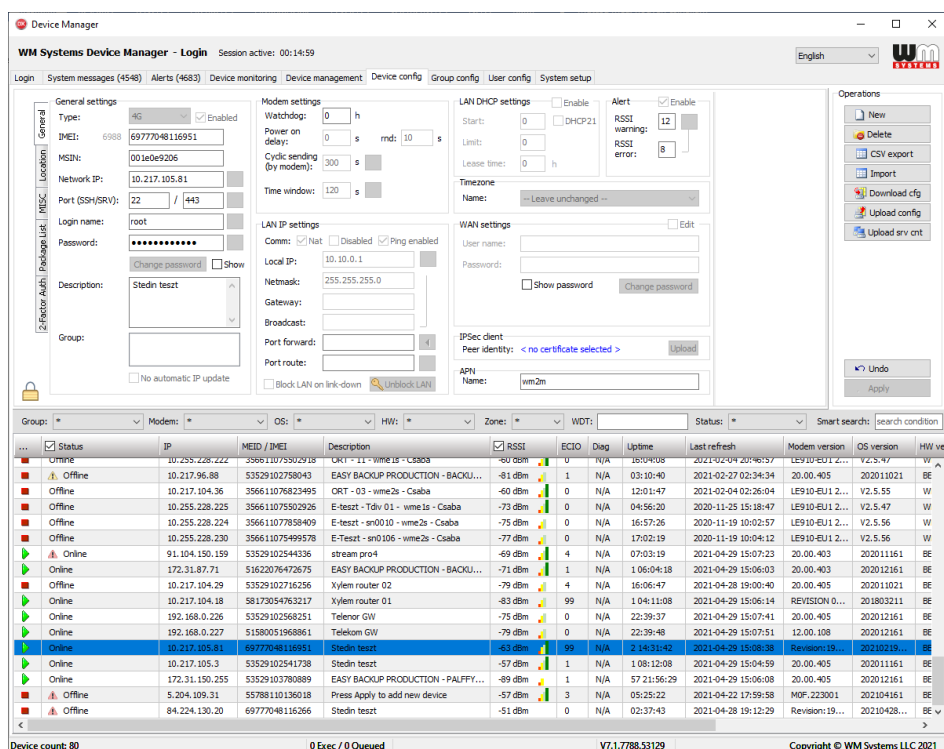


# Device Manager®

## for metering modem devices

# User Manual

## v2.20



2021-08-13

# 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.

<b>Document category:</b>	User Manual
<b>Document subject:</b>	Device Manager®
<b>Author:</b>	WM Systems LLC
<b>Document version No.:</b>	REV 2.20
<b>Number of pages:</b>	37
<b>Device manager version:</b>	v7.1
<b>Software version:</b>	DM_Pack_20210804_2
<b>Document status:</b>	FINAL
<b>Last modified:</b>	13 August, 2021
<b>Approval date:</b>	13 August, 2021

# Table of contents

<b>1. Introduction .....</b>	<b>4</b>
<b>2. Setup and Configuration.....</b>	<b>5</b>
2.1 Prerequisites .....	5
2.2 System elements.....	5
2.3 Installation.....	5
2.4 TLS protocol communication .....	7
<b>3. System configuration.....</b>	<b>9</b>
3.1 System setup .....	9
3.2 User settings.....	13
<b>4. Device settings .....</b>	<b>17</b>
4.1 Device group configuration .....	17
4.2 Device configuration for modems .....	18
4.3 Device status .....	21
4.4 GSM Settings .....	23
4.5 Management settings .....	24
4.6 TLS .....	25
4.7 Certificates & PKI information .....	26
4.8 SMI (Standard Meter Interface) settings .....	26
4.9 AMM settings .....	27
4.10 Watchdog settings.....	29
<b>5. Device monitoring.....</b>	<b>31</b>
<b>6. Device management .....</b>	<b>32</b>
<b>7. Alerts.....</b>	<b>33</b>
<b>8. System messages.....</b>	<b>355</b>
<b>9. Support .....</b>	<b>36</b>
9.1 Technical Support .....	36
9.2 GPL license .....	36
<b>10. Legal notice .....</b>	<b>37</b>

# 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 (modems) can be managed by a Device Manager.

Here we describe the software usage with our electricity metering modems (WM-Ex family) and WM-I3 device.

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

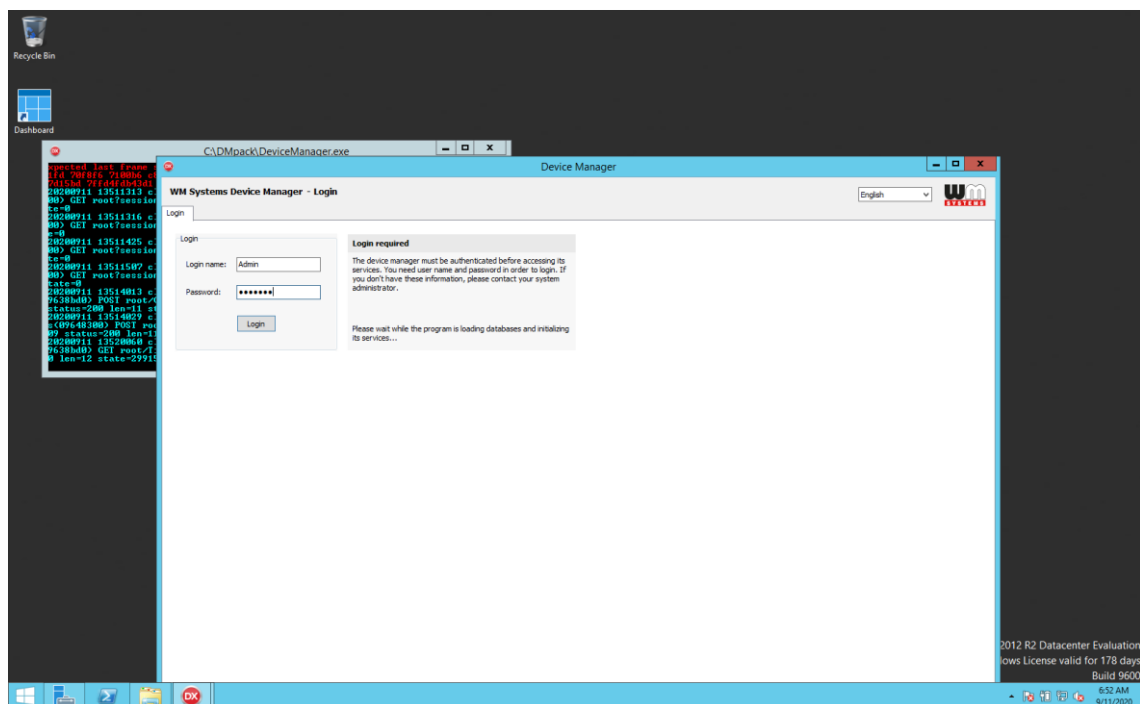
1. Create the root folder on the destination system. eg. C:\DMv7.1
2. Unzip the Device Manager compressed software package into the folder.
3. Modify the configuration file: *DeviceManager.config*

(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 modem communication
- *ServerPort* → external port for the modem 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<sup>®</sup> software will then be started soon.

