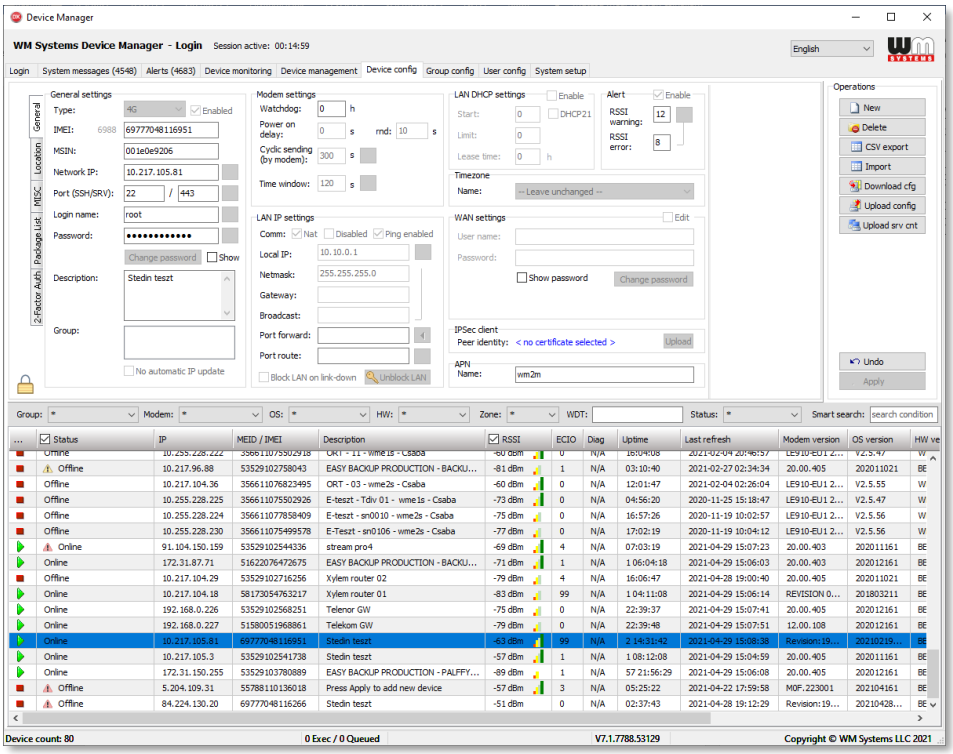
Device Manager®

for M2M Router devices

User Manual

v2.20



2021-08-13

WM Systems LLC 8 Villa str., Budapest H-1222 HUNGARY
Phone: +36 1 310 7075
Email: sales@wmsystems.hu Web: www.wmsystems.hu

Document specifications

This document was made for the **Device Manager®** software and it contains the detailed description of configuration and usage for the proper operation of the software.

Document category:	User Manual
Document subject:	Device Manager®
Author:	WM Systems LLC
Document version No.:	REV 2.20
Number of pages:	32
Device manager version:	v7.1
Software version:	DM_Pack_20210804_2
Document status:	FINAL
Last modified:	13 August, 2021
Approval date:	13 August, 2021

Table of contents

Chapter 1. Introduction

The Device Manager can be used for remote monitoring and central management of our industrial routers, data concentrators (M2M Router, M2M Industrial Router, M2M Router PRO4) and for smart metering modems (WM-Ex family, WM-I3 device).

A remote device management platform which provides continuous monitoring of devices, analytic capabilities, mass firmware updates, reconfiguration.

The software allows to check the service KPIs of the devices (QoS, life signals), to intervene and control the operation, running maintenance tasks on your devices.
It's a cost-effective way of continuous, online monitoring of your connected M2M devices on remote locations.

By receiving info on the device's availability, the monitoring of life signals, operation characteristics of onsite devices - owing to the analytics data derived from them - it continuously checks the operation values (signal strength of the cellular network, communication health, device performance).

With the usage of the application - as a service provider or maintenance company - you can manage the installation of new firmware releases for groups or devices, or distribute a basic configuration for a bunch of devices.

The Windows®-based application provides the possibility to install or replace the firmware running on the device. In addition, you can install or replace certifications (CSR, CA certifications, etc.) for your devices.
You can configure the usage of the encrypted TLS protocol communication between the M2M device and the Device Manager® software.

You can also remotely control your devices (rebooting them or executing other tasks on the device).

The application enables the grouping, arrangement and management of devices in groups according to on-site installation or according to other logic. In this way, you can manage the installation of new firmware releases and the maintenance of devices individually or even per installation site.

Chapter 2. Setup and Configuration

2.1 Prerequisites

Approximately 10 000 endpoint devices (routers) can be managed by a Device Manager.

Here we describe the software usage with our router devices (M2M Router, M2M Industrial Router, M2M Secure Industrial Router, M2M Router PRO4) and data concentrators (M2M PRO4 DCU, M2M PRO4 Mbus, M2M PRO4 wMbus).

The usage of Device Manager client application requires the following conditions.

Hardware environment:

- Physical or virtual environment supported
- 2 Core Processor (minimum) - 4 Core (preferred)
- 4GB RAM (minimum) - 8GB RAM (preferred)
- 1Gbit LAN connection
- 500MB free disk space

Software:

- Windows 10, 64-bit family
- Other operating systems are not supported

2.2 System elements

The Device Manager consists of one main software element:

- Device Manager UI – for monitoring and control the devices.

Device Manager UI

This is the device management user interface, and business logic. It communicates with the Data Broker via a REST API, and with the M2M devices through WM Systems' proprietary device management protocol. The communication flows in a TCP socket, which can optionally be secured with industry standard TLS v1.2 transport layer security solution, based on mbedTLS (on the device side) and OpenSSL (on the server side).

2.3 Installation

1. Create the root folder on the destination system. eg. C:\DMv7.1
2. Unzip the Device Manager compressed software package into the folder.

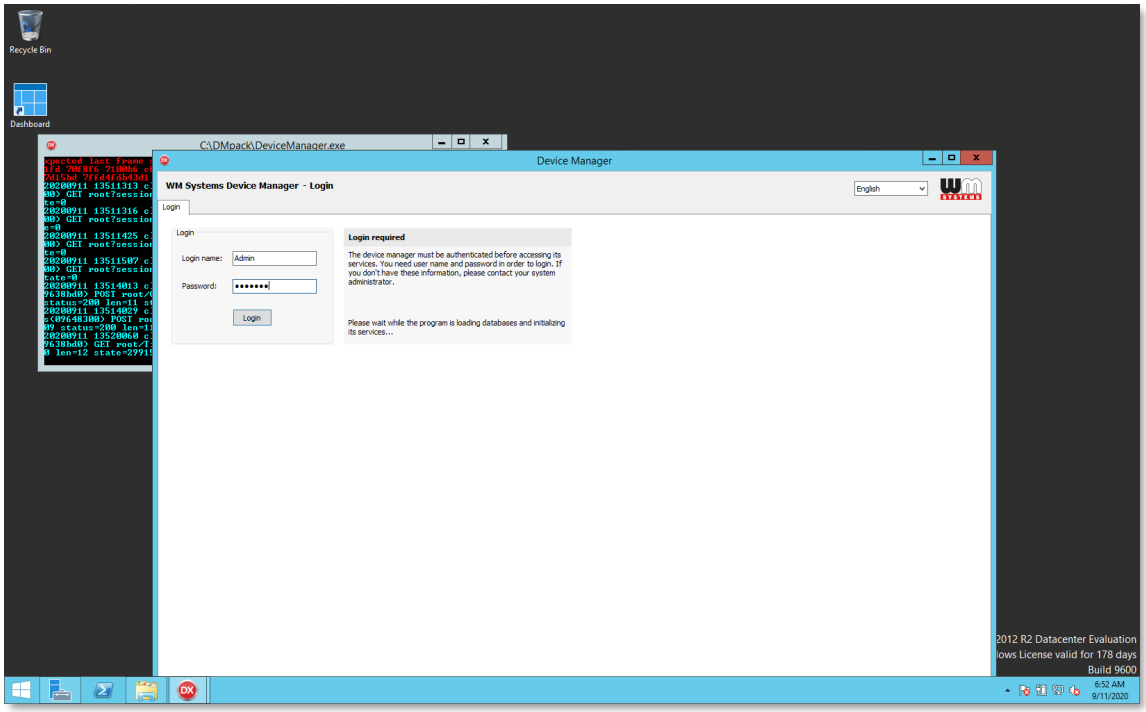
3. Modify the configuration file: *DeviceManager.config*

   (This is a JSON based configuration file which must be modified in order for the Data Broker to access the SQL Server.)

   You must set the following recommended parameters:

   - *DataBrokerAddress* → IP address of the data broker
   - *DataBrokerPort* → communication port of the data broker
   - *SupervisorPort* → communication port of the supervisor
   - *ServerAddress* → external IP address for the router communication
   - *ServerPort* → external port for the router communication
   - *CyclicReadInterval* → 0 – disable, or greater than 0 value (in sec)
   - *ReadTimeout* → parameter or state reading timeout (in sec)
   - *ConnectionTimeout* → connection attempt timeout to the device (in sec)
   - *ForcePolling* → must be 0
   - *MaxExecutingThreads* → max paralel threads in same time (recommended: dedicated CPU core(s) x 16, eg.: if you dedicated 4 processor cores for the Device Manager, then the value should be 64)
   - After saving the modifications of the config file, please run the **DeviceManager.exe**

4. Now this will connect to the database server through the Data Broker. The Device Manager® software will then be started soon.

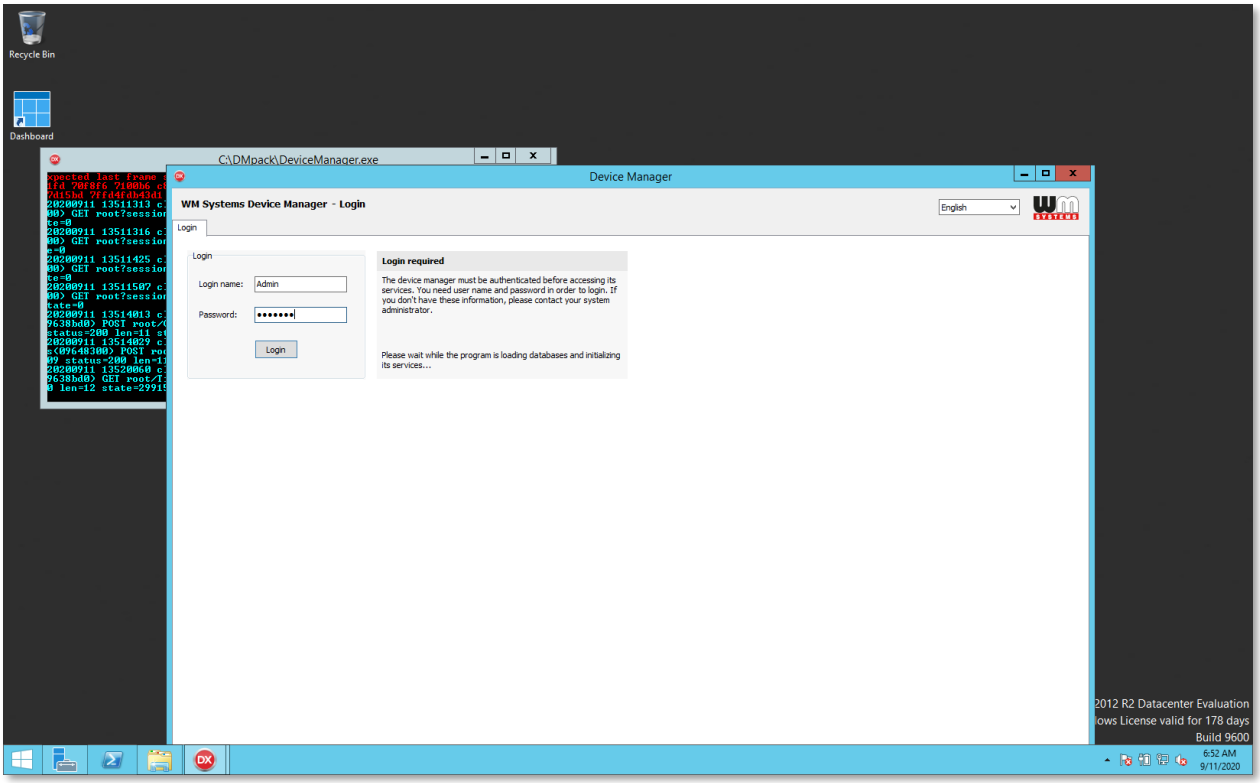


5. You have to **Login** by the following creditentials:

   - **Login name**: ***Admin*** - **Password**: ***synopse***

   (The login data are case sensitive!)

