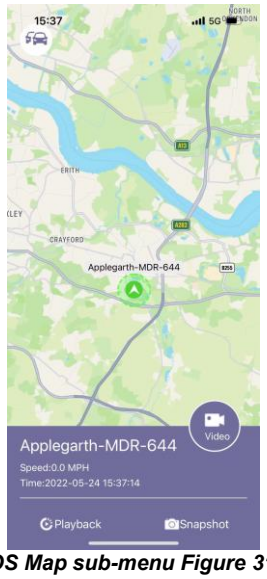
iOS Group List Figure 316

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

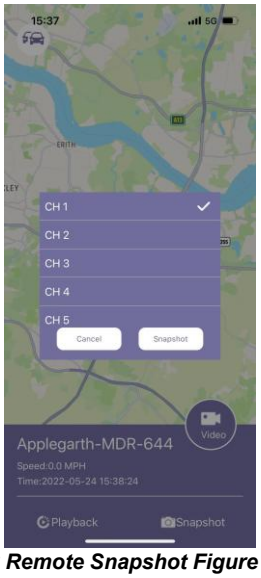
Type in the Mobile Network server address (public IP address of the firewall) into MDR 6.0 e.g. 12.345.6.78.

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

Type in the Wi-Fi server address in MDR 6.0, e.g. 192.168.1.14.



iOS Map sub-menu Figure 317



iOS Remote Snapshot Figure 318

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.

Login timeout is 30 seconds. If it takes longer than 30 seconds to establish a connection to the server, this will result in a timeout error. Please change your connection method and try again.

Once logged in you will be presented with the **MAP** window. As shown in *iOS Map View Figure 315*.

Tap on  to bring up the **GROUP** list as shown in *iOS Group List Figure 316*. The white 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.

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

To exit the **GROUP** list, tap on any other parts other than **Group**. See *iOS Group List Figure 316*.

Tapping on a device will bring up the map sub-menu.

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

To access **video menu** (liveview), click on a vehicle from a fleet list bring up a sub-menu (*iOS Map sub-menu Figure 317*). Press the "Video" button to enter the video interface. See *iOS Video Window Figure 320*.

Video menu used for online liveview. numbers at the bottom to enable/disable each channel. Control button from left to right are Mute/Unmute; Snapshot; Open all/Close all; Map View (See *iOS Video Window - Map Figure 326*); Full Screen.

Playback can be accessed via the map view or the bottom banner "Playback" icon, which has 3 sub tabs: **Online MDR**; **Server** and **Evidence**. They are shown in the MDR- Dashboard functionality.

Remember to choose a vehicle from the fleet list on the left. Otherwise, the Playback page will display any data.

After choosing a vehicle, swipe left or right to change the months or click on the date beside the vehicle registration number to quickly define the date range.

 Green means a recording is available.  Orange means has alarm recording at that day. A small red dot represents GPS data that will support tracking on the map. Playback sub-pages see *iOS Playback Detail Figure 327*.

Evidence supports 2 search modes:

General Search: search by vehicle registration number.

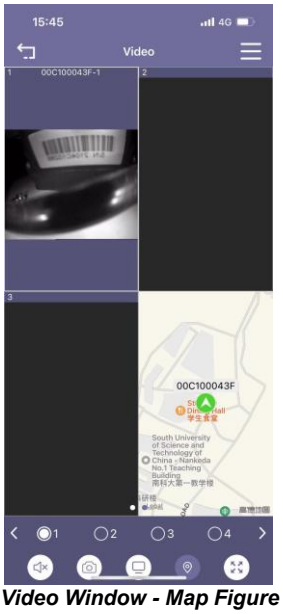
Advanced Search: based on alarm types and occurrence time. Search results will be listed below, and playback will be available. See *iOS Evidence –Search Results Figure 323*.

Statistics can be accessed by the navigation button at bottom banner. It consists of 5 types of statistic information: Alarm, Location info, Mileage, Online rate and Active Alarm Centre (top right corner).

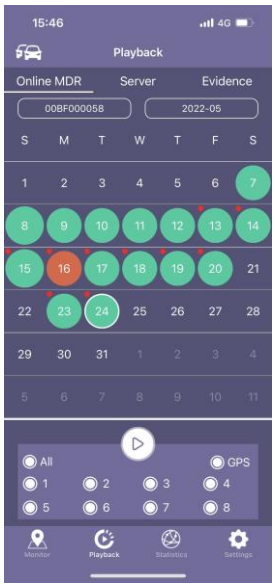
Each page gives collected data based on vehicle/fleet selection and time defined. Each statistic tab consists of a chart in the middle and detail list at the bottom.

In the **Alarm** tab, the bottom list gives each selected vehicle a total alarm amount. By clicking on the , each

iOS Video Window Figure 320

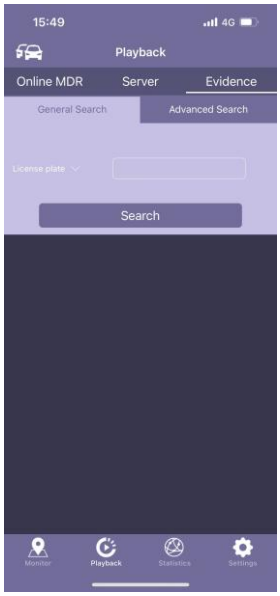


iOS Video Window - Map Figure 326

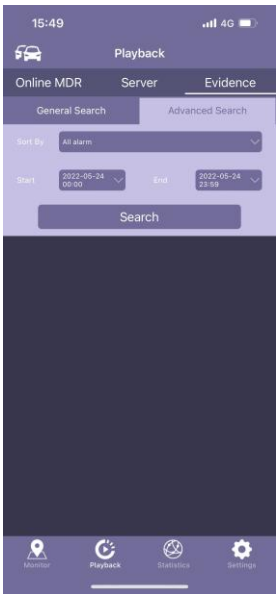


iOS Playback Figure 321

iOS Playback Detail Figure 327



iOS Evidence – General Search Figure 322



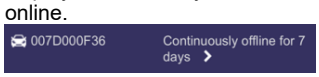
iOS Evidence – Advanced Search Figure 328

alarm item can be viewed in detail with location available on the map.

In **Location** info tab, the chart displays the amount of GPS data received and bottom detail list gives each GPS data contain information.

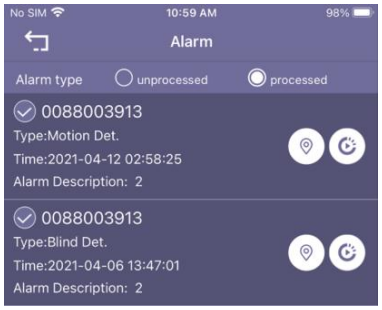
In the **Mileage** tab, the bottom list provides each vehicle's total mileage for each day.

In the **Online rate** tab, the bottom list gives information on how long each vehicle has offline for. 'No display' means every vehicle on the list are always online.



Active Alarm Centre displays real-time alarms, which provides alarm location shown on the map and alarm footage playback.