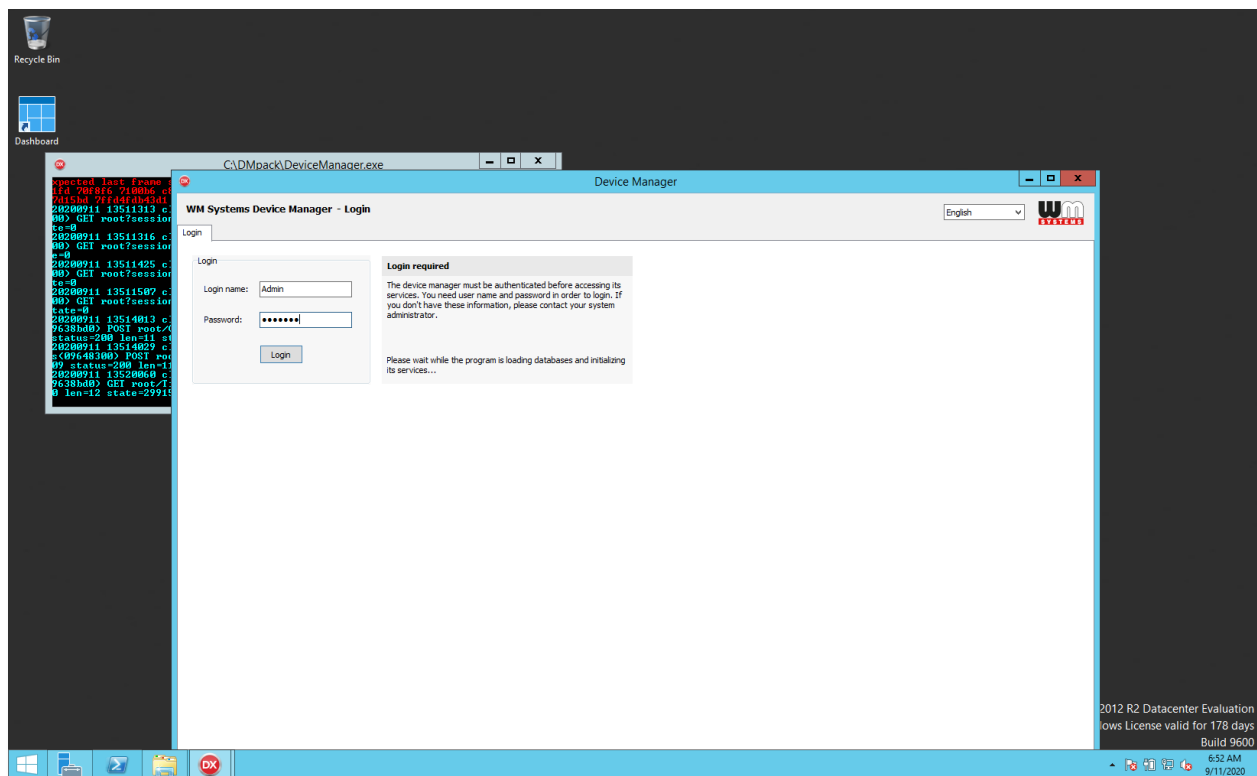


5. You have to **Login** by the following credentials:

- **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 modem and the Device Manager from the DM software side (by choosing TLS mode or legacy communication).

It used mbedTLS library on the modem 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 modem), and the public key travels in the form of a certificate.

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

Only factory default is implemented on the modem, so the modem does not check whether the certificate presented by the connected party is signed by a trusted party, so any TLS connection to the modem 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. modems). 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

Remote SNMP (manager)

SNMP level: ☒ v1 ☐ v2c ☐ v3

Host:

User name:

Password:

Privacy pass:

Trap mode: ☒ Generic ☐ Granular ☐ Variable bindings

☒ Enable trap sending

Device Manager

WM Systems Device Manager - Login Session active: 00:14:59 English

Login System messages (23) Alerts (17) Device monitoring Device management Device config Group config User config System setup

Remote SNMP (manager)

SNMP level: ☒ v1 ☐ v2c ☐ v3

Host:

User name:

Password:

Privacy pass:

Trap mode: ☒ Generic ☐ Granular ☐ Variable bindings

☒ Enable trap sending

Server settings

Server name:

Server IP address:

Listening port to modems:  listening...

Listening port of Web Service:  listening...

Proxy Settings

Cyclic reading:  sec 0 = no cyclic reading

☐ force polling all (unowned) devices

Read timeout:  sec

Connect timeout:  sec

☐ TLS Verify Peer Certificate Verify depth:

Security (AES 256)

☒ Encrypted ☒ Random IV

☒ Authenticated

☒ Default security key

☐ Specific security key (32 char):

Quick Login

☒ Remember login name and password

Automatic data maintenance

Keep data of the last:  months

Common store of packages

Timezone data

Data Broker

Address:

Port:

Supervisor Port:

Miscellaneous

Zone limit:  Update:

Comm:  Limit the number of devices per zone processing upgrade

Modem upgrade path: /var/fw

Chunk:  Block:

☒ Enable Active Directory

Time format:

Max. parallel threads:

External alarm server

☒ Not used ☐ OS Event Viewer

☐ SysLog Server:

Server:

Port:

Remote LogView Server

☐ Enable remote logging

Server:

Port:

Manage

Alarm aggregation options:

☐ Enable aggregation

DM Service Management:

2021-08-12 00:00:01 - 2021-08-12 23:59:59 0 Exec / 0 Queued V7.1.7893.37344 Copyright © WM Systems LLC 2021

- 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

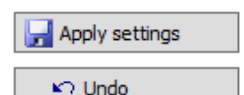
**Privacy pass:** Required when the v3 SNMP level is selected. The authentication is possible by any of the SNMP-enabled users plus the privacy pass specified here. Of course, this setting must be the same at that of the SNMP manager.