6. Press the **Login** button to enter into the system.



Important!

Consequently, only those services, views and data are visible for the current – and logged in – user, which he/she has got access / permission to. These can be limited by configuring the user rights.

Note, that in case of using Active Directory, current rights and access level of those AD-users are specified by user groups in the Device Manager.

2.4 TLS protocol communication

The TLS v1.2 protocol communication feature can be activated between the router and the Device Manager from the DM software side (by choosing TLS mode or legacy communication).

It used mbedTLS library on the router side, and OpenSSL library on the Device Manager side.

The encrypted communication is packed into a TLS socket (double encrypted, highly secure method).

The used TLS solution uses a mutual authentication method to identify the two parties involved in a communication. This means that both sides have a private-public key pair. The private key is visible only to everyone (including the DM and router), and the public key travels in the form of a certificate.

The router firmware includes a factory default key and a certificate. Until you have your own custom certificate from DM, the router will authenticate itself with this embedded.

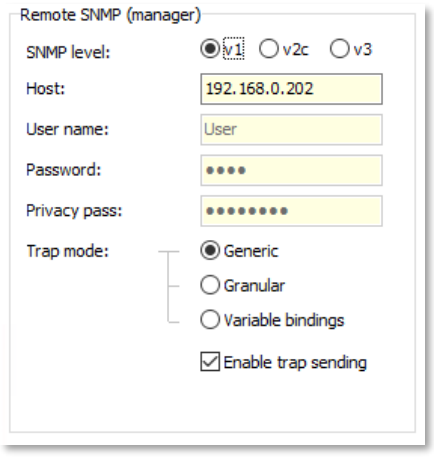
Only factory default is implemented on the router, so the router does not check whether the certificate presented by the connected party is signed by a trusted party, so any TLS connection to the router can be established with any certificate, even self-signed.

(You need to know the other encryption that is inside the TLS, otherwise, the communication will not work. It also has user authentication, so the connected party does not know enough about the communication, but you also have to have the root password, and successfully self-authenticate).

Chapter 3. System configuration

3.1 System setup

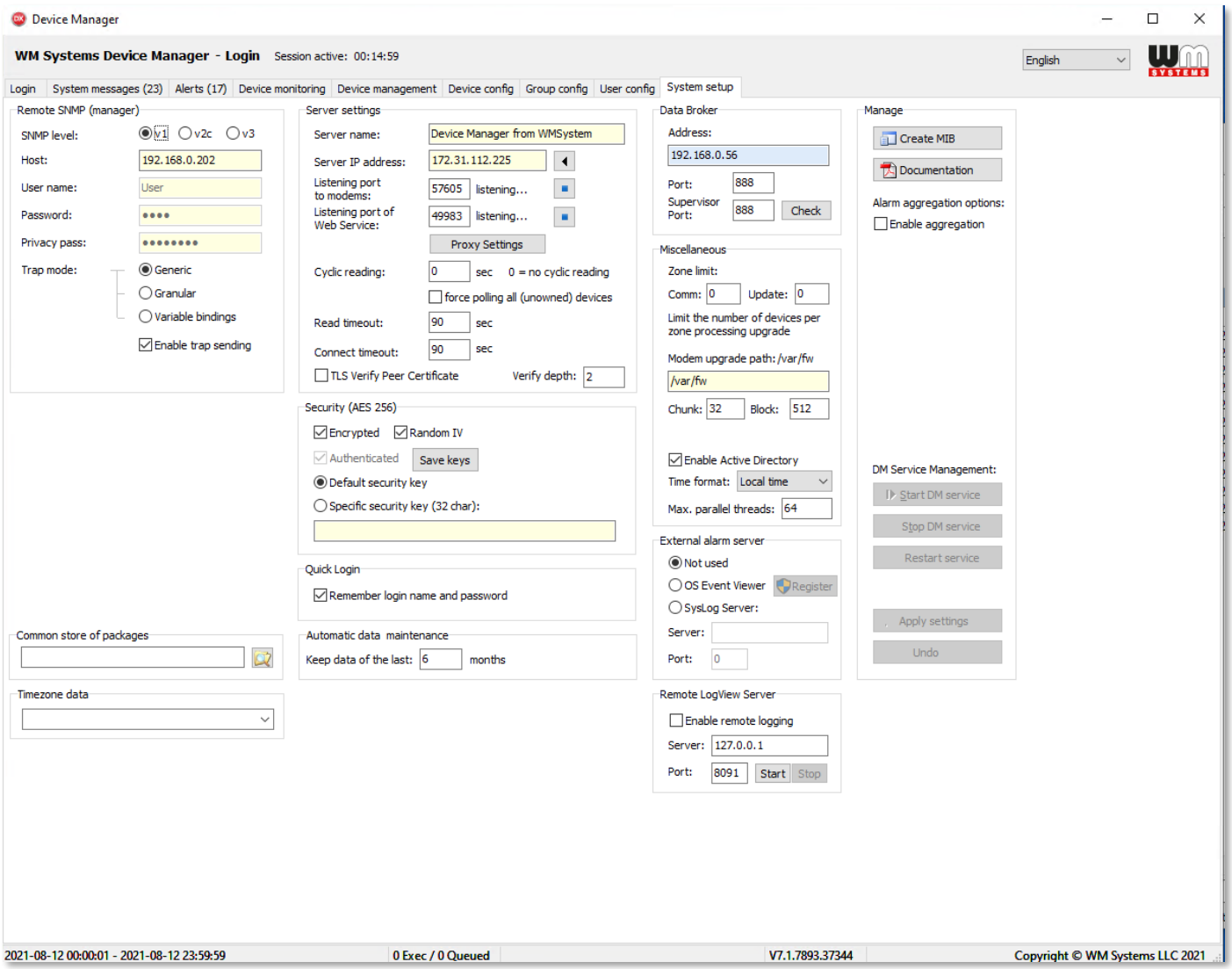
After login to the system, choose first the **System setup** tab. Each parts of the screen are listed here with the relevant fields. The Device Manager application has some default parameters of operation, but is must be checked, if necessary should be modified.



Remote SNMP (manager)

The Device Manager uses SNMP manager to collect data of connecting devices (e.g. routers). It sends the following SNMP traps to the SNMP server and the devices are sending their events:

- 1.3.6.1.6.3.1.1.5.1 – Cold Start
- 1.3.6.1.6.3.1.1.5.2 – Warm Start
- 1.3.6.1.6.3.1.1.5.3 – Ethernet link down
- 1.3.6.1.6.3.1.1.5.4 – Ethernet link up



- 1.3.6.1.6.3.1.1.5.5 – Authentication failure (unauthorized login attempt or wrong password)

The SNMP trap contains: system uptime, snmpTrapOID, device database ID, MEID (IMEI), IP, event name.

SNMP level: you can configure the SNMP protocol type (v1, v2c or v3)

Host: The SNMP server IP address

For the SNMP agent you have to define the following authentication data too.

User name: Login to the SNMP host

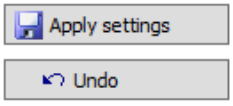
Password: Password to the SNMP host

Privacy pass: Required when the v3 SNMP level is selected. The authentication is possible by any of the SNMP-enabled users plus the privacy pass specified here. Of course, this setting must be the same at that of the SNMP manager.

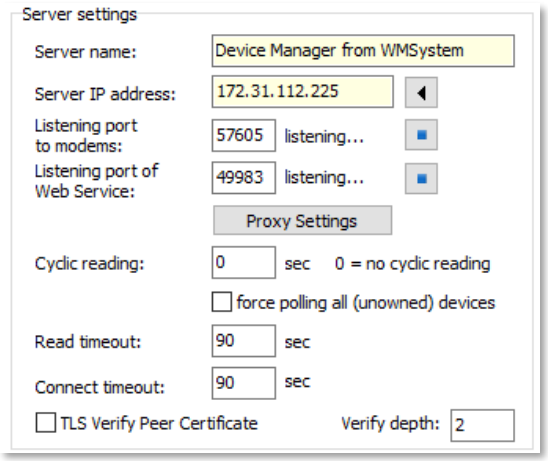
Trap mode: depending on the manager's capabilities, the program can send traps with the so-called variable bindings providing detailed information about the event and the relevant node.
You can allow here the *trap sending*, and select the usage of:

- ***generic***: Sending the standard traps only (coldStart, warmStart, linkDown, linkUp, authentication failure) without further details. This setting is for compatibility reasons to provide solution for the SNMP manager if it can only handle the standard traps.
- ***granular mode***: Sending the so-called granular trap with the unique object identifier of the device allows the SNMP manager to distinguish them from each other. The meaning of these IDs are stored in the DM generated Management Information Base (MIB) file.
- ***variable bindings***: Sending detailed information to the SNMP manager about the related object or device. Data is encoded within the SNMP trap itself using the technique of "variable bindings".

If you changed something, in case of failure, it can be revoked by the **Undo** button. When you want to save the settings, press the **Apply settings** button.



Server settings



The server uses API for presenting the collected and evaluated data for the operators. Here you can configure these settings.

Server name: Unique server name. This parameter does not affect the Device Manager operation.

Server IP address: IP address of the Device Manager server, where the devices send their data.

Listening port to modems: listening port number of data collection service (to receive the incoming messages)

Here you can stop the listening services by  *icon.*

Listening port of web service: is a future option. In this version of Device Manager, this feature not working!

Proxy settings *button*: you can disable the proxy here, or you can configure for **manual** where the ***HTTP proxy*** server name and its ***Port number*** are necessary to be defined.

Cyclic reading (sec): you can define a periodic reading of the devices. The Device Manager can poll devices in a cyclic manner when configured to do so. The zero value equals to no polling. However, we advise to setup a longer cycle (like a day or hour) for device monitoring. If you use a server service, please set this value to 0. When you use server service, then this parameter does not affect the DM operation. You can modify this parameter in the service configuration file.