Each alarm can be processed by clicking on the item. Comments can be added into **Remark** section. Click **Confirm** to move the alarm to the "Processed" column.



iOS Processed Alarm Log Figure 319

Setting can be accessed by clicking on the last icon on the bottom banner. As shown in ***Error! Reference s ource not found.***.

Server IP Address displays the IP address or the Server name which the app is connected to.

Username displays the currently logged in user.

Push displays push notifications from the MDR app if it is running in the background. (Phones notification centre and top banner).

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

Alarm Center allows the vehicle to be displayed in the centre of the map when an alarm occurs.

Auto-Logout a configurable setting that automatically logs an idle user out after 1 minute (set by default).

Auto-Close Video a configurable setting that will automatically close open video channels after a set period. This prevents the unnecessary use of data.

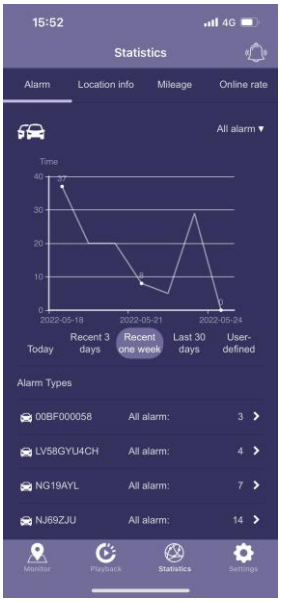
Speed Unit controls the speed unit shown within the app, this can be mph or km/h.

Auto-Playback Time controls when the user clicks on vehicle playback, the playback starts from the selected amount of minutes either before or ahead of current time (the user cannot select from the current time).

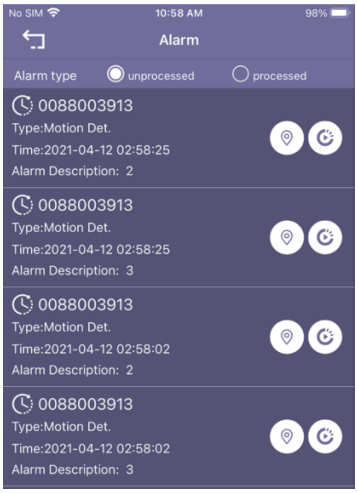
Free and Open-Source Software List displays which 3rd party software has been used for building up this app.

Version displays the app version details.

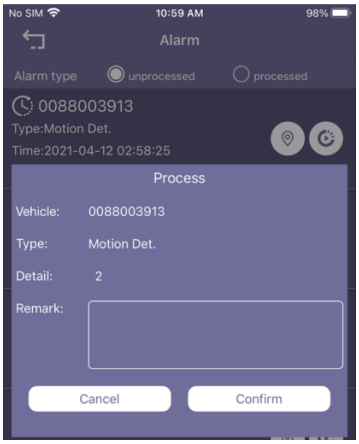
iOS Evidence –Search Results Figure 323



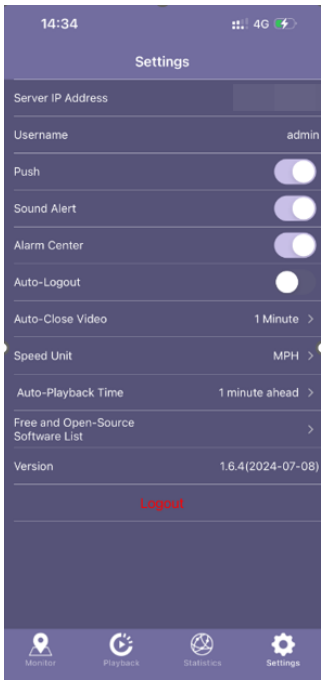
iOS Statistics Figure 329



iOS Alarm Log Figure 324



iOS Process Alarm Figure 330



iOS Settings Figure 325

7.2 Android App

7.2.1 Android App Requirements

Table 17: The minimum requirements below are for MDR 6.0 to run on Android

DEVICE	MINIMUM REQUIREMENTS
Android Phone	Android 7.0 Screen Resolution of 720P Screen Size of 4 inch
Android Tablet	Android 7.0 Screen Resolution of 720P

7.2.2 Android App Installation

Open the Google Play Store App

Search for “Brigade Electronics” or “MDR 6.0”.

Tap the MDR 6.0 app. Click the **INSTALL** button.

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

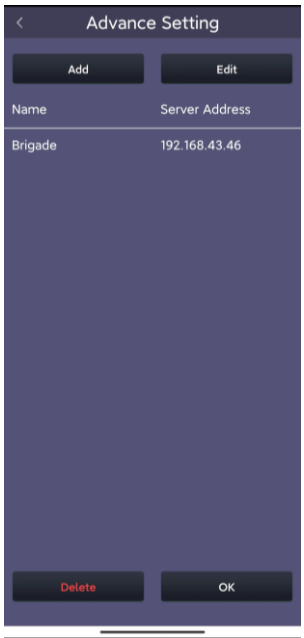
The app will then begin to install. The progress will be shown.

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

The login window will be displayed. These login details correspond to MDR-Dashboard 6.0 login details.

It is advised to create User accounts (in MDR-Dashboard 6.0 System Management Area) for MDR 6.0 app logins so this can be tracked in the MDR-Dashboard Alarm processing area.

Start-up Screen Figure 331



Login Advance Setting Figure 332

7.2.3 Android App Operation

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

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

Tap the application icon as shown in *Application Icon Figure 333*.

The start-up screen will be displayed.

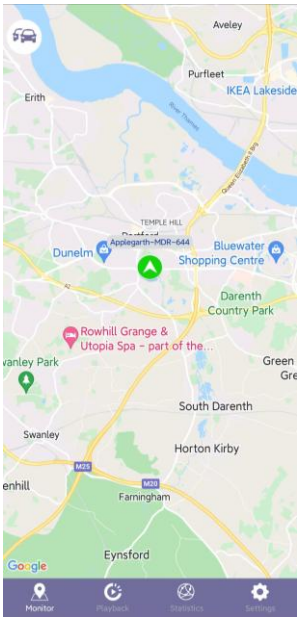
The Android login screen is then displayed as shown in *Android Login Figure 334*.

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 6.0 e.g. 12.345.6.78.

Application Icon Figure 333

Android Login Figure 334



Android Map View Figure 335

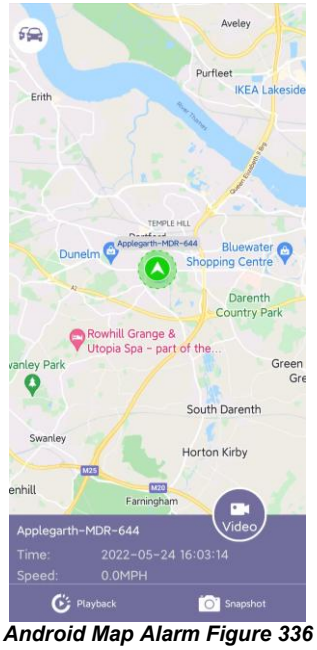
To log into the Wi-Fi server, ensure the device is connected to the **SAME** Wi-Fi network that the MDR Server and unit is connected to.