**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.

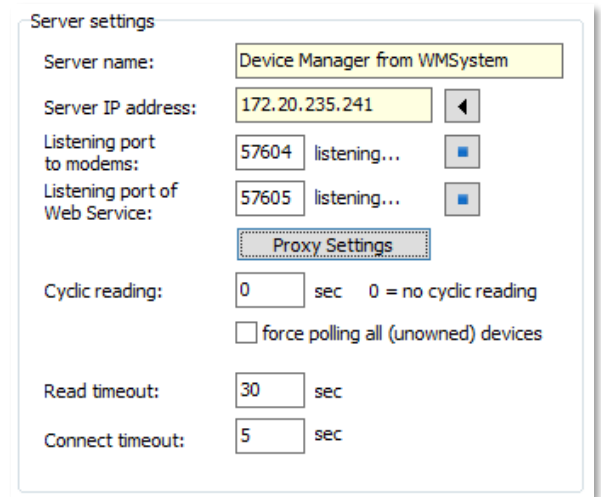


## **Server settings**

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 selecting 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.

Security (AES 256)

☒ Encrypted ☒ Random IV

☒ Authenticated **Save keys**

☒ Default security key

☐ Specific security key (32 char):

Quick Login

☒ Remember login name and password

Automatic data maintenance

Keep data of the last: 6 months

### Quick Login

**Remember login name and password:** to save your login credentials

### 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,

Data Broker

Address: 192.168.0.202

Port: 888

Supervisor Port: 0 **Check**

Miscellaneous

Zone limit:

Comm: 10 Update: 10

Limit the number of devices per zone processing upgrade

Modem upgrade path: /var/fw

/tmp/fw

Chunk: 32 Block: 128

☒ Enable Active Directory

Time format: Local time

Max. parallel threads: 32

without these settings, the CDMA network could be easily 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

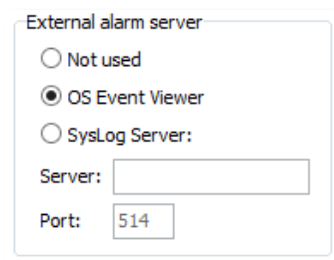
**Time format:** can be *Local time* or *UTC*

**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



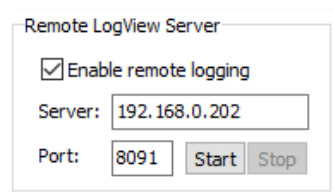
The screenshot shows a window titled "External alarm server". It contains three radio buttons: "Not used", "OS Event Viewer" (which is selected), and "SysLog Server:". Below the radio buttons, there are two input fields: "Server:" and "Port:". The "Port:" field has the value "514" entered.

### 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

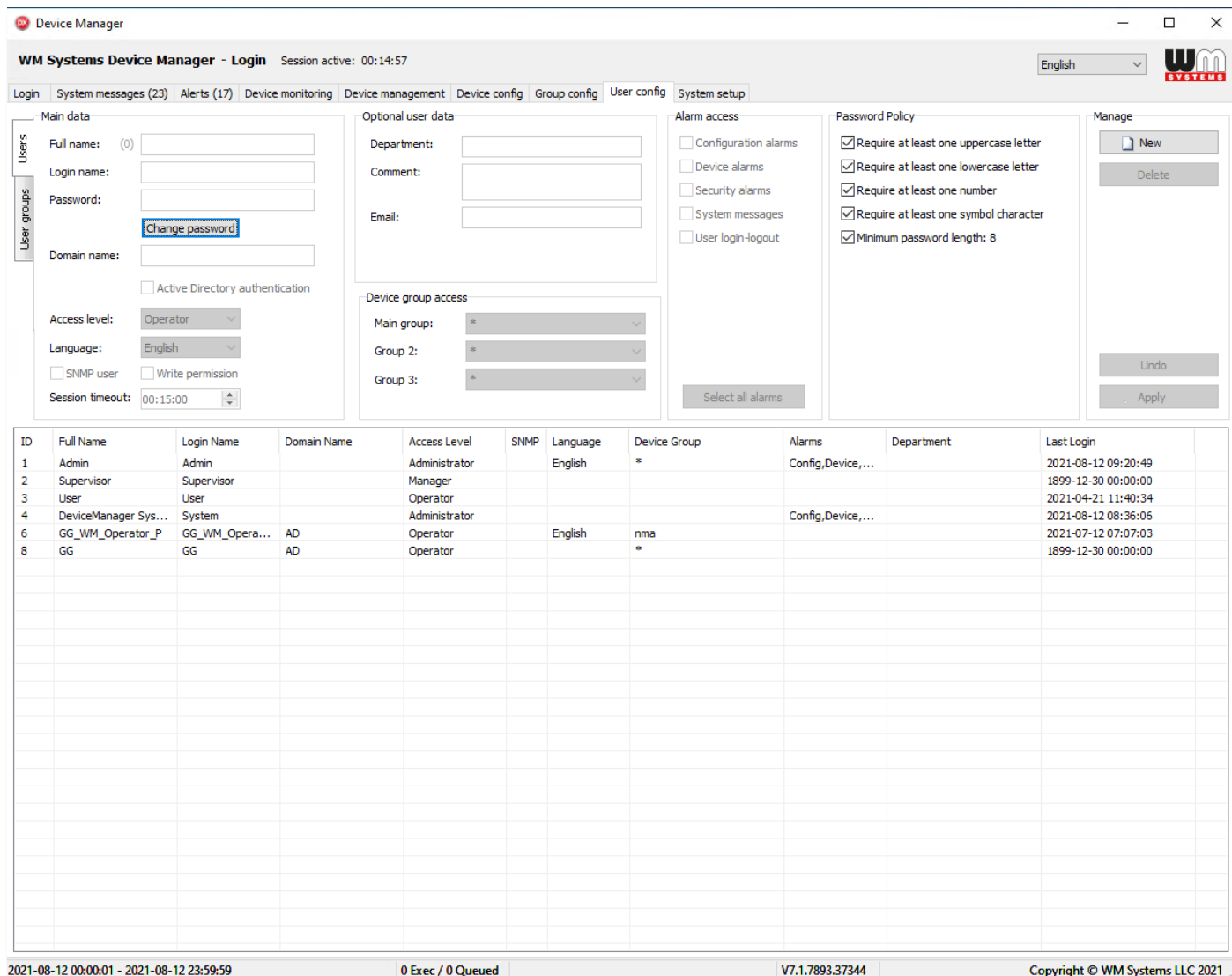


The screenshot shows a window titled "Remote LogView Server". It contains a checked checkbox labeled "Enable remote logging". Below the checkbox, there are two input fields: "Server:" and "Port:". The "Server:" field has the value "192.168.0.202" entered. The "Port:" field has the value "8091" entered. To the right of the "Port:" field are two buttons: "Start" and "Stop".