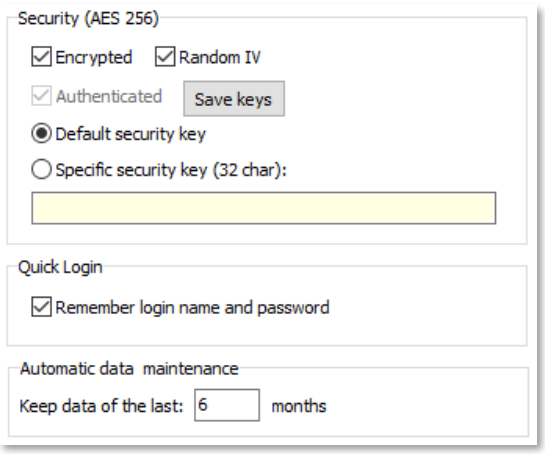
Force polling all (unowned) devices: The client application is able to receive the devices data directly. In this case the application is able to polling the direct communicating devices and the main server devices too. In normal case this feature is disabled. Optional to use.

Read timeout (sec): configurable timeout for reading the devices. The read timeout of communication with devices should be fitted to the worst node of the network. When you use server service, then this parameter does not affect the Device Manager operation. You can modify this parameter in the service configuration file.

Connect timeout (sec): here you can define the connection timeout for the devices. When you use server service, then this parameter does not affect the DM operation. You can modify this parameter in the service configuration file.

Security (AES 256)

Option: **Encrypted**: you can allow the data encryption here



Option: **Random IV**: random vector tag for the authentication process – you can enable it for a higher level of security

Authenticated: you can allow the authentication by seleting the **Save keys** *button:*

- **Default security key**: you can choose the default key
- **Specific security key** (32 char): or you can specify a special security key here.

Quick Login

Remember login name and password: to save your login creditentials

Automatic data maintenance

You can define data retention length here (value in months).

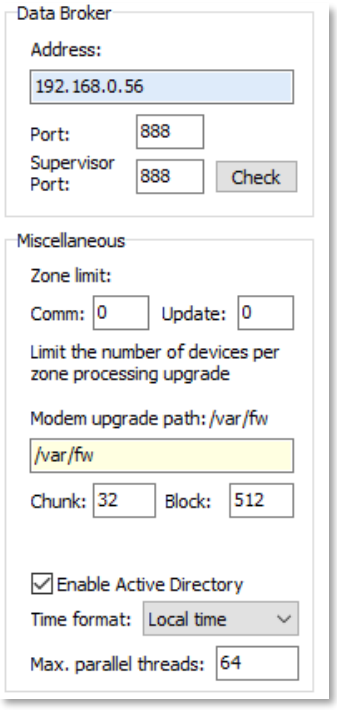
Data broker

Address: Broker IP address (data connector between the DM server and the remote clients)

Port: port number of the broker

Supervisor port: supervision port number

You can **Check** the accessibility of the configured supervisor service.



Miscellaneous

Zone limit: Restricts the number of simultaneous uploads to modems in the same zone (In the case of non-cdma devices the zone is 0). Thus reduces the load of the network. Recall that users can initiate upload upgrade packages in the Device Manager screen to a large number of devices, and even to all devices in the network. If you use CDMA devices,

without these settings, the CDMA network could be easiliy overloaded, and freeze. We offer to configure these limits.

- **Comm**: the client can communicate with this number of devices at a time when reading or sending data to the devices
- **Update**: the client can update with this number of devices at a time

Modem upgrade path: where the modem upgrade files (firmware) are stored temporary on the device. The default path is: /tmp/fw

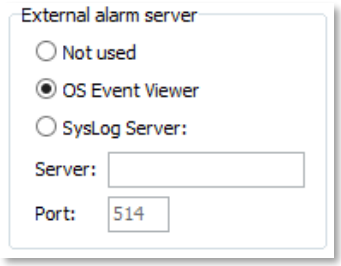
Enable Active directory: you can enable or disable the AD service for the Device Manager here

Time format: can be *Local time* or *UTC*

Max. parallel threads: Max. how many threads can be simultaneously executed by the system

External alarm server

The client can send device alarm messages to the event log of the operating system or for the external syslog server. Here you can configure these.



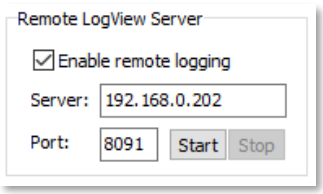
- **Not used**
- **OS Event Viewer**
- **SysLog Server –** *Note that this feature in the DM is not yet working*
  - **Server**: Syslog server IP address
  - **Port**: Syslog server port number

Remote LogView Server

Option: **Enable remote logging** – you can enable or disable the feature

Server: IP of the LogView server

Port: port number of the LogView logging server

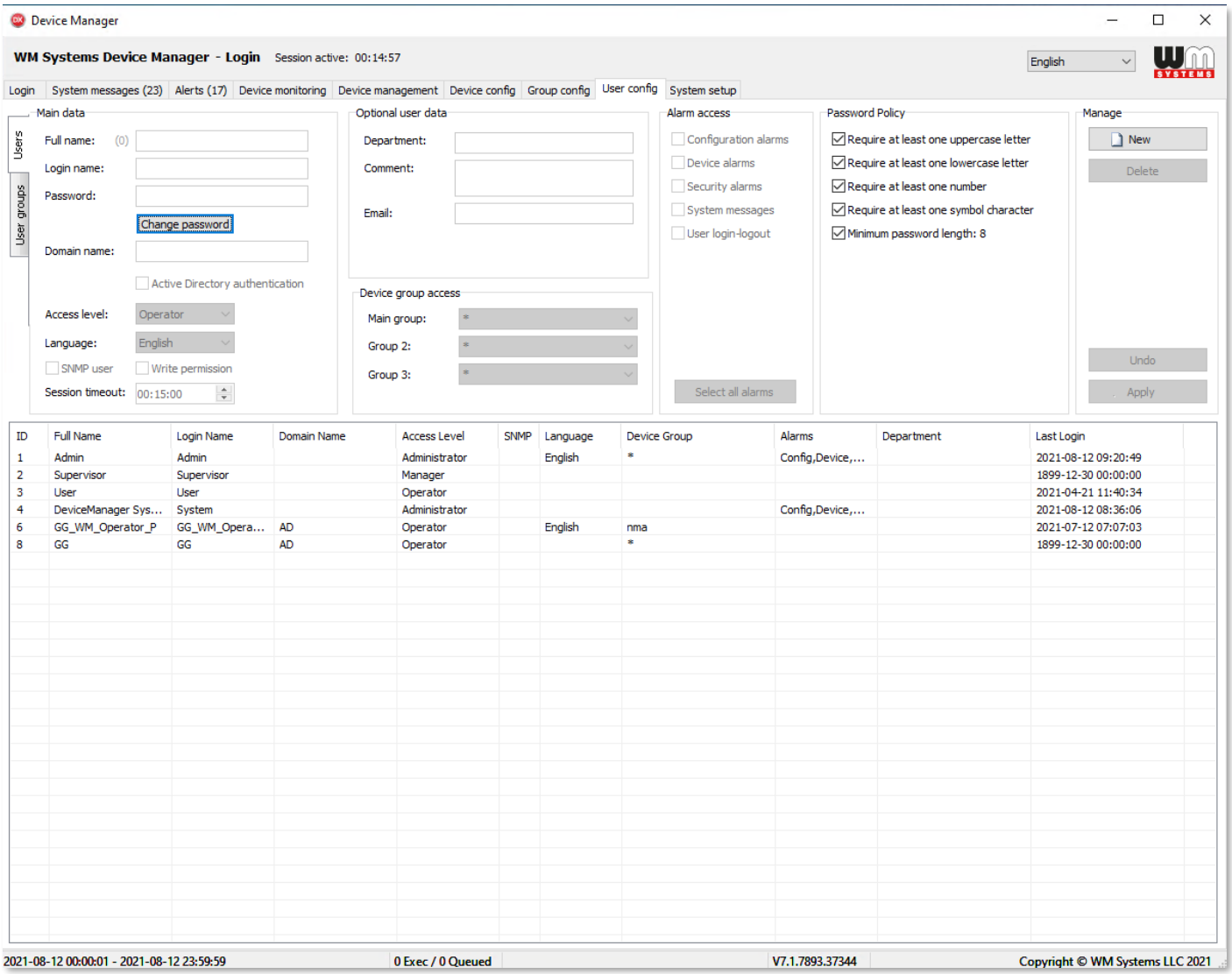


3.2 User settings

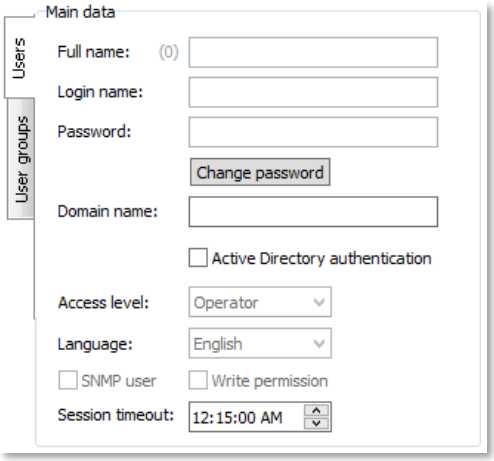
The DM features are available only for authenticated users who have permissions. The user-level and group-level configuration can be achieved in the **User config** tab.

In this screen, you can see the listed existing users and groups here. By selecting one, you can modify their data. Or you can create a new one by the 

button at right of the screen.



Main data



Full name: User real name

Login name: Name for login access

Password: Authenticating for login name

If you to change the password, select the user and press the 

button.

Domain name: you can define the domain for the account

You can enable the **Active directory authentication** also.

Access level:

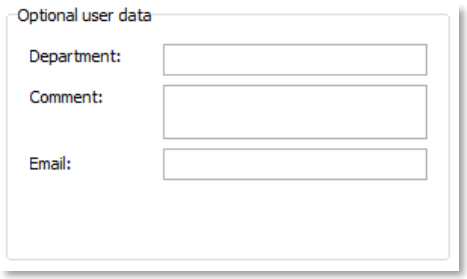
- **Disabled** – with this access level, you can disable the selected user. The selected user not able to access to the program.
- **Administrator** – full access to all services including user config and system setup + SNMP
- **Manager** – device configuration only on top of the system messages and monitoring
- **Operator** – can only visit the system messages and the device monitoring screens

Language: user interface language.

Session timeout: automatic logout can be also defined.

Optional user data

Department: office, company department of the user

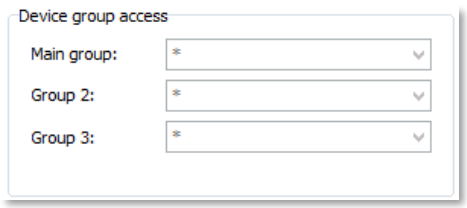


Comment: free text

Email: email address of the user (the DM is not able to send email to the user!)