Type in the Wi-Fi server address in MDR 6.0, e.g. 192.168.1.14.

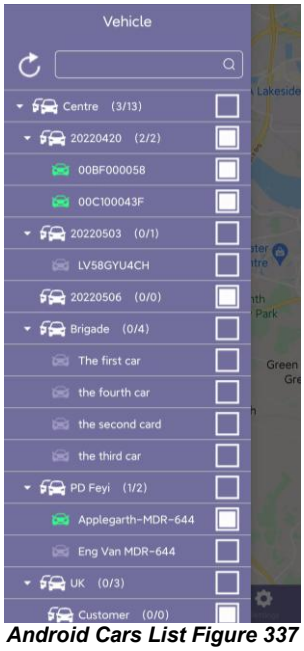
Note: When connecting to the Wi-Fi server, if the Wi-Fi network does not have internet access then the map function will appear blank. The Wi-Fi network may be configured to have internet access if necessary, please contact your IT department.

The operation of the Android application MDR 6.0 is explained in the above section 7.1 iOS App.

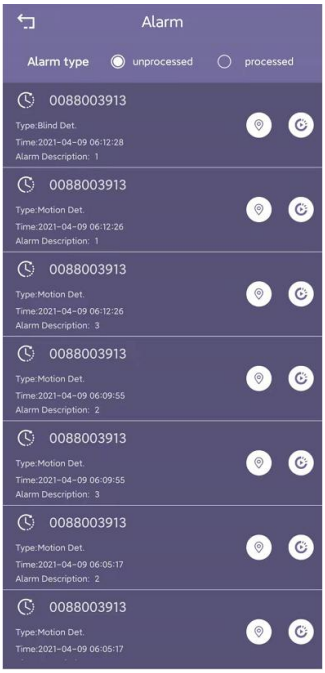
Some of the Android operation interface snapshots are shown below.



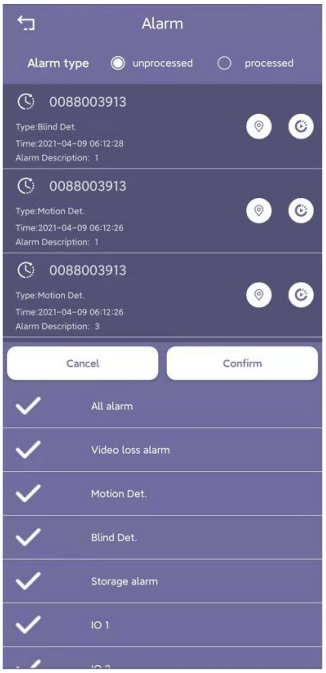
Android Map Alarm Figure 336



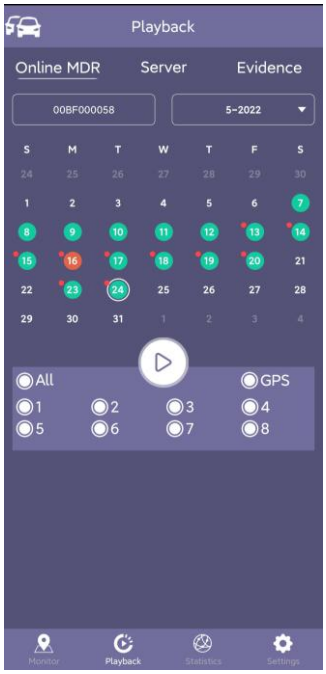
Android Cars List Figure 337



Android Alarm Log Figure 338



Android Alarm Log Filter Figure 339

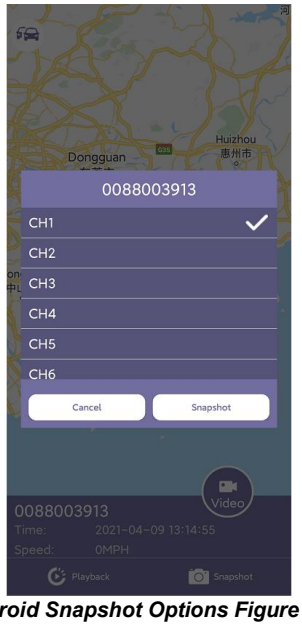


Android Playback Figure 340

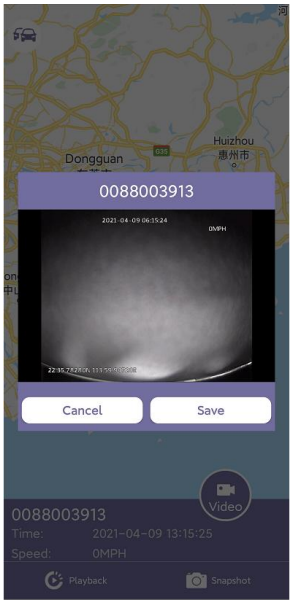
Further examples of typical android windows are shown *Android Snapshot Save Figure 344* onwards.

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

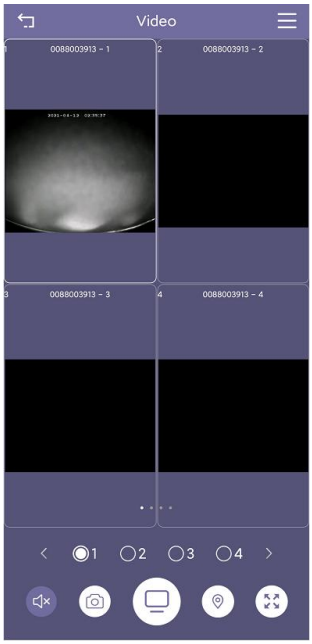
Push outwards to zoom in on a point and inwards to zoom out.



Android Snapshot Options Figure 342



Android Snapshot Save Figure 344



Android Video Window Figure 341

Android Evidence Figure 343

Android Statistic Figure 345

Server IP Address displays the IP address or the Server name which the app is connected to.

Username displays the currently logged in user.

Push displays push notifications from the MDR app if it is running in the background. (Phones notification centre and top banner).

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

Alarm Center allows the vehicle to be displayed in the centre of the map when an alarm occurs.

Auto-Logout a configurable setting that automatically logs an idle user out after 1 minute (set by default).

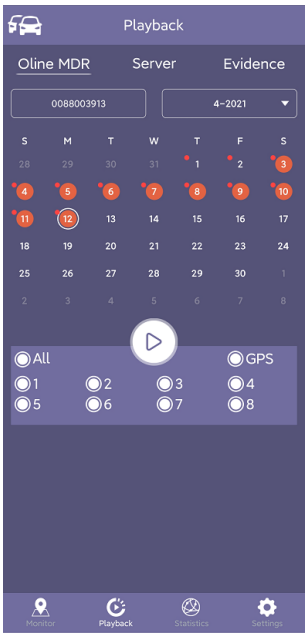
Auto-Close Video a configurable setting that will automatically close open video channels after a set period. This prevents the unnecessary use of data.