## 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.



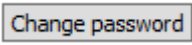
ID	Full Name	Login Name	Domain Name	Access Level	SNMP	Language	Device Group	Alarms	Department	Last Login
1	Admin	Admin		Administrator		English	*	Config,Device,...		2021-08-12 09:20:49
2	Supervisor	Supervisor		Manager						1899-12-30 00:00:00
3	User	User		Operator						2021-04-21 11:40:34
4	DeviceManager Sys...	System		Administrator				Config,Device,...		2021-08-12 08:36:06
6	GG_WM_Operator_P	GG_WM_Opera...	AD	Operator		English	nma			2021-07-12 07:07:03
8	GG	GG	AD	Operator			*			1899-12-30 00:00:00

## Main data

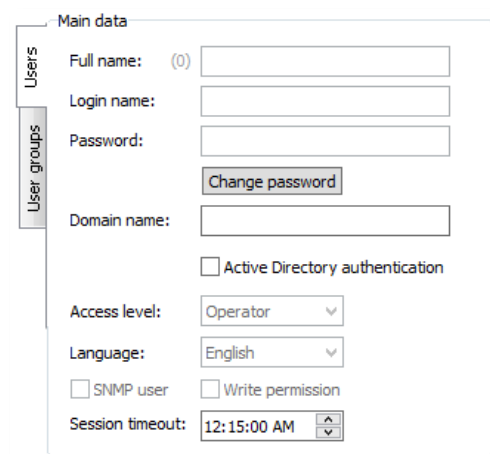
**Full name:** User real name

**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.

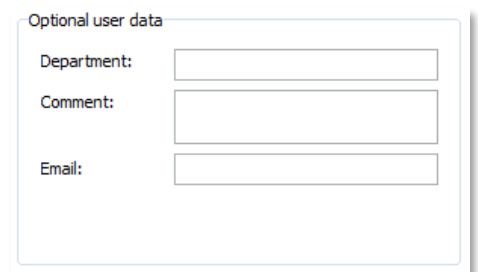
**Session timeout:** automatic logout can be also defined.

### 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!)

A screenshot of a web form titled "Optional user data". It contains three input fields: "Department:" with a text box, "Comment:" with a larger text box, and "Email:" with a text box.

### 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)

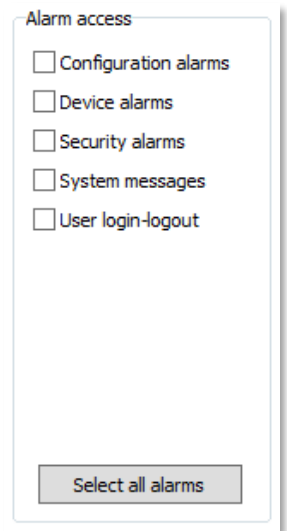
**Group 3:** you can choose further and additional device group for the user account (not obligatory to use)

A screenshot of a web form titled "Device group access". It contains three dropdown menus: "Main group:", "Group 2:", and "Group 3:". Each dropdown menu has a small asterisk icon and a downward arrow.

## **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.

A dialog box titled "Alarm access" with a list of five alarm categories, each with an unchecked checkbox: "Configuration alarms", "Device alarms", "Security alarms", "System messages", and "User login-logout". At the bottom right is a button labeled "Select all alarms".

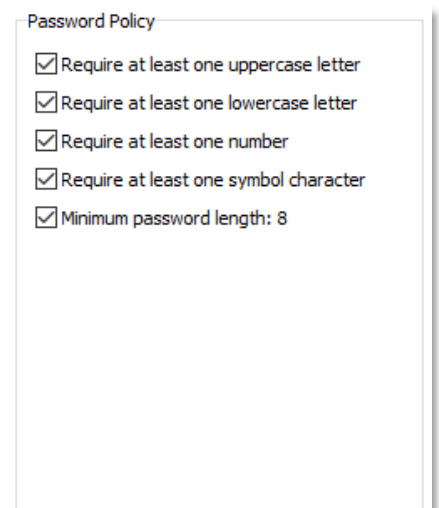
Alarm access

- ☐ Configuration alarms
- ☐ Device alarms
- ☐ Security alarms
- ☐ System messages
- ☐ User login-logout

Select all alarms

## **Password Policy**

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

A dialog box titled "Password Policy" with a list of five password requirements, each with a checked checkbox: "Require at least one uppercase letter", "Require at least one lowercase letter", "Require at least one number", "Require at least one symbol character", and "Minimum password length: 8".

Password Policy

- ☒ Require at least one uppercase letter
- ☒ Require at least one lowercase letter
- ☒ Require at least one number
- ☒ Require at least one symbol character
- ☒ Minimum password length: 8



# 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  **New** 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.

Device Manager

WM Systems Device Manager - Login Session active: 00:14:59 English

Login System messages (23) Alerts (17) Device monitoring Device management Device config Group config User config System setup

Group

Name: TEST Description: demonstration group

ID	Group Name	Description
1	Group 1	This is a group
2	TEST	demonstration group
3	csaba	csaba
4	nma	nma
5	aaaa	
6	Lajos	

Filter

IMEI: IP: Description:

IMEI	IP	Description
<input checked="" type="checkbox"/> 53529102568251	192.168.0.226	Press Apply to add new device
<input checked="" type="checkbox"/> 51580054112384	10.202.163.62	Press Apply to add new device
<input checked="" type="checkbox"/> 69777048119468	10.255.227.232	Press Apply to add new device 172.31.13.226 869777048119716
<input checked="" type="checkbox"/> 69777048119716	172.31.13.226	Press Apply to add new device
<input checked="" type="checkbox"/> 53529102636421	37.234.21.1	Press Apply to add new device
<input checked="" type="checkbox"/> 55788110055523	10.255.227.232	test device
<input type="checkbox"/> 69777048115573	10.255.228.205	NMA home-office
<input type="checkbox"/> 356611077640252	10.255.228.230	csaba-teszt
<input type="checkbox"/> 53529102536068	172.31.112.5	Csaba 120
<input type="checkbox"/> 53529102756757	127.0.0.1	Csaba 170
<input type="checkbox"/> 53529103771433	172.20.89.241	Csaba 130
<input type="checkbox"/> 69777048119807	10.255.227.232	Lajos teszt eszköze.
<input type="checkbox"/> 69777048116324	10.255.228.205	TLS Enabled 10.255.228.205
<input type="checkbox"/> 69777048161718	10.255.227.232	Lajos Non-TLS
<input type="checkbox"/> 69777048162161	10.255.230.190	NMA Router v2
<input type="checkbox"/> 69777048161726	127.0.0.1	Lajos TLS
<input type="checkbox"/> 355001092127884	10.255.228.227	Press Apply to add new device
<input type="checkbox"/> 356611077635187	10.255.228.221	Press Apply to add new device

Manage

New

Delete

Assign selectd

☒ Assign all

Unassign selectd

Undo

Apply

2021-08-12 00:00:01 - 2021-08-12 23:59:59 0 Exec / 0 Queued V7.1.7893.37344 Copyright © WM Systems LLC 2021

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 modems

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 hardware 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).