Device group access

Main group: choose a defined device group for the user (branch of devices)



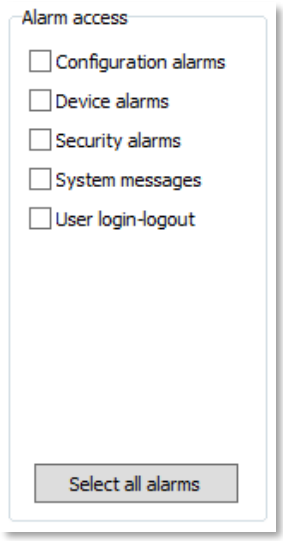
Group 2: you can choose further and additional device group for the user account (not obligatory to use)

Group 3: you can choose further and additional device group for the user account (not obligatory to use)

Alarm access

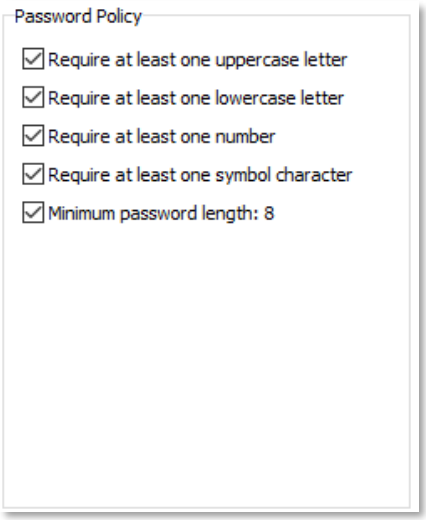
You can select the alarm notification types for the user account.

With the **Select all alarms** button you can turn on every alarm groups at once.



Password Policy

Here you can define requirements and obligatories for the password usage.



Chapter 4. Device settings

4.1 Device group configuration

At the **Group config** tab, the device groups can be checked and modified here.

Choose a **Group name** and see the marked devices below.

If you want to add more devices for an existing group, just check in the new device(s).

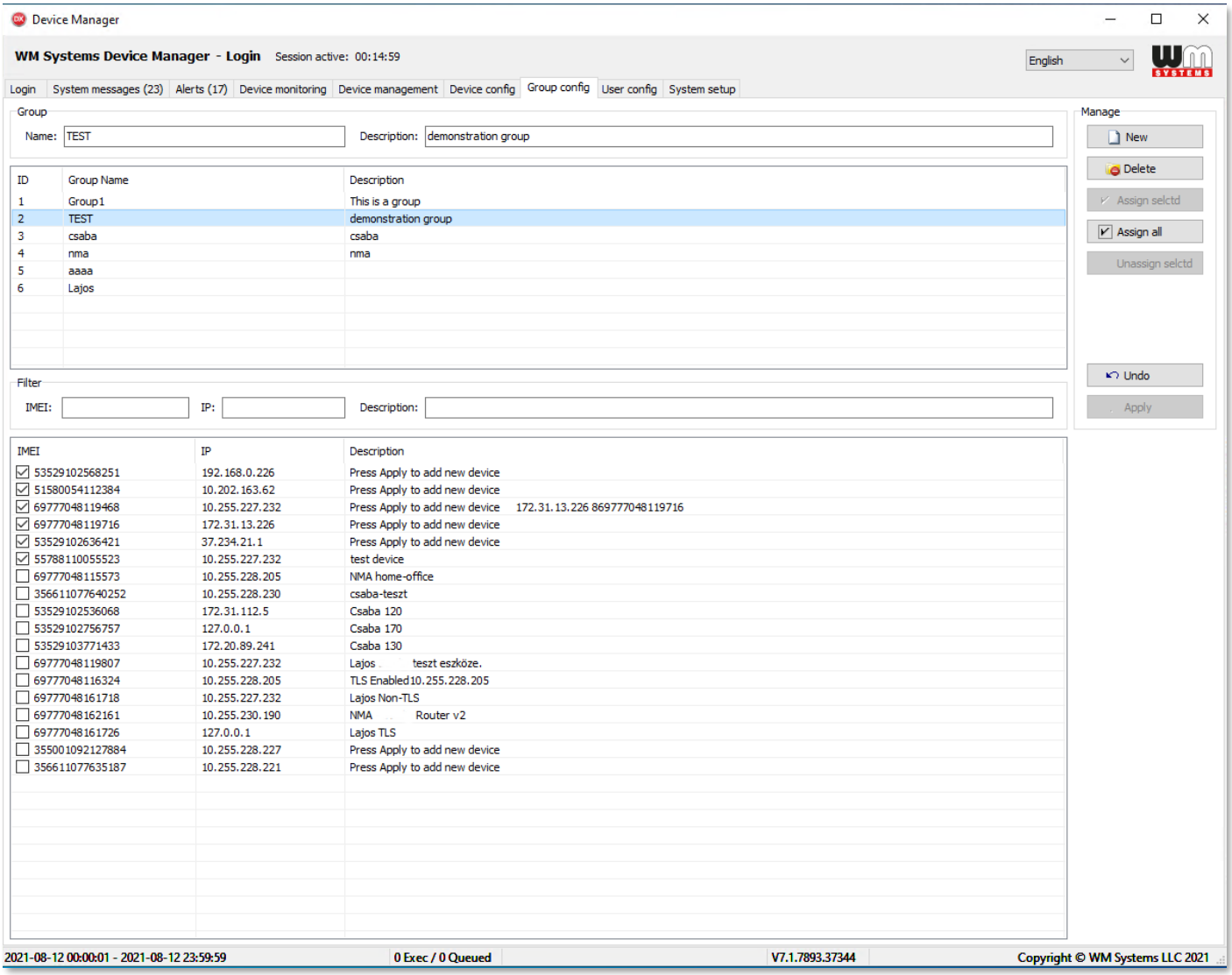
The **Assign all** button will mark all the devices for a selected group.

A new device group can be also defined here.

Press the 

button for making a new group and fill in the **Name** field (mandatory) and the description (optional).

Press the **Apply** button for saving the settings.



After the group creation, you can able to select even more devices for a group. You can see the Device Manager managed devices at the bottom side. The selected devices will automatically assign to the designated group.

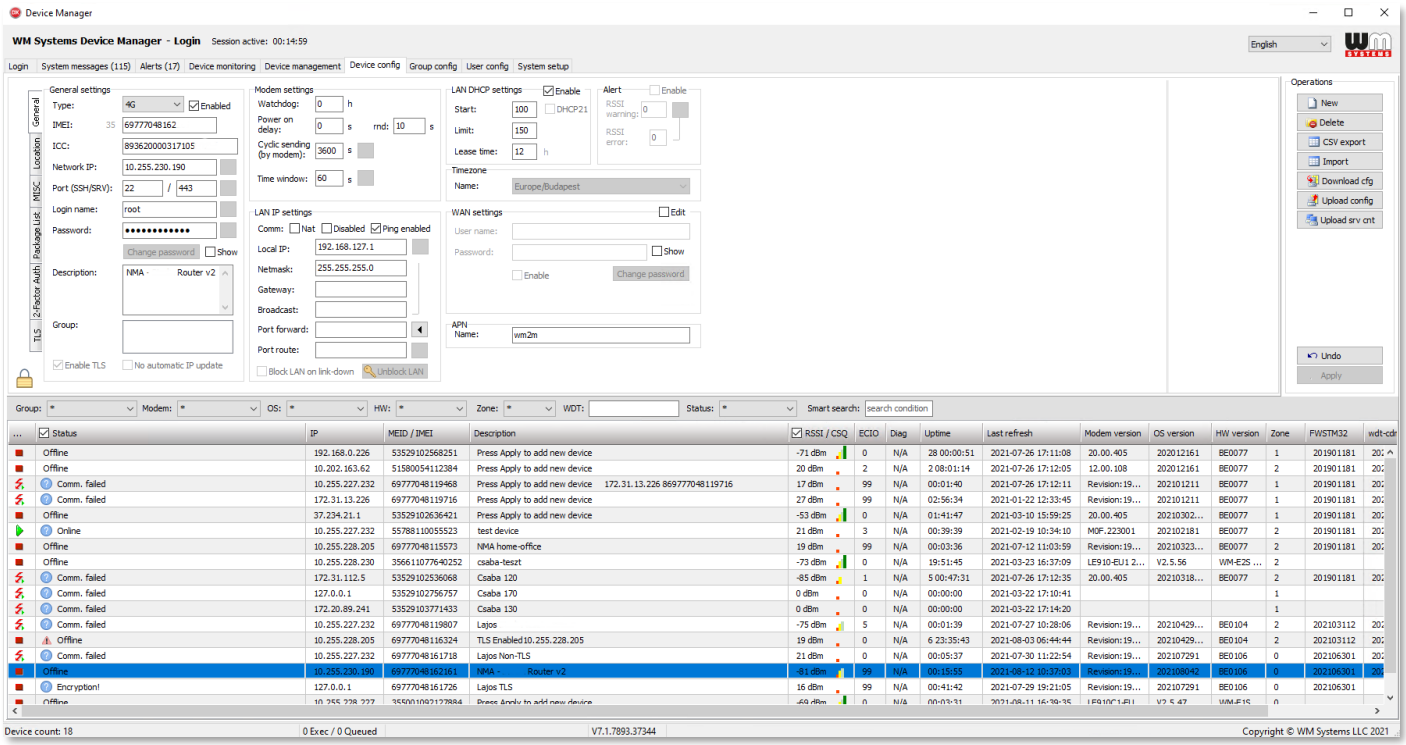
4.2 Device configuration for routers

At the **Device config** tab, you can check the current settings of a device. You can filter the list results if you want or select a device.

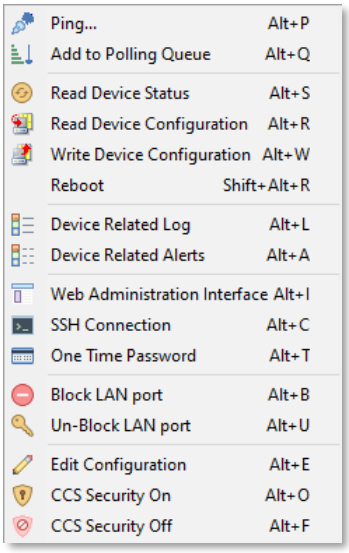
Filters:

- Group → device group filtering
- Modem → modem firmware version filtering
- OS → device firmware version filtering
- HW → device hardvare version filtering
- Zone → it is working with CDMA devices only
- WDT → it is working with CDMA devices only
- Status → device status filtering
- Smart search → the typed characters will be search entire the database by this function

On this screen you can see all devices with current **Status** (*Online*, *Offline*, *Disabled*, etc).



You can check the device- and network properties (**IP** address, **IMEI/MEID**), their availability by analysing the **Last Refresh** information (date/time of last known status) with the **Uptime** (when the device was rebooted / started last time).

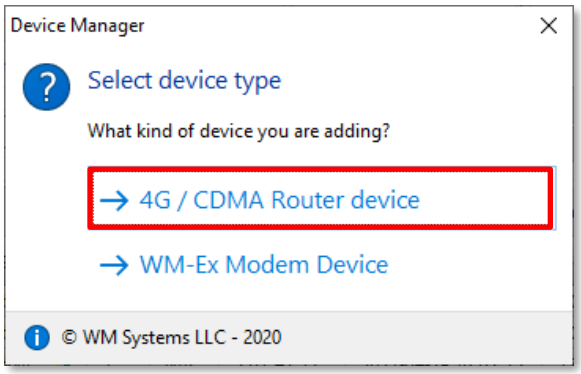


The cellular network performance indexes are also available at **RSSI** / **CSQ** (signal strength), **ECIO**.
The **Modem version**, **OS version** (date of the build), **HW version** (PCB identifier), **FWSTM32** (Microcontroller firmware version) are also available here.