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

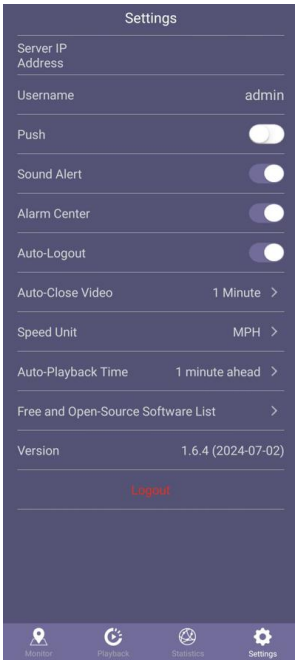
Auto-Playback Time controls when the user clicks on vehicle playback, the playback starts from the selected amount of minutes either before or ahead of current time (the user cannot select from the current time).

Free and Open-Source Software List displays which 3rd party software has been used for building up this app.

Version displays the app version details.



Android Playback Figure 346



Android Settings Figure 347

8 MDR Server 6.0 Advanced Features

8.1 Database Backup and Restore

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

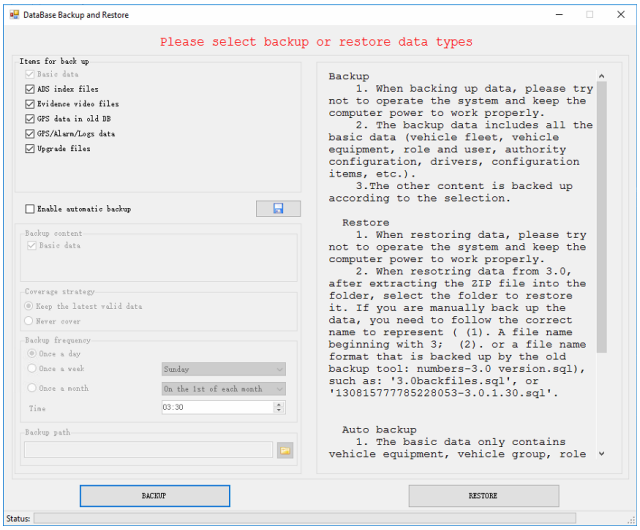
(1) Run the program as **ADMINISTRATOR**.
(2) Leave the server running, do not operate the system and ensure there is no power cut during backing up or restoring process. A notification window pops-up before restoration start to remind the user to make sure all services are running. Click on **OK** to proceed.
(3) During Backup or Restore process, the services in MDR Server Control will be stopped automatically. After the process is complete, those services will start to work immediately. Do not manually operate them until the process has finished.
(4) If a backup or restoration operation fails, please attempt to do it again. If it fails once more, please contact Brigade Technical Support.

Backup:
Backup items can be chosen from the list:

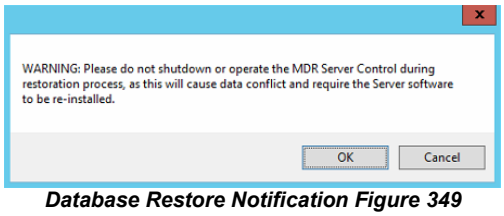
(1) **Basic data** (mandatory): information of the vehicle system, such as fleet/group information, device information and driver information.
(2) **ADS index files**: Historic Auto Download videos which are saved in the server currently.
(3) **Evidence video files**: Historic uploaded Evidence files.
(4) **GPS data in old DB** (MDR-Dashboard): old GPS data created by older version server software (before 2.2.2.0.32).
(5) **GPS/Alarm/Log data**: all data for GPS info, Alarm info and logs can be found in the Mongodb_3.2 folder.
(6) Upgrade files: uploaded MDR upgrade files.

Enable automatic backup:
Click the  to save the auto backup setting. Settings below are only for auto-backups:

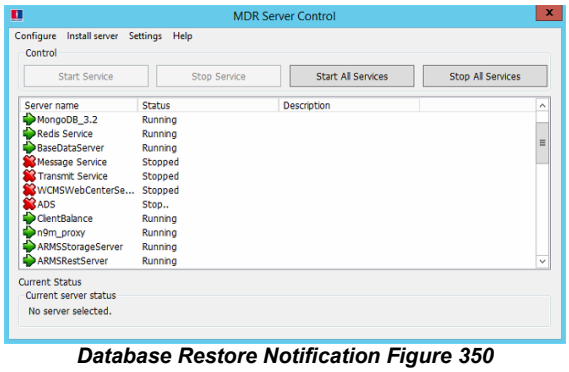
(1) Basic data: information of the vehicle system, such as fleet/group information, device information and driver information.
(2) Coverage strategy: either create a new file every time or covering previous backup file to keep the latest. Users to choose depending on their preference.
(3) Backup frequency: Once a day, Once a week or Once a month.
(4) Backup path: to determine a local file for saving the auto backup file.



Database Backup and Restore Figure 348



Database Restore Notification Figure 349



Database Restore Notification Figure 350

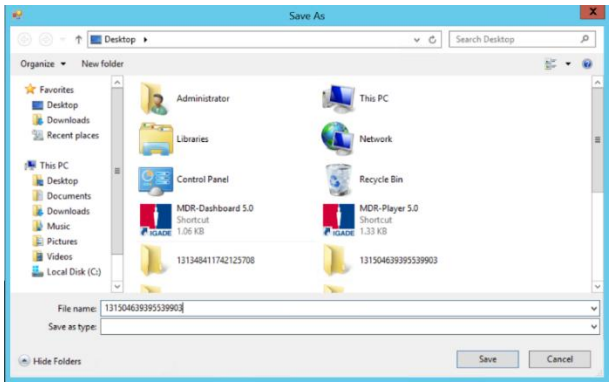
8.1.1 Database Backup

Warning*:The backup folder name cannot have any spaces as this will cause an error window. As shown in *Backup Define Path Figure 351.

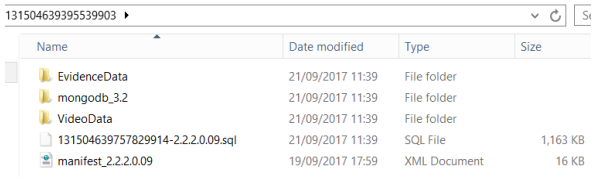
Follow the below steps to create a database backup:

- Brigade recommends backup processes to be completed after hours when the MDR Server will not be used because the backup process will automatically stop/start services.
- Leave the Server Control open and keep every service running or it will cause the backup process to fail.
- 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 time taken to create each backup can differ depending on the content, size, etc.
- Once the backup has been completed successfully, a prompt will be shown stating, “Data Backup success”. As shown in *Successful Backup Figure 353*.

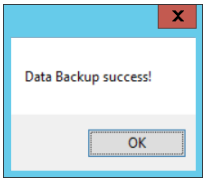
Typical Structure of an MDR Server backup is shown below. This must not be manipulated in any way. It could render the backup unusable.