The screenshot displays the WM Systems Device Manager interface. The top navigation bar includes tabs for Login, System messages (115), Alerts (17), Device monitoring, Device management, Device config (selected), Group config, User config, and System setup. The left sidebar shows a tree view with categories like General, Location, MISC, TLS, 2-Factor Auth, and Package List. The main area is divided into several configuration panels: General settings (Type: 4G, Enabled), Modem settings (Watchdog: 0h, Power on delay: 0s, mtd: 10s, Cyclic sending: 3600s, Time window: 60s), LAN DHCP settings (Enabled, Start: 100, Limit: 150, Lease time: 12h), Alert settings (RSSI warnings: 0, RSSI error: 0), LAN IP settings (Comm: Nat, Disabled, Ping enabled, Local IP: 192.168.127.1, Netmask: 255.255.255.0), WAN settings (User name, Password, Enable), and APN settings (Name: wmm2m). The bottom section features a table of managed devices with columns for Status, IP, MEID / IMEI, Description, RSSI / CSQ, ECTO, Diag, Uptime, Last refresh, Modem version, OS version, HW version, Zone, FWSTK32, and wdt-ctrl. The table lists various devices with their current status (Online, Offline, Comm. failed) and associated details. The bottom status bar shows 'Device count: 18', '0 Exec / 0 Queued', 'V7.1.7893.3744', and 'Copyright © WM Systems LLC 2021'.

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**.

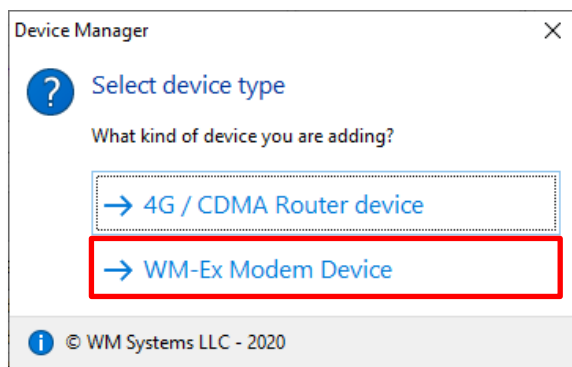
The **Modem version**, **OS version** (date of the build), **HW version** (PCB identifier), **FWSTM32** (Microcontroller firmware version) are also available here.

	Ping...	Alt+P
	Add to Polling Queue	Alt+Q
	Read Device Status	Alt+S
	Read Device Configuration	Alt+R
	Write Device Configuration	Alt+W
	Reboot	Shift+Alt+R
	Device Related Log	Alt+L
	Device Related Alerts	Alt+A
	Web Administration Interface	Alt+I
	SSH Connection	Alt+C
	One Time Password	Alt+T
	Block LAN port	Alt+B
	Un-Block LAN port	Alt+U
	Edit Configuration	Alt+E
	CCS Security On	Alt+O
	CCS Security Off	Alt+F

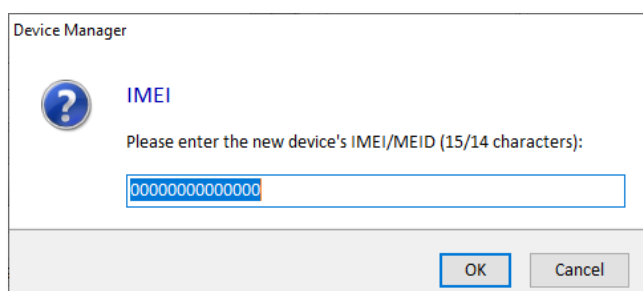
When you've selected a device from the list, you can click with right mouse button to the element, and the following right submenu appears, where you can choose from the available features to perform an interaction on the device.

You can also add further new devices by the  button.

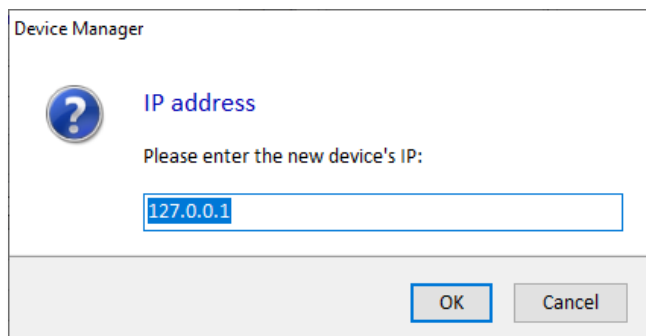
For modems you have to first select the device type: **WM-Ex Modem device**.



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

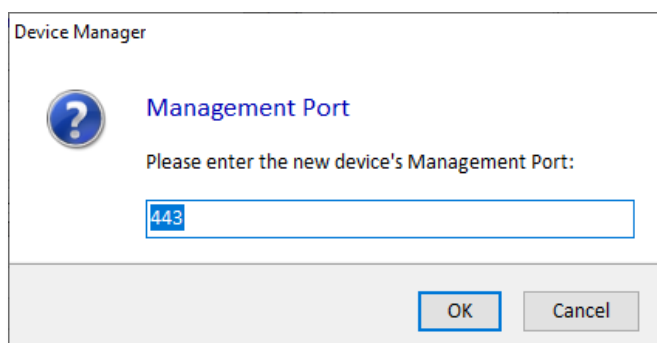


Add the **IP address** of the device.



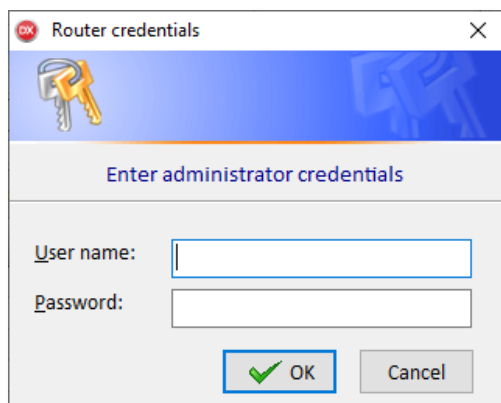
The 'Device Manager' dialog box has a title bar with 'Device Manager' and a close button. It features a blue question mark icon on the left. The text 'IP address' is displayed in blue. Below it, the instruction 'Please enter the new device's IP:' is shown. A text input field contains '127.0.0.1'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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