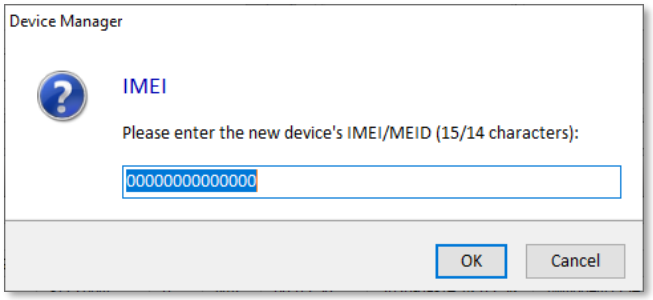
When you've selected a device from the list, you can click with right mouse button to the element, and the following right submenu appears, where you can choose from the available features to perform an interaction on the device.

You can also add further new devices by the  button.

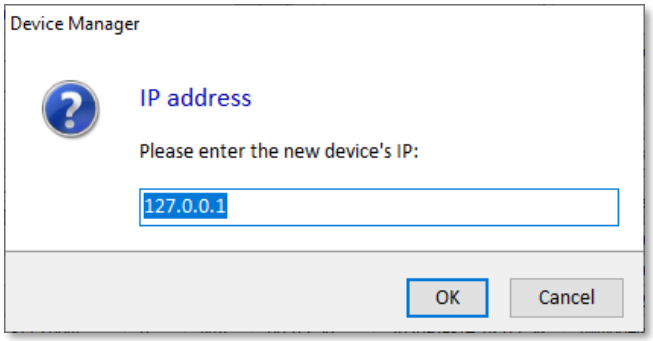
For routers you have to first select the device type: **4G / CDMA Router device**.



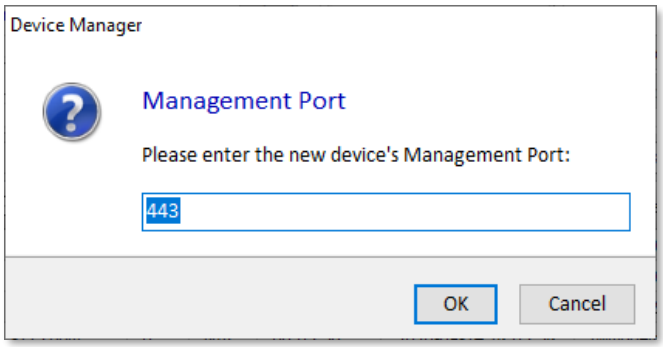
Then you have to enter the **IMEI/MEID** number of the cellular module of the router - as a unique identifier.



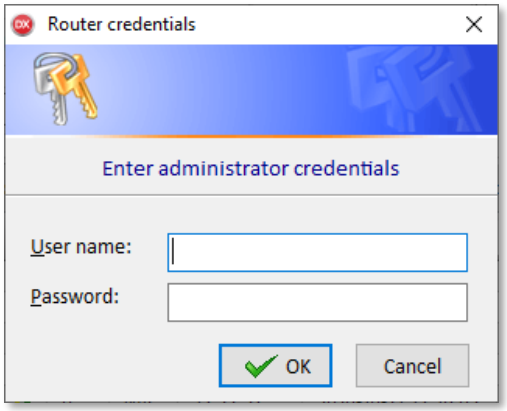
Add the **IP address** of the device.



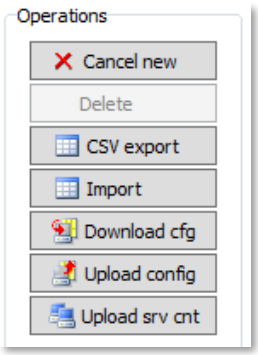
Add the **DM management port** number which is already configured on the endpoint device's side (at the router side). The Device Manager will connect to the router through this port.



Then you have to fill the administrator creditentials (**user name, password**) to add the new device to the Device Manager.



After selecting a device from the list, you can use the configuration command buttons from the right sidebar.



- **Cancel new**: will cancel the new device configuration or modifications
- **Delete**: this will delete the current / selected device(s) from the device list
- **CSV export**: you can export the device list with configuration data into CSV file

- **Import**: you can import devices with configuration into the database from CSV or XML file
- **Download cfg**: you can download the current configuration from the device into the database – when it will be online.
- **Upload config**: you can directly upload a configuration to the device when it will be online
- **Upload srv cnt**: you can upload the server settings (IP, port) from the current client

Now let's check the **Device configuration** tabs one by one.

4.3 General settings

On the **General** tab **General settings** part, you can get information about the device and its operation, then it will be listed here.

IMEI – Device's cellular module's unique identifier

MSIN – CDMA450 router specific identifier (because there is no available IMEI number) – not used for 4G LTE or other type of routers

Network IP – device IP address

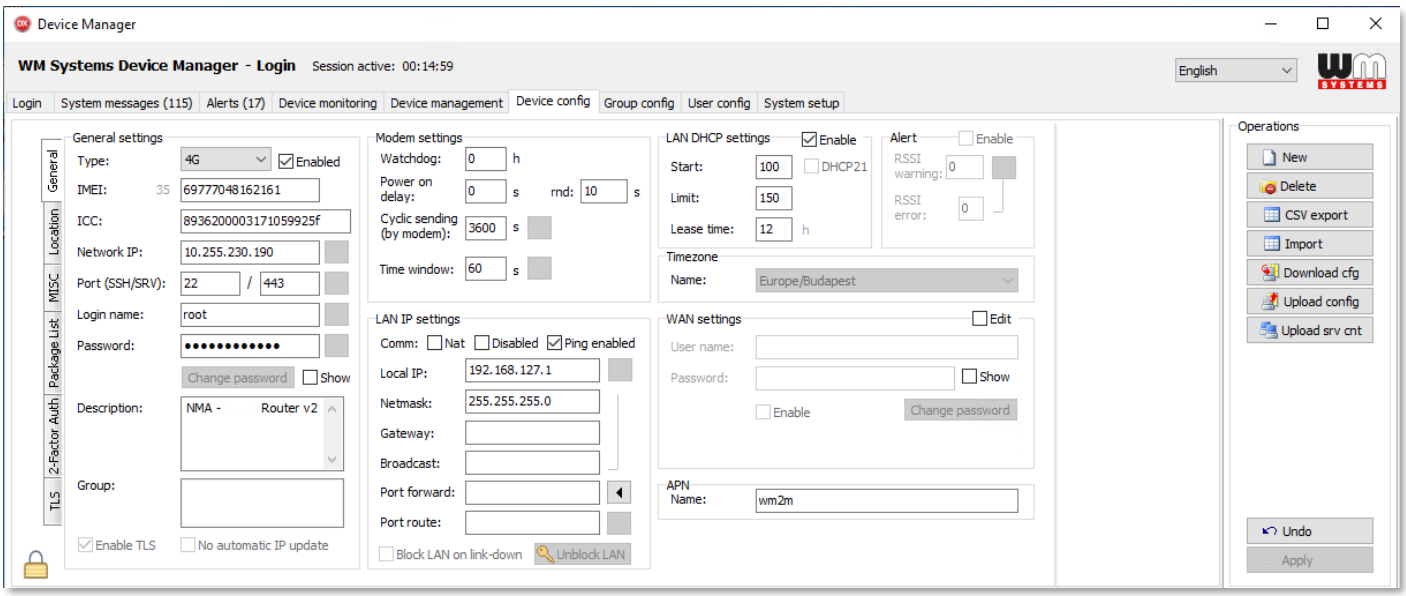
Port (SSH/SRV) – device's SSH port number and the Device Manager communication port number

Login name – device's admin account name

Password – password for login

Description – You can add further information about the device. It is a free text content.

Group – Group information



Modem settings part

Watchdog – watchdog module monitoring interval (value in hours)

Power on delay – you can define the delay for power on (in seconds)

Cyclic sending (by modem) – cyclic data sending interval (in seconds)

Time window -

LAN IP settings part

Comm. (Nat / Disabled / Ping enabled) – you can choose of these

Netmask – IP netmask

Gateway – Gateway IP address

Broadcast – Broadcast IP address

Port forward

Port route

LAN DHCP settings part

Option: **Enable –** enable the DHCP service here

DHCP21 – you can enable the DHCP21 option

Start – Beginning IP address

Limit – Number of max. given IP addresses

Lease time – Renewal time interval

Time zone part

Name

WAN settings part

User name

Password

APN part

Name – APN name for cellular network registration

Alert part

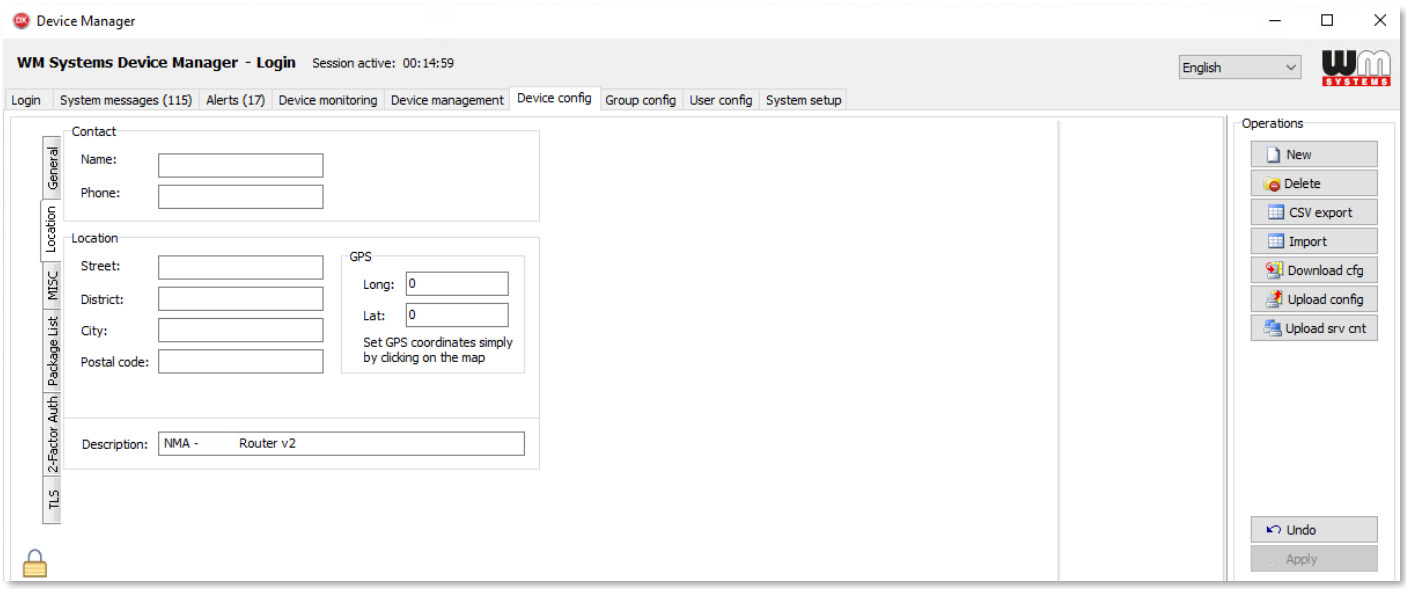
Option: **Enable** – you can enable the RSSI monitoring feature