Backup Define Path Figure 351



Structure of Backup Folder Figure 352

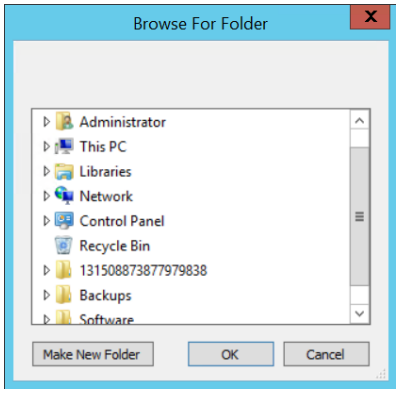


Successful Backup Figure 353

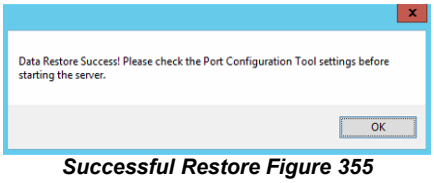
8.1.2 Database Restore

Follow the below steps to restore a database:

- Brigade recommends backup processes to be completed after hours when the MDR Server will not be used because the restore process will automatically stop/start services.
- Leave the Server Control open and keep every service running or it will cause the restore process to fail.
- 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 time taken implement each restoration can differ depending on the content, size, etc.
- Once the restoration has been completed successfully, a prompt will be shown stating, “Data Restore Success! Please check the Port Configuration Tool settings before starting the server.” As shown in *Successful Restore Figure 355*.
- Click the “Save Config” button in the Port Configuration Tool after any change to the settings, to ensure all the parameters have been saved.
- If you are already logged into MDR-Dashboard 6.0, 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 6.0.



Restore Define Path Figure 354



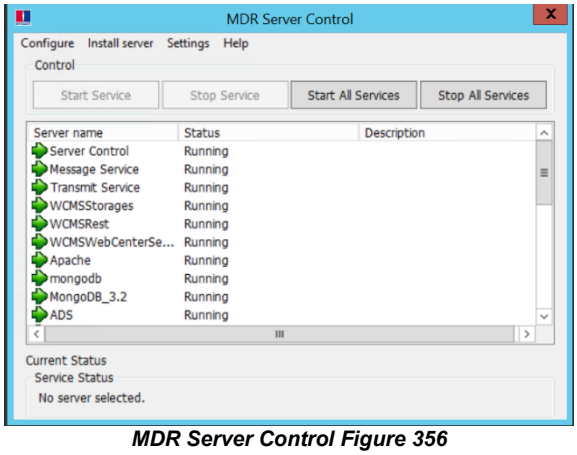
Successful Restore Figure 355

8.2 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.

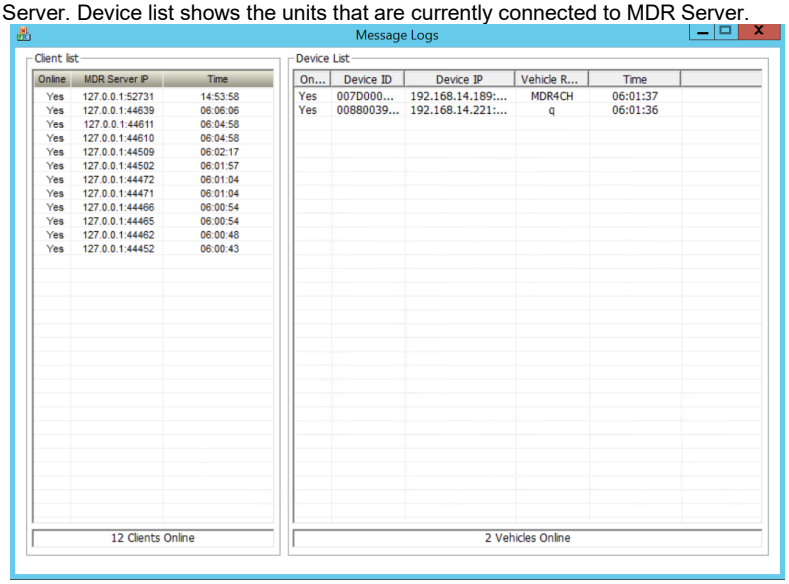
Install Server is used to install or uninstall a service. You can choose a specific service or all services.



MDR Server Control Figure 356

8.2.1 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 units that are currently connected to MDR Server.

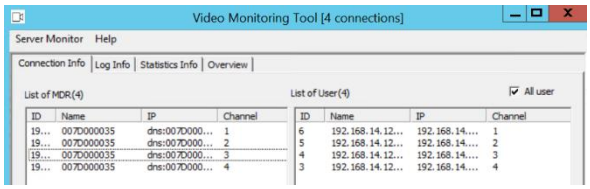


Message Logs Figure 357

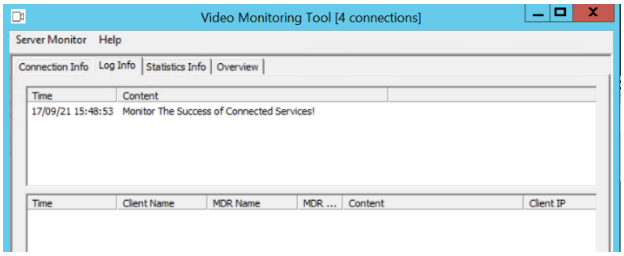
8.2.2 Video Monitoring Tool

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

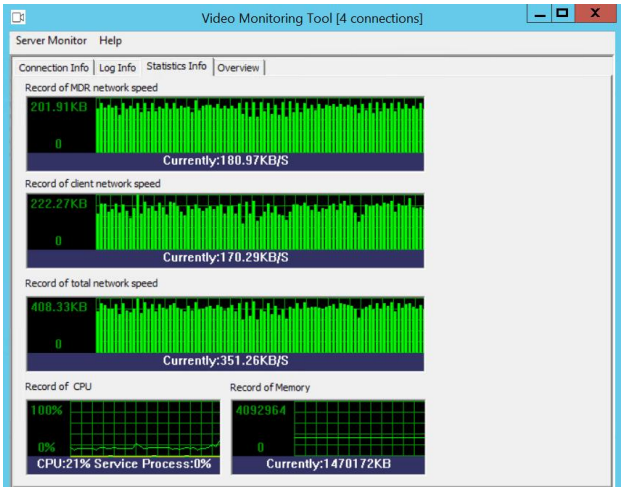
The Video monitoring tools can be used to monitor device/client connections to MDR Server when doing live view. Network speeds can also be monitored within this tool.