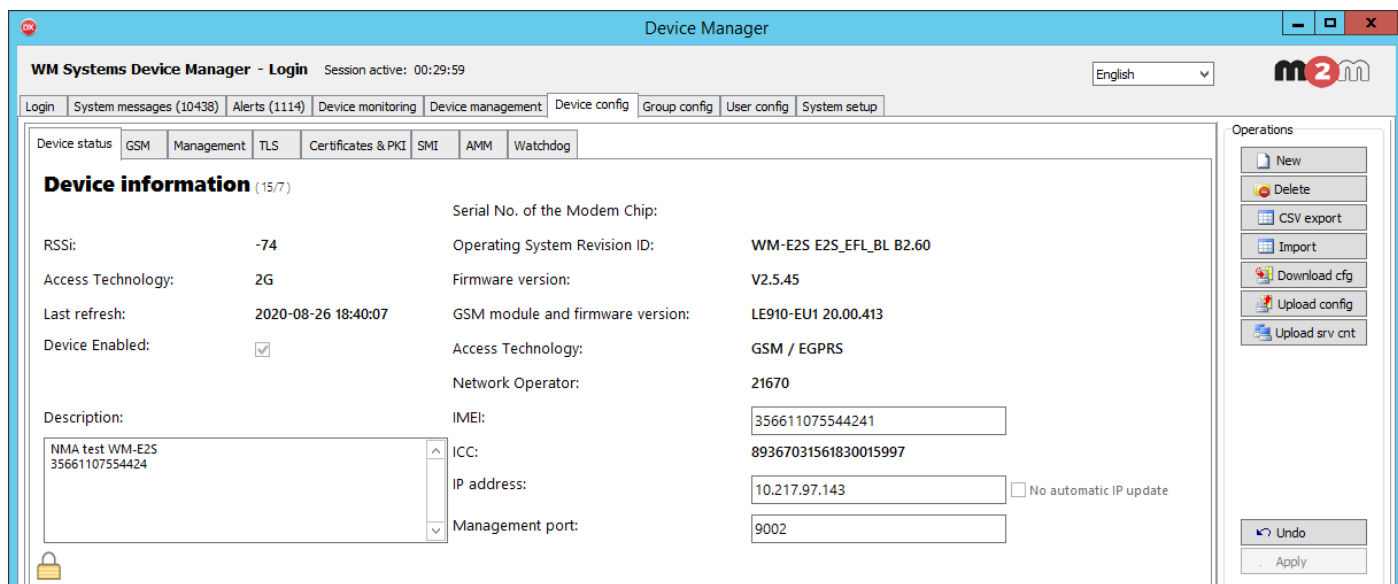
The 'Device Manager' dialog box has a title bar with 'Device Manager' and a close button. It features a blue question mark icon on the left. The text 'Management Port' is displayed in blue. Below it, the instruction 'Please enter the new device's Management Port:' is shown. A text input field contains '443'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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

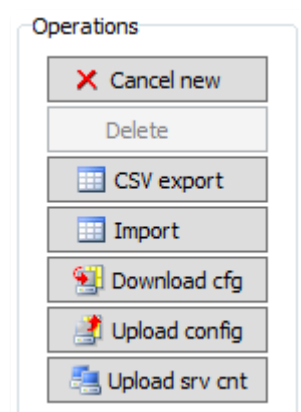


The 'Router credentials' dialog box has a title bar with 'Router credentials' and a close button. It features a blue header with a key icon and the text 'Enter administrator credentials'. Below this, there are two text input fields: 'User name:' and 'Password:'. At the bottom right, there are 'OK' and 'Cancel' buttons, with a green checkmark icon next to the 'OK' button.

Then the following screen will appear to provide more information about the device settings. There are available tabs on the screen to categorize the settings.



- You can use the configuration command buttons during the settings anytime at 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 Device status

If there are available info already about the device and its operation, then it will be listed here.

**RSSI** – cellular network signal strength

**Access Technology** – currently used cellular network

Device Manager

WM Systems Device Manager - Login Session active: 00:29:59 (changes!)

English

Login | System messages (6331) | Alerts (137) | Device monitoring | Device management | Device config | Group config | User config | System setup

Device status | GSM | Management | TLS | Certificates & PKI | SMI | AMM | Watchdog

### Device information (5202/11)

RSSI: -59  
Access Technology: LTE  
Last refresh: 2020-06-16 11:55:12  
Device Enabled: ☒

Serial No. of the Modem Chip: 012302000520000010  
Operating System Revision ID: WM-E2S E2S\_EFL\_B1 B2.60  
Firmware version: V2.5.37  
GSM module and firmware version: LE910-EU1 20.00.416  
Access Technology: LTE - E-UTRAN  
Network Operator: 21670

Description: wme2s új 2020.06.11  
IMEI: 356611077858409  
ICC: 89367031561930046637  
IP address: 10.217.102.187 ☐ No automatic IP update  
Management port: 9001

Operations: New, Delete, CSV export, Import, Download cfg, Upload config, Upload srv cnt, Undo, Apply

Group: \* Modem: \* OS: \* HW: \* Zone: \* WDT: Status: \* Smart search: search condition

...	✓ Status	IP	MEID / IMEI	Description	✓ RSSI	ECIO	Diag	Uptime	Last refresh	Modem version	C
	Online	10.202.171.42	51580051894620	EASY BACKUP PRODUCTION	-91 dBm	0	N/A	5 19:35:58	2020-09-11 07:16:35	12.00.108	
	Online	10.217.99.39	59852054119517	EASY BACKUP PRODUCTION	-89 dBm	2	N/A	00:07:12	2020-09-11 07:15:31	17.01.522	
	Online	10.255.226.214	59852054111100	EASY BACKUP PRODUCTION	-75 dBm	4	N/A	8 01:26:15	2020-09-11 07:18:58	17.01.522	
	Online	172.31.153.92	59852054108155	EASY BACKUP PRODUCTION	-99 dBm	2	N/A	00:07:07	2020-09-11 07:18:16	17.01.522	
	Online	10.202.163.62	51580050503529	EASY BACKUP PRODUCTION	-73 dBm	0	N/A	35 15:23:54	2020-09-11 07:15:04	12.00.106	
	Online	10.217.100.151	53529102526846	EASY BACKUP PRODUCTION	-89 dBm	1	N/A	34 08:33:38	2020-09-11 07:16:21	20.00.403	
	Online	10.217.96.98	59852054108007	EASY BACKUP PRODUCTION	-63 dBm	5	N/A	6 16:04:33	2020-09-11 07:18:44	17.01.522	
	Offline	10.217.102.187	356611077858409	wme2s új 2020.06.11	-59 dBm	0	N/A	00:00:00	2020-06-16 04:55:12	LE910-EU1 2...	
	Disabled	192.168.0.233	A100005F850076	;,\$%*"@&#><_	-369 dBm	-31	N/A	00:11:24	2020-06-29 07:17:35	22.00.001	
	Online	192.168.0.228	53529102558625	VO	-71 dBm	0	N/A	15 11:45:56	2020-09-11 07:18:00	20.00.405	
	Online	10.217.102.245	53529102743482	TEST DEVICE 01	-61 dBm	3	N/A	03:58:39	2020-09-11 07:16:41	20.00.405	
	Online	10.217.102.224	53529102728020	TEST DEVICE 02	-59 dBm	2	N/A	03:58:46	2020-09-11 07:16:39	20.00.405	
	Online	10.217.102.246	53529102738904	TEST DEVICE 03	-59 dBm	1	N/A	03:58:50	2020-09-11 07:16:56	20.00.405	
	Online	10.217.102.244	53529102748788	TEST DEVICE 04	-57 dBm	1	N/A	04:49:39	2020-09-11 07:18:48	20.00.405	
	Online	10.217.102.200	53529102753531	TEST DEVICE 05	-57 dBm	2	N/A	03:58:41	2020-09-11 07:16:21	20.00.405	
	Online	10.217.102.242	53529102744415	TEST DEVICE 06	-61 dBm	2	N/A	03:58:44	2020-09-11 07:17:05	20.00.405	
	Online	10.217.102.225	53529102738953	TEST DEVICE 07	-61 dBm	2	N/A	03:53:37	2020-09-11 07:16:33	20.00.405	