RSSI warning – low cellular signal strength value

RSSI error – critical low cellular signal strength value

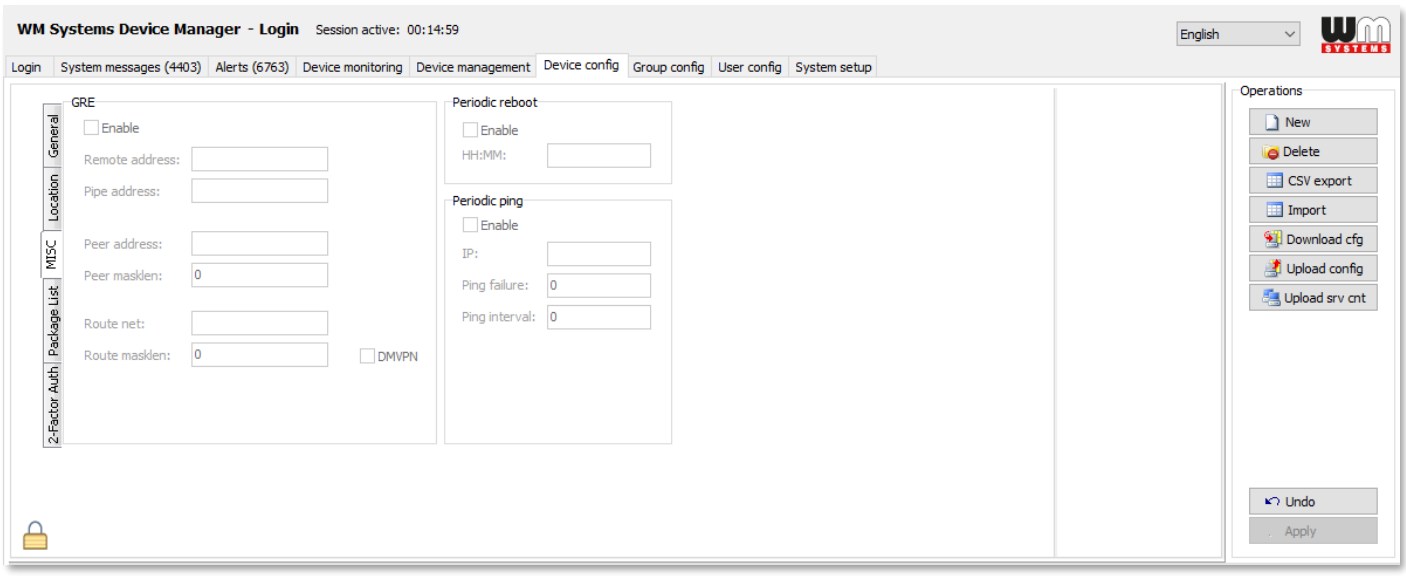
4.4 Location settings

At the left **Location** tab, you can configure the device's location information (contact, address, description, etc).



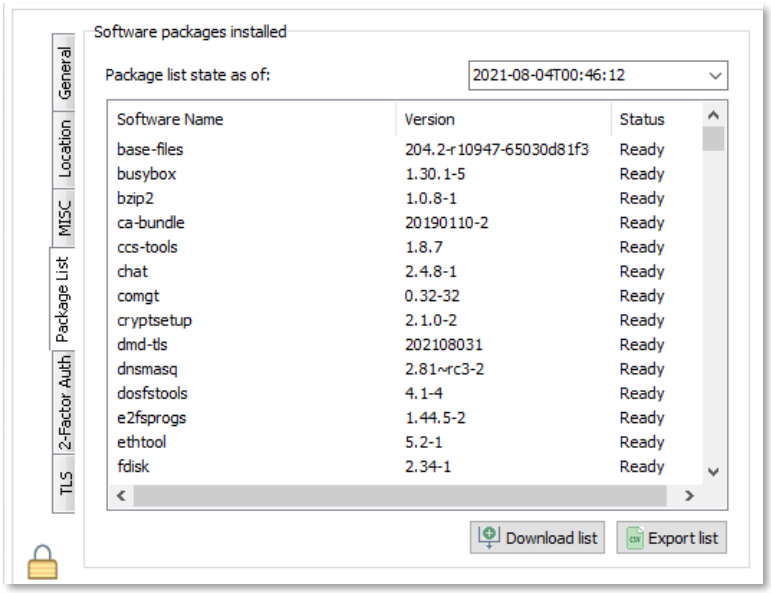
4.5 Miscellaneous settings

The **MISC** tab at left will allow to use GRE or apply **Periodic reboot**, **Periodic ping** features on the device.



4.6 Package List

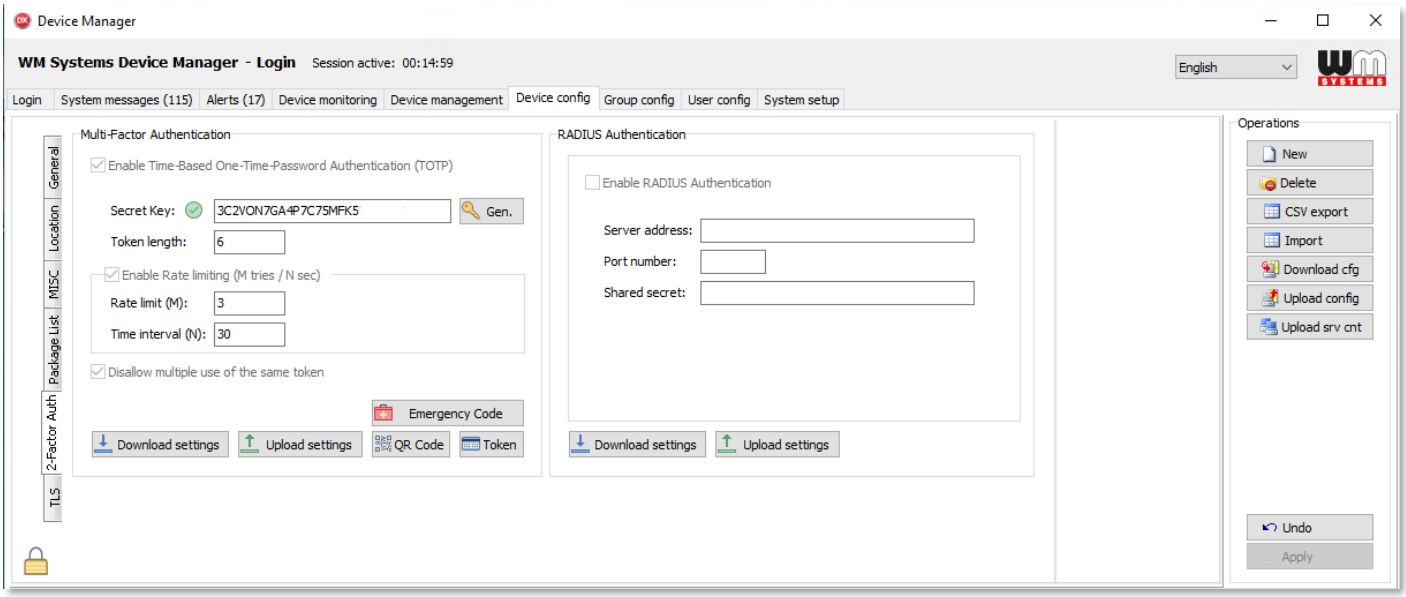
The **Package List** tab shows the installed software components, sw tools of the device. You can **Download list** or **Export list** (to a file).



4.7 2-Factor Authentication settings

The **2-Factor Auth** tab can be used for configuring the **Multi-Factor Authentication** feature, where you can add a **Secret key** or define a new one by the **Generate** button.

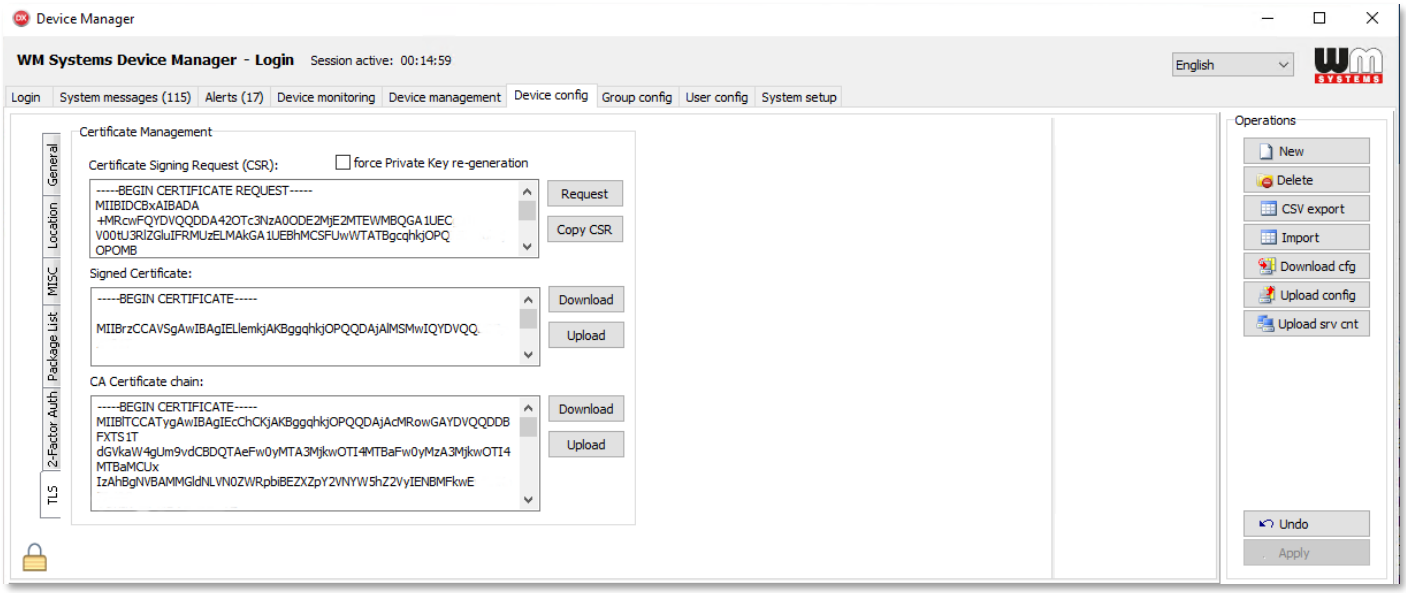
Further options are the **Token length**, **Rate limit** or the **Time interval** fields, here.
Here you can also select the **Download settings** or **Upload settings** by its buttons for the easier configuration.



The **RADIUS Authentication** feature can be also configured here if you require. For that, fill the **Server address** (of Radius server), **Port number** (of the server) and **Shared secret key** fields for the safe connection.

4.8 TLS settings

At **TLS** tab you can configure the TLS v1.2 protocol compatible communication for the router(s). If you allow the feature, then the device will communicate with the Device Manager software with this protocol.



At the **Certificate Signing Request (CSR)** you can **Request** the CSR file, or you can choose the **Copy CSR** button.