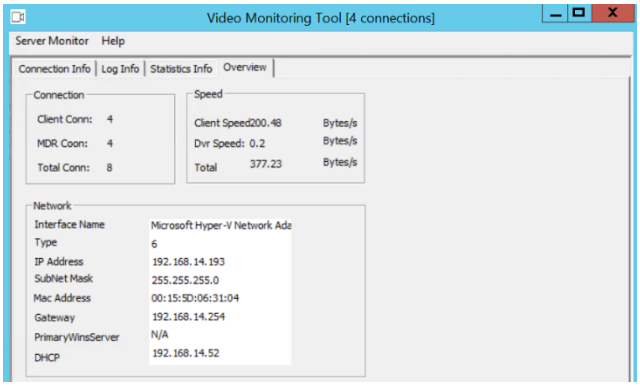
Connection Information Figure 358



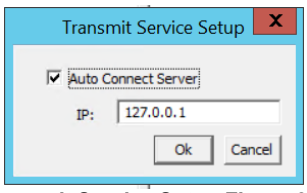
Log Information Figure 359



Statistics Information Figure 360



Overview Figure 361



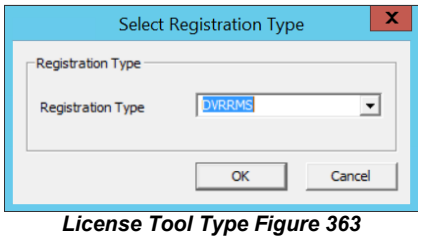
Transmit Service Setup Figure 362

8.2.3 License Tool

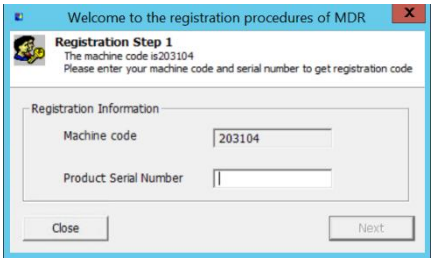
This tool is currently unused. Future purposes will be internal only (Brigade).

Follow the steps below to complete unlimited licensing:

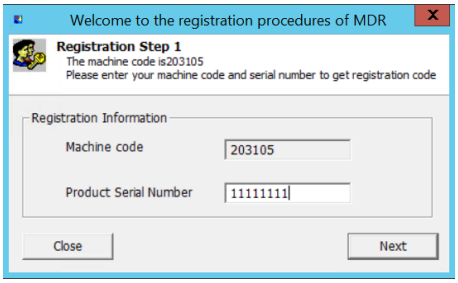
- Click **Settings** on the MDR Server control window then license tool to access it
- Choose DVRRMS and click **OK**.
- Take note of the Machine code - 203104.
- Submit this code to a Brigade engineer.
- Brigade engineer will create a registration code
- Once you have received the registration code, 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 363



License Registration Figure 364



Product Serial Number Figure 365

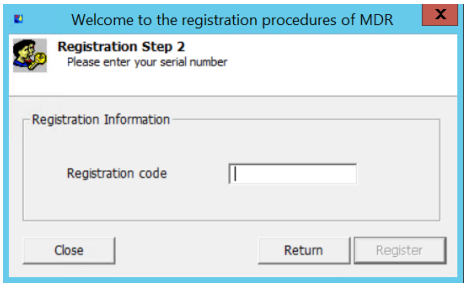


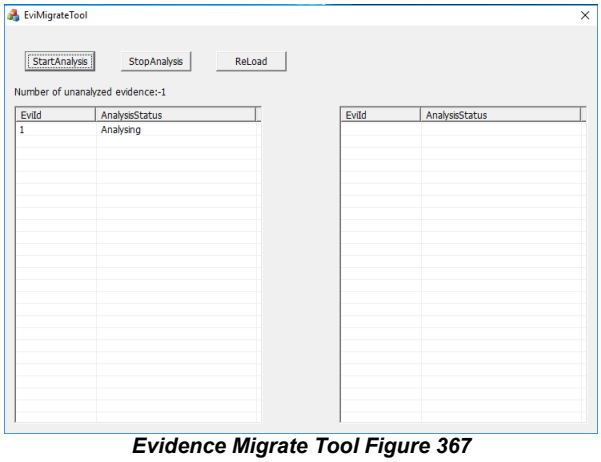
Figure 366

8.3 Evidence Migrate Tool

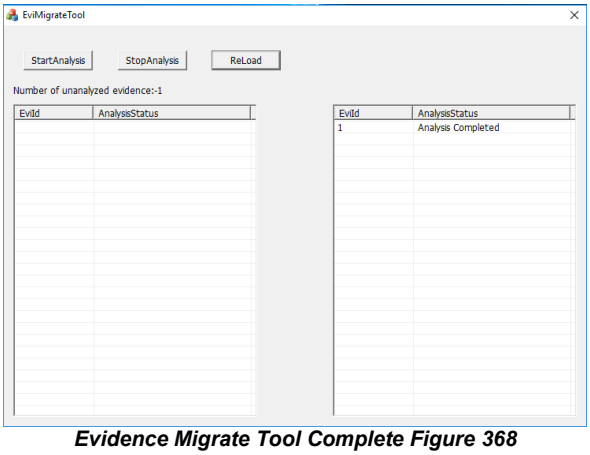
This tool is used to transfer evidence from a previous version of the server to the current version of the server. Because the database has been upgraded between versions, this tool is needed to migrate the evidence video on the previous server to the new server and MDR-Dashboard client.

After installing the new server and completing the restore process, open the EviMigrate tool, it will scan the folder and detect non-readable evidence items and display them as shown on the list below. The user can then click the "StartAnalysis" button to start the transition. After the process is complete, all evidence items should be listed in the right column.

Open the latest MDR-Dashboard 6.0, Evidence items created by the previous MDR-Dashboard 6.0 version, can be viewed and edited.



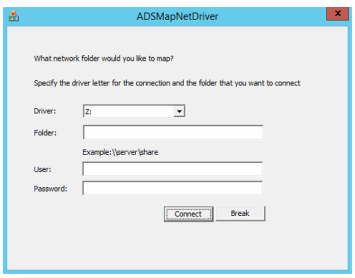
Evidence Migrate Tool Figure 367



Evidence Migrate Tool Complete Figure 368

8.4 Check Disk Tool

This tool is used after the user expands the server storage with the DAS devices (Directly Attached Storage) and NAS (Network Attached Storage). If NAS is being used, run the MDR-Server dedicated tool "ADSMapNetDriver.exe" in **C:\Program Files (x86)\MDR Server\TransmitServer\AdsServer** to map the network drive. Then the Check Disk Tool can be used. After running the program, restart the MDR-Dashboard client, then newly added storage devices will appear in the setting.



ADSMapNetDrive Tool Figure 369

Check Disk Tool Figure 370

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 (H.264)	1080P (AHD)	8192	6390	5505	4068	3712	2818	1919	1024
	960P (AHD)	7987.2	6240	5366.4	4492.8	3619.2	2745.6	1872	998.4
	720P (AHD)	6144	4800	4128	3456	2784	2112	1440	768
	WD1	2662.4	1996.8	1664	1331.2	1170	1040	936	832
	D1	2048	1536	1280	1024	900	800	720	640
	WHD1	1996.8	1664	1331.2	998.4	832	728	650	585
	HD1	1536	1280	1024	768	640	560	500	450
	WCIF	1331.2	998.4	832	665.6	572	455	405.6	364
	CIF (Lowest)	1024	768	640	512	440	350	312	280
Video Streaming Data Rate (Kbps) depending on resolution (H.265)	1080P (AHD)	5734	4473	3847	3221	2596	1970	1344	717
	960P (AHD)	5591	4368	3756	3145	2533	1922	1310	699
	720P (AHD)	4301	3360	2890	2419	1949	1478	1008	538
	WD1	1597	1198	998	799	702	624	562	499
	D1	1331	998	832	666	630	560	504	448
	WHD1	1198	998	799	599	499	437	390	351
	HD1	998	832	666	538	448	392	400	360
	WCIF	799	599	499	399	343	273	243	218
	CIF (Lowest)	717	538	448	358	352	280	250	224

9.2 Normal / Alarm Recording Parameters

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

For typical recording sizes for a one-hour duration and HDD recording times in hours versus storage capacity, please use the MDR storage calculator: https://brigade-electronics.com/mdr-hub/.