Device count: 69 0 Exec / 0 Queued V7.1.7559.56113 Copyright © WM Systems LLC 2020

**Last refresh** – Datetime of the last QoS information

**Device enabled** – You can disable or enable the device monitoring here.

**Description** – You can add further information about the device

**Serial No. of the Modem Chip** – unique module identifier

**Operating System Revision ID** – Device firmware (RToS) version

**Firmware version** – Module fw version

**GSM module and firmware version** – Cellular module information

**Network Operator** – Current cellular network provider

**IMEI** – Cellular module unique identifier

**ICC** – SIM card unique identifier

**IP address** – device IP

**Management port** – device DM management port number

## 4.4 GSM Settings

You can configure the cellular module settings here.

The screenshot shows the 'Device Manager' application window. The title bar reads 'Device Manager'. Below the title bar, there's a navigation bar with tabs: 'Login', 'System messages (10438)', 'Alerts (1115)', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. The 'Device config' tab is active. Under this tab, there are sub-tabs: 'Device status', 'GSM', 'Management', 'TLS', 'Certificates & PKI', 'SMI', 'AMM', and 'Watchdog'. The 'GSM' sub-tab is selected. The main area displays 'Operator settings' and 'Mobile data' sections. The 'Operator settings' section includes fields for 'PIN number (SIM):', 'Frequency band:' (set to '2G only'), 'Password for CSD call:', and 'Number of rings before accepting call:' (set to '3'). The 'Mobile data' section includes fields for 'APN name:' (set to 'wm2m'), 'APN Username:', and 'APN Password:', each with a 'Generate automatically' checkbox. On the right side, there's an 'Operations' panel with buttons: 'New', 'Delete', 'CSV export', 'Import', 'Download cfg', 'Upload config', and 'Upload srv cnt'. At the bottom right, there are 'Undo' and 'Apply' buttons.

**PIN number (SIM):** SIM PIN code

**Frequency band:** Choose a dedicated cellular access technology from the dropdown list. Here you can limit which networks could be used – e.g. only LTE will be used or LTE with 2G fallback (when no LTE access, will be using the 2G) should be used, etc.

The screenshot shows a dropdown menu for selecting the frequency band. The options are: 'All available access technology (default)', 'LTE only (default on LTE Cat. 1 modem)', '3G with fallback to 2G', 'LTE with fallback to 2G', 'LTE with fallback to 3G', 'CAT-M1', 'NB-IoT', and 'CAT-M1 and NB-IoT'. The 'LTE only (default on LTE Cat. 1 modem)' option is currently selected and highlighted in blue.

**Password for CSD call:** you can define password for CSD (GPRS) call

**Number of rings before accepting call**

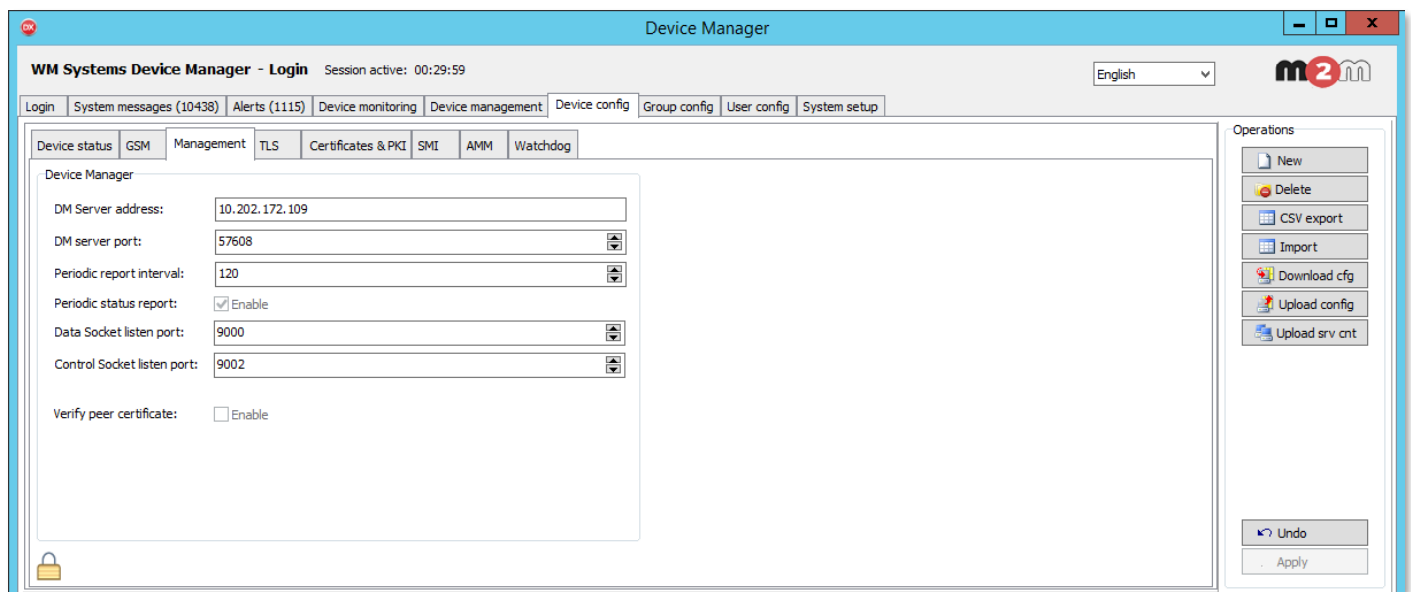
**APN name:** APN name (obligatory)

**APN Username:** if it exists for the APN

**APN Password:** if it exists for the APN

## 4.5 Management settings

Here you can configure the management settings for the remote device.