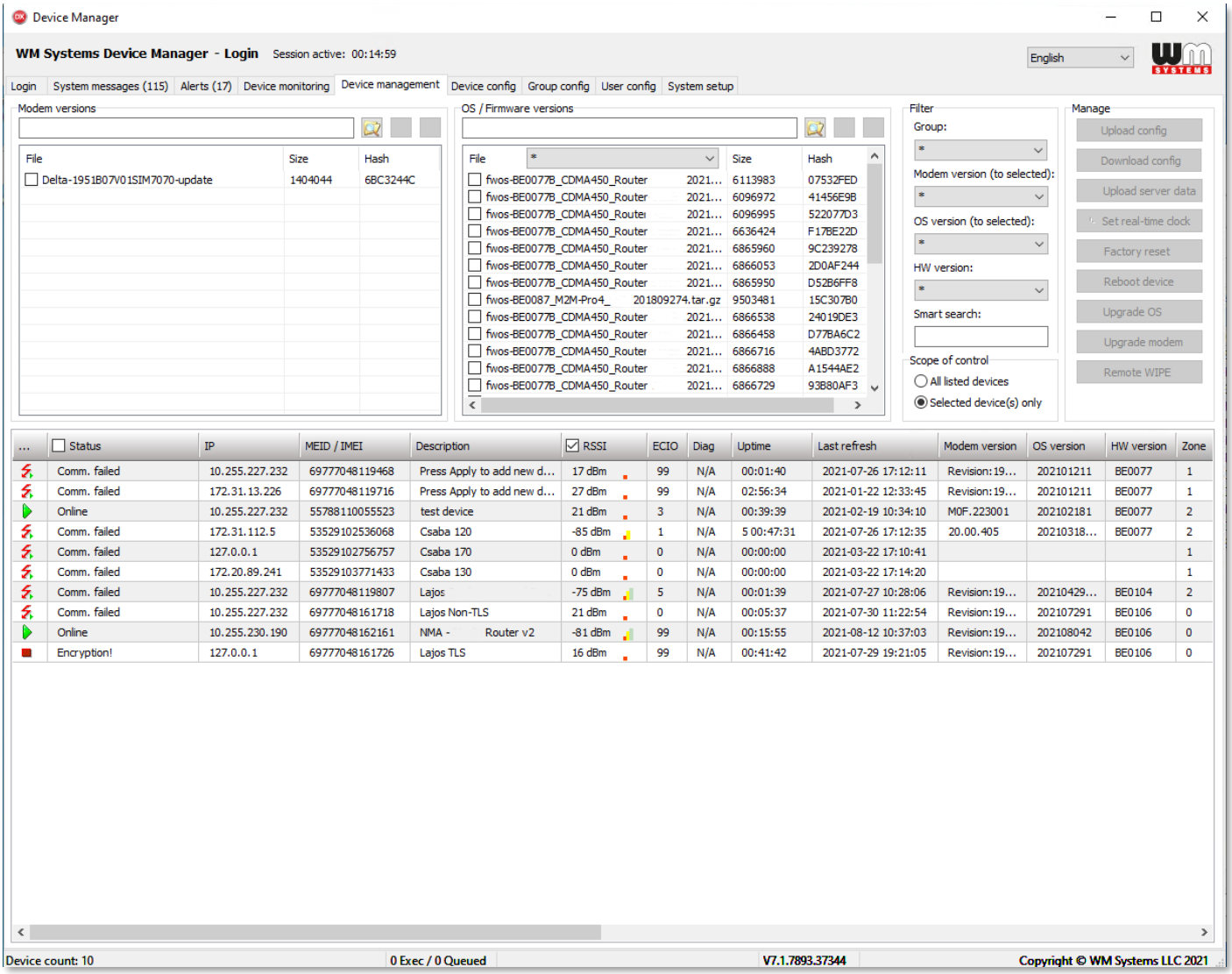
You can also define the **Signed Certificate** for the TLS communication – **Download** or **Upload** the certificate.

The **CA Certificate chain** can be also requested to **Download** or you can **Upload** one.

After choosing a certificate method, the **TLS handshake** will be signed at the **Status** of the device and the requested action will be performed.

Chapter 5. Device Management

On the **Device Management** tab, you can remotely manage the devices by various commands. At first, choose a device or a branch or group of devices and the right command buttons will be active.



As you can see, next to the pictograms, there are listed stopped, disabled (red) and online (green) devices.

Three you will find the device's IP address and IMEI data.

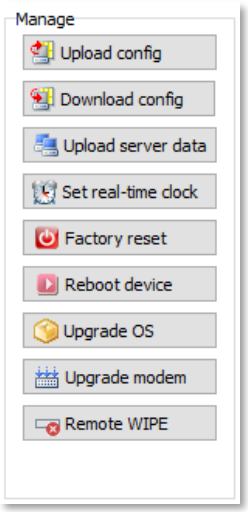
QoS information are available in the following coloumns: **RSSI** (mobile network signal quality), **EC/IO** (signal interference quality), Uptime.

The device **Modem version** and the operating system / firmware version (**OS version**) are also listed.

The validity of the data valid for the device can be checked in the **Last refresh** column.

Important! Note that the data is not fully real-time, the status values show the last known operational behavior and vital signs.

At right, you can browse an **OS / Firmware version file** to upload and refresh for the device.
You can add a firmware to the Device Manager or delete a firmware from the list. The listed firmware files are uploaded into the system and are stored in the server's database.



You have to select a device – or device(s) – and select an uploaded firmware from the list and you can perform a *complete* firmware refresh – or *delta* firmware update.

You can do the following interactions for selected device(s):

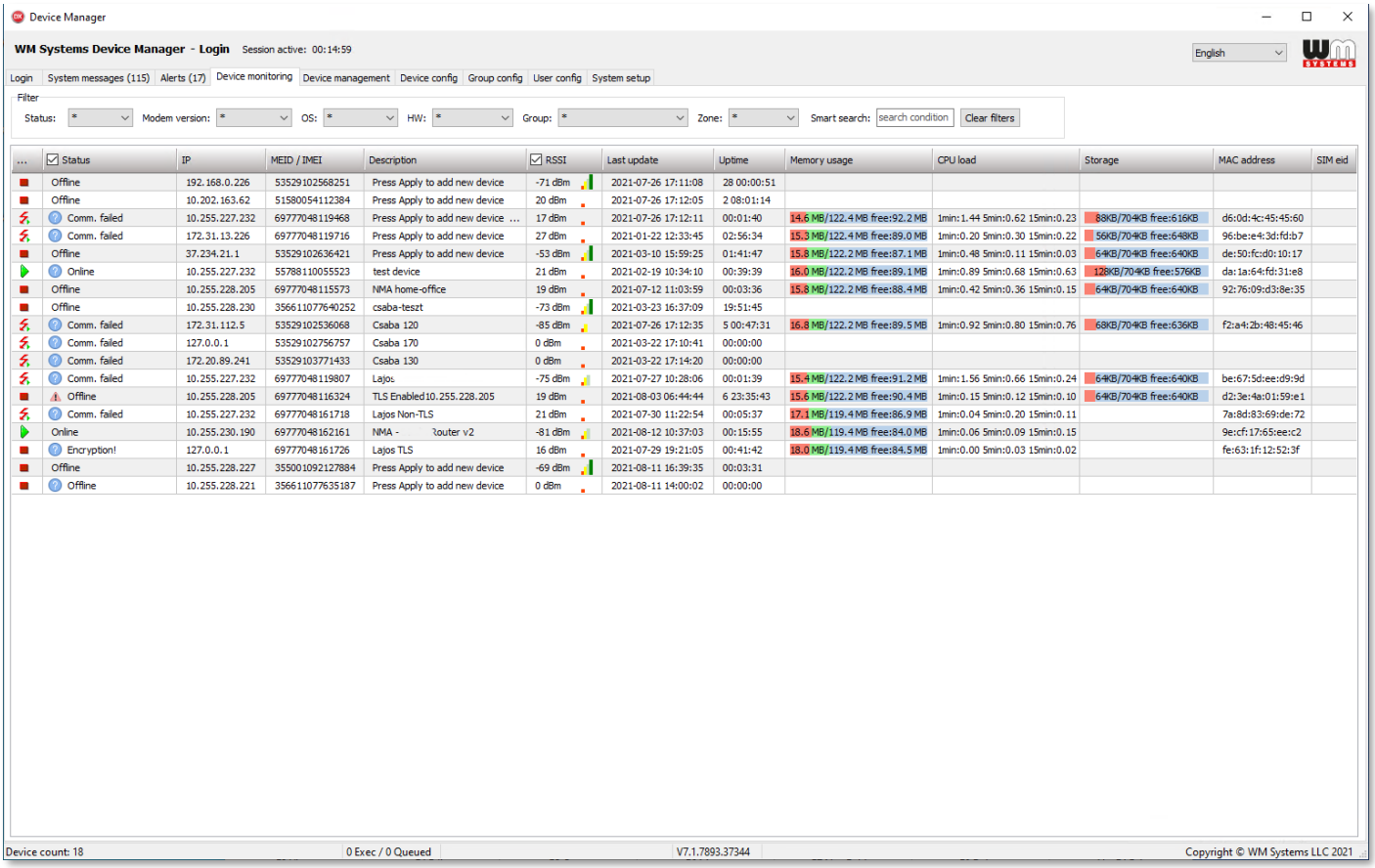
- **Upload config**: you can write the configuration to the device (settings will be overwritten on the device)
- **Download config**: you can read the configuration from the remote device into the DM's database
- **Upload server data**: Upload server data from the DM to the device. This data contains the server IP address, port, and name (for routers only)
- **Set real-time clock**: configure date/time of the device (for routers only)
- **Factory reset**: doing a confugration reset of the remote device to the factory default (for routers only)
- **Reboot device**: immediate restart of the remote device
- **Upgrade OS***: Device software / firmware upgrade or downgrade from the selected list to the remote device
- **Upgrade modem***: Refresh of the device's cellular module's refresh on remote device (for routers only)
- **Remote WIPE**: reset the settings of the device from the system and the remote device will be restarted

6. Device monitoring

On the **Device Monitoring** tab, you will find the current known status of your configured devices. Here you can also filter for some device properties. As you can see there are *offline*, *disabled* and *online* devices listed beside the pictograms by the first coloumns in the list. Some of them are listed with *Comm. failed* status.

Here you can check the **IP address**, **MEID/IMEI** info of the internet module and **Description** details of the device.

The last known and detected **Status** information about the devices are also listed, such as the signal strength of the cellular network (**RSSI**), the **Last update** date/time, **Uptime** (spent time since last reboot or device start), **Memory usage** and **CPU load** of the device**, Storage status** (free space), **MAC address**, **SIM eid**.
The QoS information will always help you to check and maintain your devices.



IMPORTANT!