9.3 MDR-Dashboard 6.0 Silent Installation

MDR-Dashboard 6.0 supports silent installation using PowerShell switches. Follow the steps below to complete a silent installation:

Copy the installer to a directory, such as: C:\install\MDR-Dashboard_6.0_2.3.1.0.83.exe
Enter the PowerShell window
Run the command: C:\install\MDR-Dashboard_6.0_2.3.1.0.83.exe /VERYSILENT /SP-
You can also put the command in the batch file install.bat and double-click install.bat to run it. An example is shown below

```
ECHO.
ECHO Installing MDR-Dashboard 6.0
ECHO Please wait...
start /wait %systemdrive%\install\MDR-Dashboard_6.0_2.3.1.0.83.exe /VERYSILENT /SP-
ECHO
ECHO Killing MDR-Dashboard_6.0_2.3.1.0.83.exe process
taskkill.exe /F /IM MDR-Dashboard_6.0_2.3.1.0.83.exe
ECHO
```

*If the software needs to be updated, users can run "C:\MDR-Dashboard\unins000.exe /VERYSILENT /SP-" command to uninstall the previous version first, then proceed to install the new version.

9.4 Additional PowerShell Switches

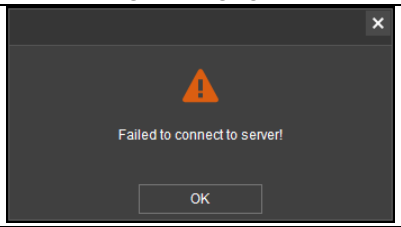
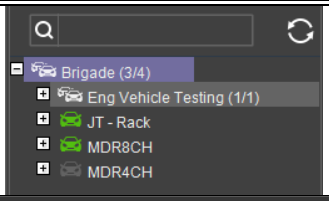
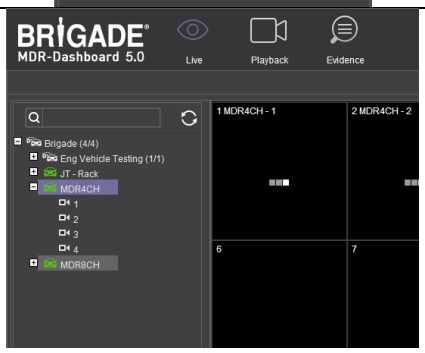
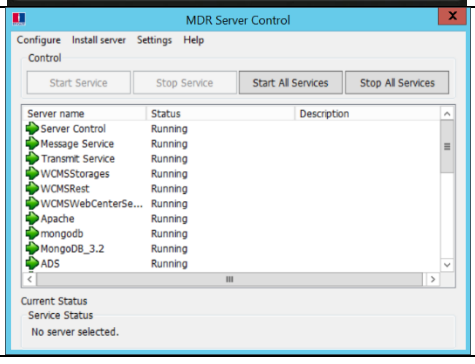
SP-	Disables the "This will install... Do you wish to continue?" prompt at the beginning of the setup. This will have no effect if the DisableStartupPrompt [Setup] section directive was set to yes.
/SILENT, /VERYSILENT	Instructs Setup to be silent or very silent. When Setup is silent the wizard and the background window are not displayed but the installation progress window is. When a setup is very silent this installation progress window is not displayed. Other prompts display as normal, for example error messages during installation are displayed as well as the startup prompt is (if you haven't disabled it with DisableStartupPrompt or the "/SP-" command line option explained above) If a restart is necessary and the "/NORESTART" command isn't used (see below) and Setup is silent, it will display a Reboot now? messagebox. If it is very silent it will reboot without prompting.
/NORESTART	Instructs Setup not to reboot even if it is necessary.
/LOADINF="filename"	Instructs Setup to load the settings from the specified file after having checked the command line. This file can be prepared

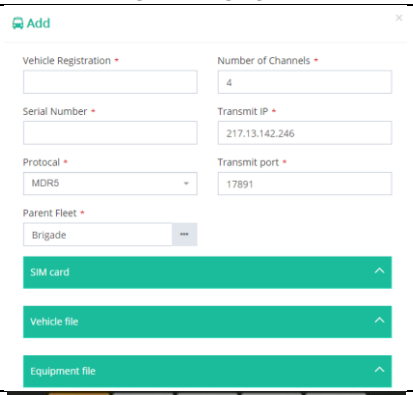
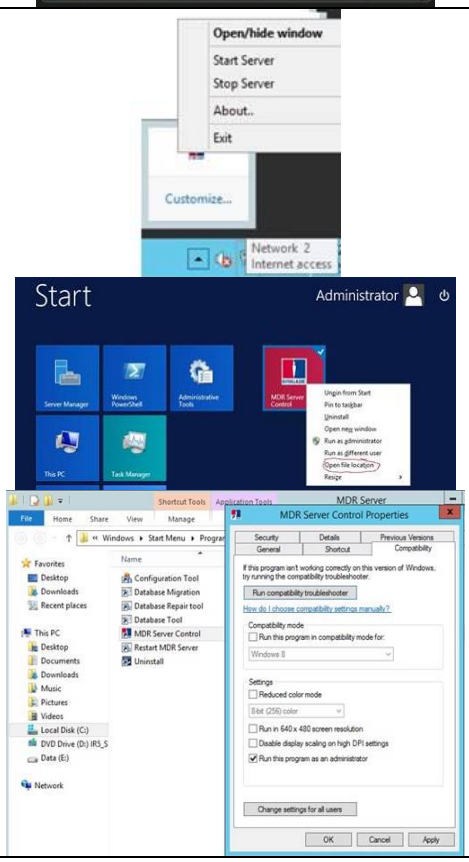
using the "/SAVEINF=" command as explained below. /SAVEINF="filename"	Instructs Setup to save installation settings to the specified file.
/DIR="x:\dirname"	Overrides the default directory name displayed on the Select Destination Directory wizard page. A fully qualified pathname must be specified. If the [Setup] section directive DisableDirPage was set to yes, this command line parameter is ignored.
/GROUP="folder name"	Overrides the default folder name displayed on the Select Start Menu Folder wizard page. If the [Setup] section directive DisableProgramGroupPage was set to yes, this command line parameter is ignored.
/NOICONS	Instructs Setup to initially disable the Don"t create any icons check box on the Select Start Menu Folder wizard page.
/COMPONENTS="comma separated list of component names"	Overrides the default components settings. Using this command line parameter causes the setup to automatically select custom.