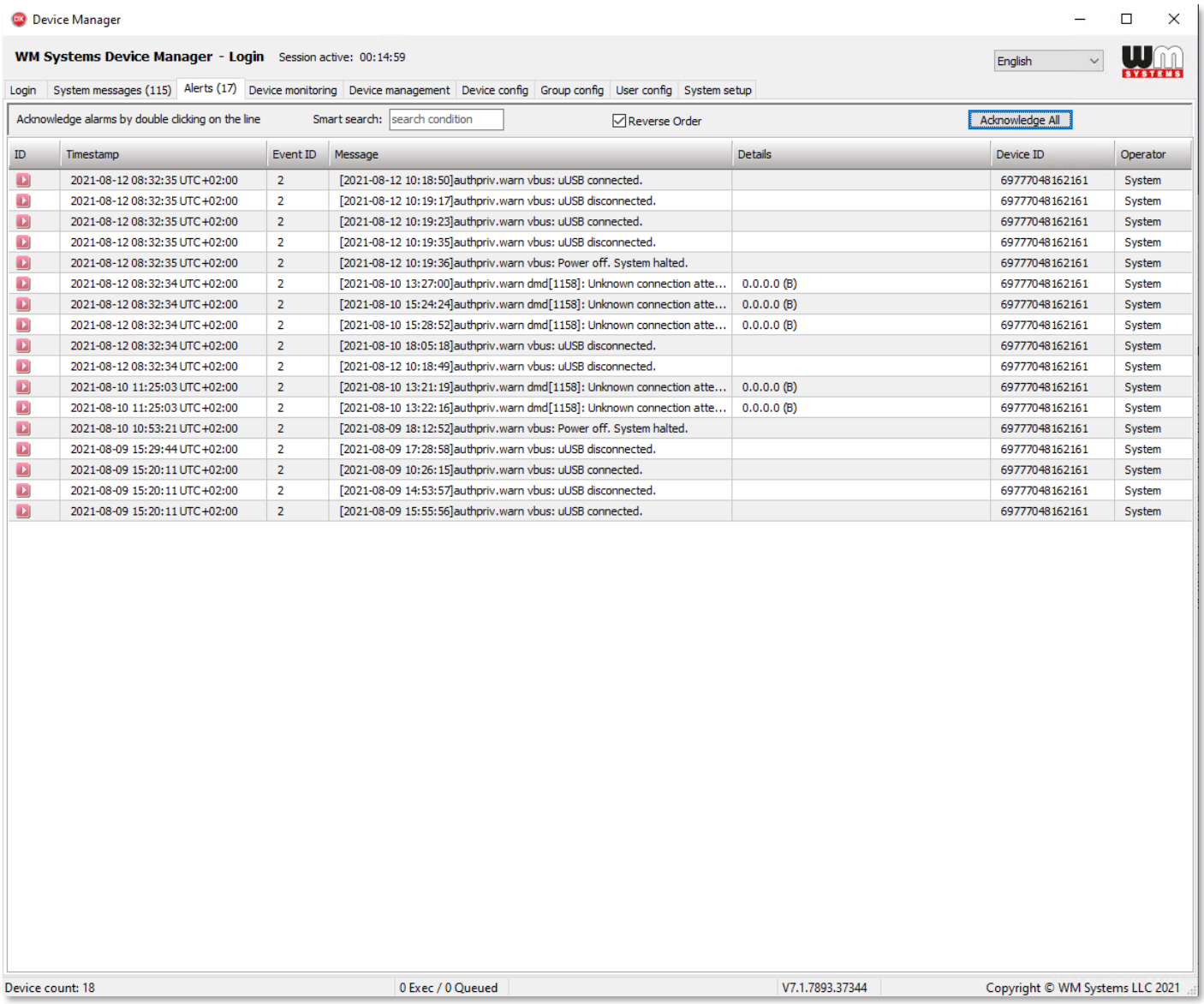
Note, that these data are not realtime, the status values showing the last known operation behaviour and life signals of the devices.

7. Alerts

On the **Alerts** tab you can check the incoming alert notifications of the remote devices.

The events are listed by date and time, but you can change it by the **Reverse Order** option. You can also filter the messages by searching a message string (word).

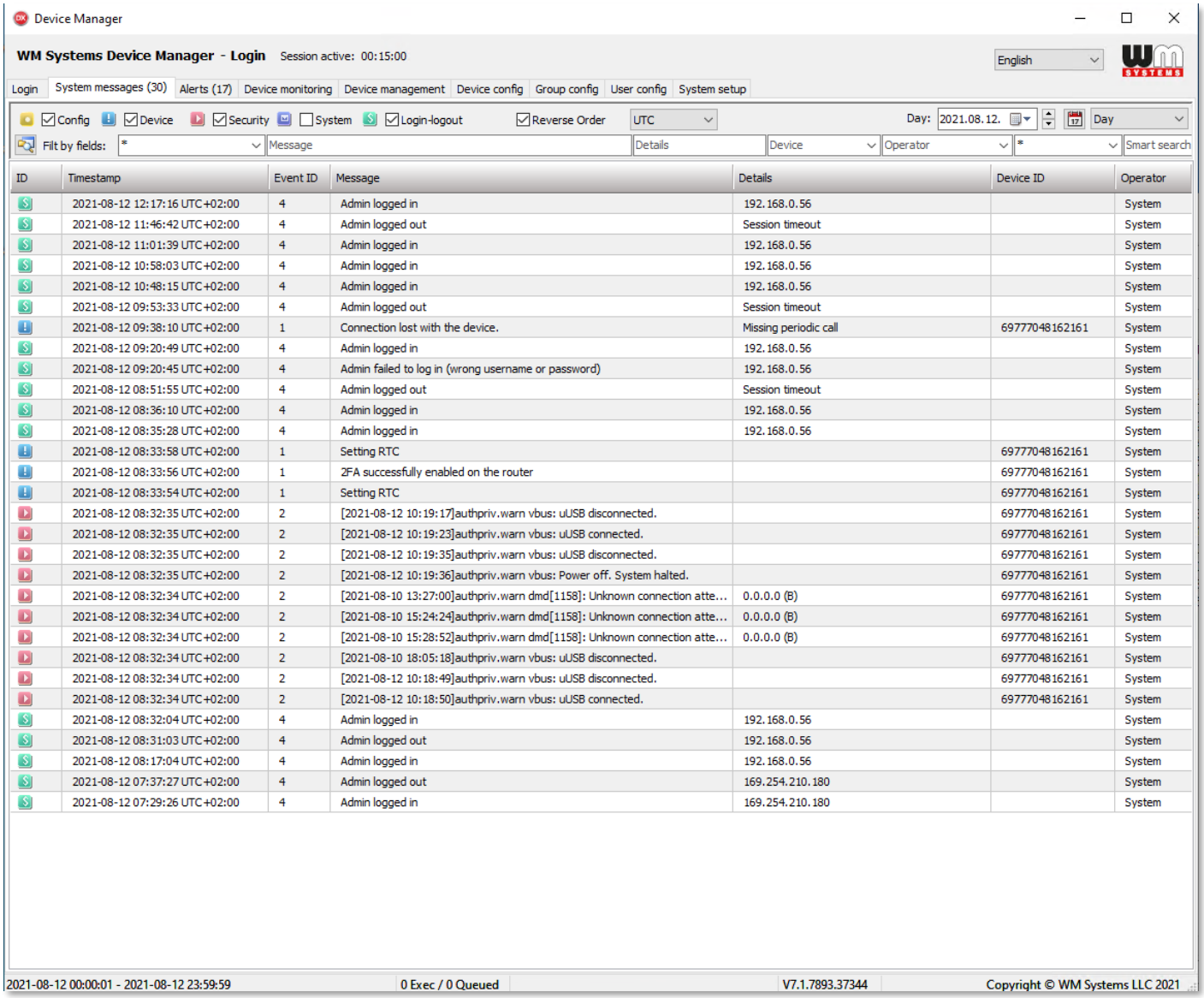
After you have read the messages by using the **Acknowledge All** button, the messages will be removed from the list.



8. System messages

On the **System messages** tab, you can check the incoming system messages and notifications. By default, all event types are listed here. You can also modify the list content by enabling some checkbars on the coloured message type icons – to filter the messages by event type(s).

You can also search / filter the events further for time interval - by a day, a week or an exact time or a time range.



9. Support

9.1 Technical Support

If you have any questions concerning the usage of the device, contact us through your personal and dedicated salesman.

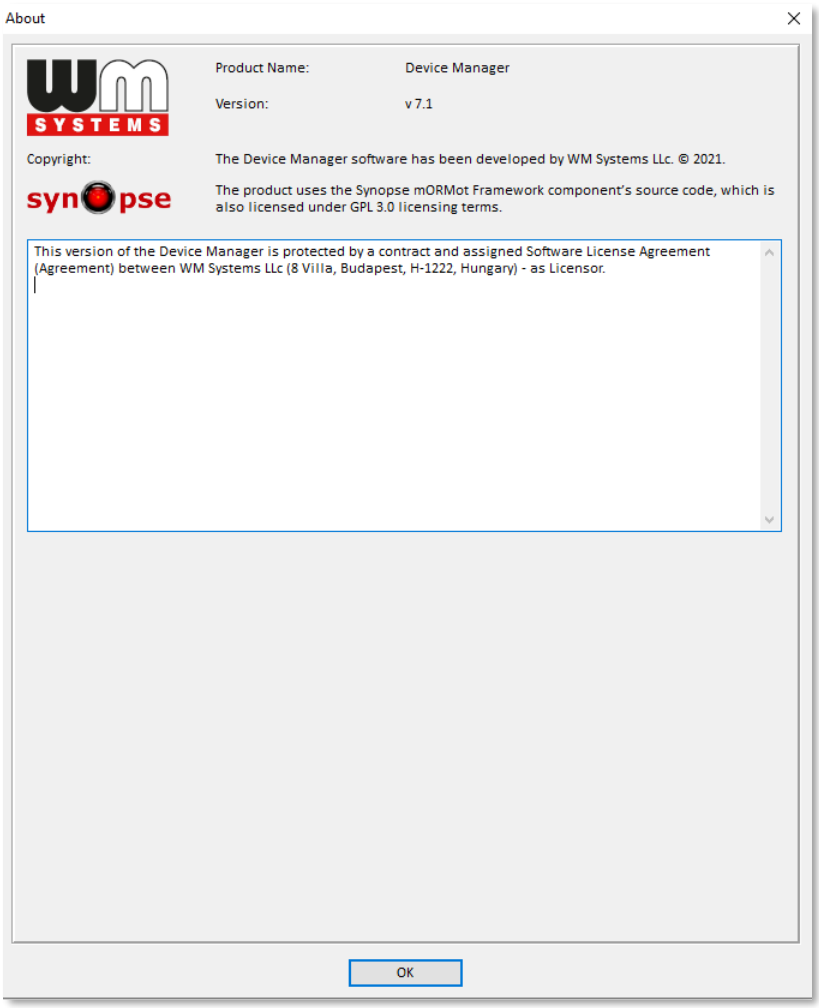
Online product support can be required here at our website:
https://www.m2mserver.com/en/support/

The documentation and software release for this product can be accessed via the following link:
https://www.m2mserver.com/en/product/device-manager/

9.2 GPL license

The Device Manager software is not a free product. WM has the application's copyrights. The software is ruled by the GPL licensing terms.

The product uses the Synopse mORMot Framework component's source code, which is also licensed under GPL 3.0 licensing terms.



10. Legal notice

The pictures in the user guide are only for illustration purposes.
WM Systems LLC. does not acknowledge or accept responsibility for any mistakes in the information contained in the user guide.
The published information in this document is subject to *change without notice*.
All data contained in the user guide is for information purposes only. For further information, please, contact our colleagues.

Warning

Any errors occurring during the firmware upgrade process may result in failure of the device.