10 Troubleshooting

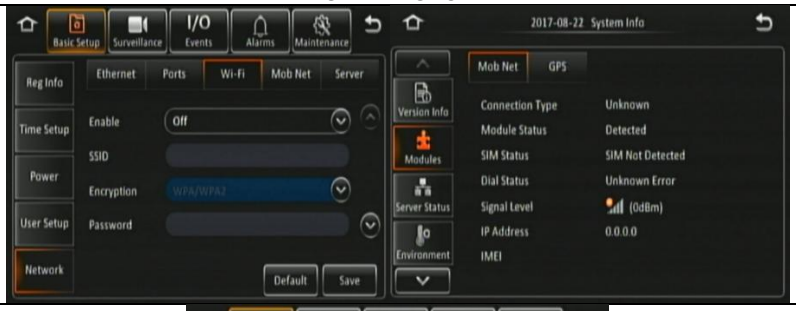
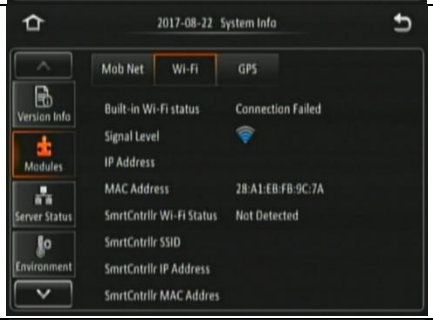
10.1 Mobile Network and Wi-Fi Troubleshooting

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

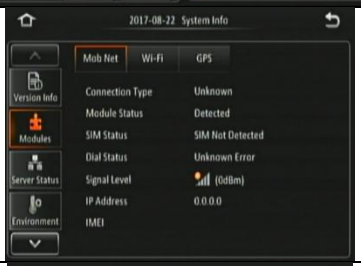
#	SCENARIO	SCREENSHOT	RESOLUTION
(1)	Unable to connect to my Wi-Fi Server		1. Check if you are connected to the MDR Server Wi-Fi network 2. Check your login details 3. Check if the Wi-Fi Windows Server is on 4. Confirm all services are running in the MDR Server software 5. Check if the TLS setting on the MDR Dashboard 6.0 login page matches the server's actual TLS status in config tool.
(2)	Device shows offline		1. Check if the MDR is powered up. 2. Check if the MDR is out of network coverage. 3. Confirm the MDR Network settings 4. Check if the Server status window indicates it is online 5. Confirm SERIAL NUMBER (in MDR-Dashboard settings) = SERIAL NUMBER (in unit settings).
(3)	Able to connect to a device, but cannot see Live Video in MDR-Dashboard		1. Check if Transmit service is running in MDR Server 2. Check if the Streaming IP in Server is set correctly. If set with an Intranet IP address but login MDR-Dashboard with external IP address, the Live View will be unable to show 3. First attempt to stop and restart the service using the MDR Server control window 4. 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 5. Check network speeds, low speeds will result in video loading issues
(4)	DEVICE Dial Status says Failed Dial Up		1. Check if your SIM Data has been activated 2. Confirm the APN settings in the device are correct 3. Check if the Active mode is set to “Always”
(5)	MDR Server services refuse to start		1. Uninstall MDR Server 2. The Microsoft .NET Framework v3.5 SP1 version must be installed, from the following website: https://www.microsoft.com/net/download 3. Re-install MDR Server 4. Run MDR Server as administrator.

#	SCENARIO	SCREENSHOT	RESOLUTION
(6)	I can only view certain channels in Live View, but I know I have 4/8 cameras		1. In MDR-Dashboard 6.0 ensure the number of channels are set correctly – system manage > Vehicle.
(7)	Live View and Playback functions do not work		1. Ensure that the Media Server Port and MDR Server Port on the hardware is correct
(8)	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.

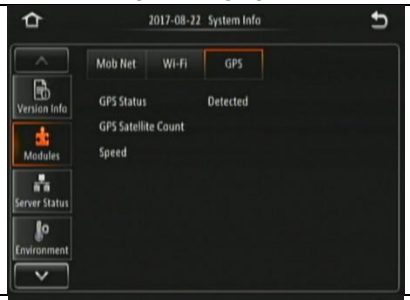
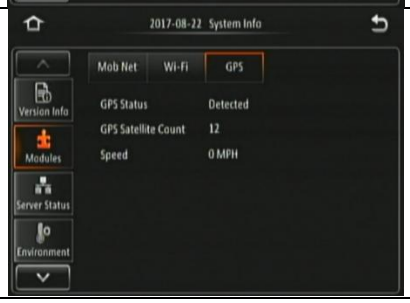
10.2 Wi-Fi MDR Status Troubleshooting

#	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 Sim card not fitted correctly, – sticking out, upside down, dislodged
(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		GPS antenna has not been connected
(2)	GPS Status: DETECTED		GPS Satellite Count being blank indicates that the GPS hardware is broken, or the current environment is not allowing the GPS to obtain satellite signal
(3)	GPS Satellite Count: 1-24		GPS has valid signal and locks onto its position, the higher the value the better
(4)	Speed: 0 MPH		GPS has valid signal and locks onto its position, speed is 0 for a stationary vehicle

11 Glossary

3G – Third Generation
4G – Fourth Generation
AC – Adaptor Cable
ADPCM – Adaptive Differential Pulse-code Modulation
G711U – Narrowband audio codec
G711A - Narrowband audio codec
Alarms – An “EVENT” that has been configured (in the MDR unit settings) to be an alarm. Alarms are identified as orange video channel data on the playback timeline. These are displayed in the real-time alarm log in the MDR-Dashboard and MDR Mobile Apps. Alarms can generate email alerts and trigger automatic downloads (dependant on MDR-Dashboard configuration).
AHD – Analog High Definition
Automatic Download – A download that is set up in the MDR-Dashboard to automatically download data related to an occurring “Alarm” or “Event” between user-defined times. Configured under Download in MDR-Dashboard.
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
EULA – End User License Agreement
Events – An activation of an input e.g., Sensor input (trigger 1-8), G Sensor, Over speed etc. Events are identified as red vertical lines on the playback timeline. These are not shown in the real-time alarm log.
EXP – Expansion
FCC – Federal Communications Commission
FOSS – Free and Open-Source Software
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
H.265 - Video compression standard
HD1 – Half Definition compared to Full Definition (See D1)
HD – High Definition
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 – iPhone Operating System (Apple Inc.)
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
Scheduled Download – A download that is manually setup from in the MDR-Dashboard (to be downloaded when the selected MDR connects to the server). Configured under Server in MDR-Dashboard.
SD – Secure Digital
SIM – Subscriber Identity Module
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
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
WEP - Wired Equivalent Privacy
WPA - Wi-Fi Protected Access
WPA2-PSK - Wi-Fi Protected Access II
WPA2-Enterprise - Wi-Fi Protected Access II Enterprise
TLS - Transport Layer Security
CRL - Certificate Revocation List
HTTP - HyperText Transfer Protocol
HTTPS - HyperText Transfer Protocol Secure