The screenshot shows the 'Device Manager' window of the 'WM Systems Device Manager - Login' application. The window has a blue title bar and a menu bar with options: Login, System messages (10438), Alerts (1115), Device monitoring, Device management, Device config, Group config, User config, and System setup. The 'Device config' tab is selected. Under this tab, there are sub-tabs: Device status, GSM, Management, TLS, Certificates & PKI, SMI, AMM, and Watchdog. The 'Management' sub-tab is active. The main area contains the following fields:

- DM Server address: 10.202.172.109
- DM server port: 57608
- Periodic report interval: 120
- Periodic status report: ☒ Enable
- Data Socket listen port: 9000
- Control Socket listen port: 9002
- Verify peer certificate: ☐ Enable

On the right side, there is an 'Operations' panel with buttons: New, Delete, CSV export, Import, Download cfg, Upload config, and Upload srv cnt. At the bottom right, there are 'Undo' and 'Apply' buttons.

**DM Server address:** add the monitoring DM server's IP address

**DM server port:** port name of the DM server

**Periodic report interval:** you can define the monitoring report cycle/interval here (in minutes)

**Periodic status report:** you can enable the cycles

**Data Socket listen port:** add port number for listener

**Control Socket listen port:** add port number for remote control of the device behaviour

**Verify peer certificate:** you can enable

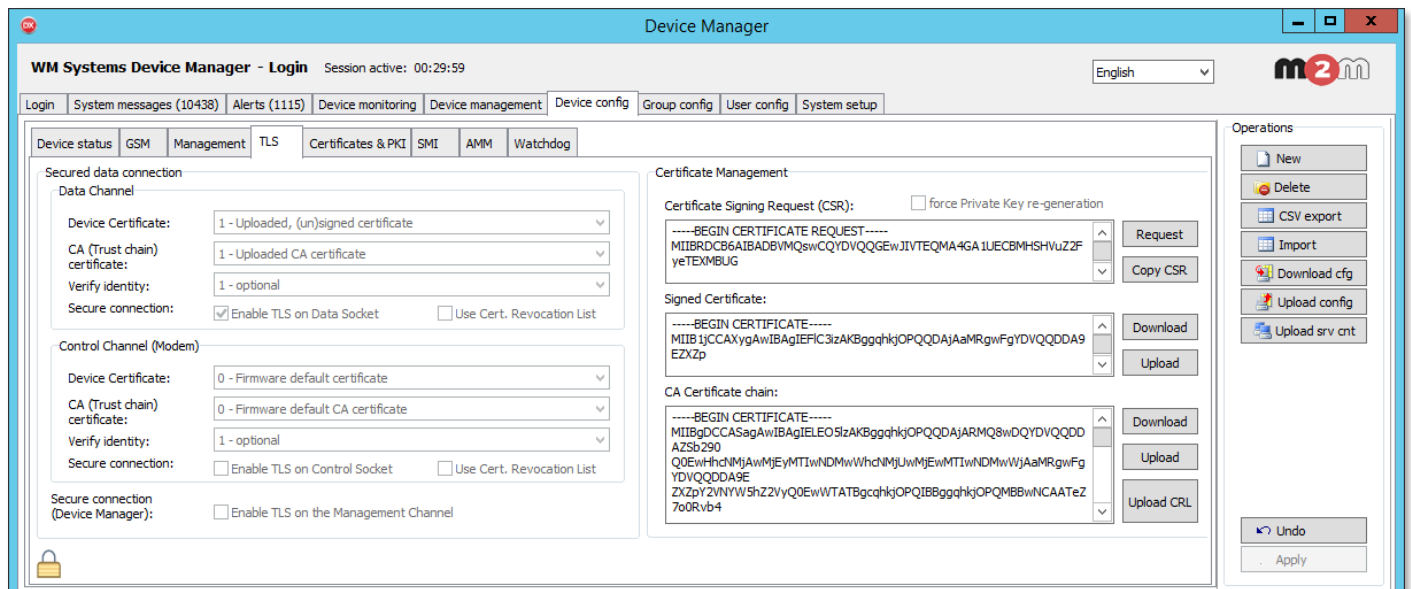


## 4.6 TLS

By using the TLS (Transport Layer Security) protocol, you can increase the communication security level of the device. Here you can define certifications for the modem ↔ Device Manager communication.

### Data channel settings

This part is about the security of the device data channel and communication.



**Device Certificate:** 0 - firmware default certificate or 1- uploaded unsigned certificate

**CA (Trust chain) certificate:** 0 - firmware default CA certificate or 1 - uploaded CA certificate

**Verify identity:** 0 – no verification or 1 – optional or 2 - required

**Secure connection:** you can enable/disable the following options here

- ***Enable TLS on Data Socket***
- ***User Cert. Revocation List***

### Control Channel (Modem):

This part is about the security of the device operation-

**Device Certificate:** 0 - firmware default certificate or 1- uploaded unsigned certificate

**CA (Trust chain) certificate:** 0 - firmware default CA certificate or 1 - uploaded CA certificate

**Verify identity:** 0 – no verification or 1 – optional or 2 - required

**Secure connection:** you can enable/disable the following options here

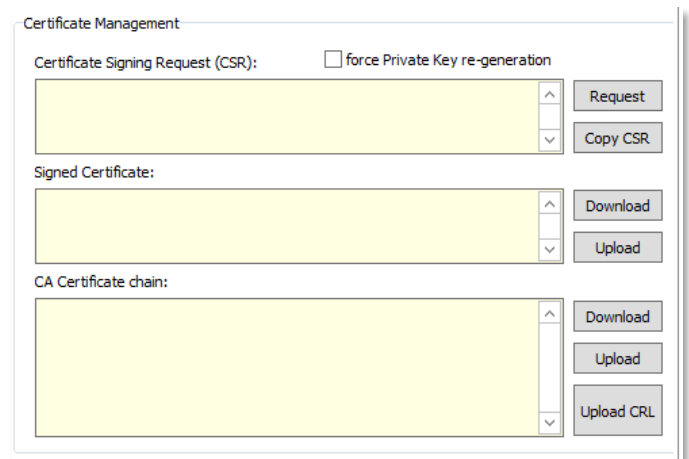
- ***Enable TLS on Control Socket***
- ***User Cert. Revocation List***

**Secure connection (Device Manager):** you can enable TLS on the Management Channel – this secures the DM management communication.

### **Certificate management:**

Here you can define the certificates by **request** or **copy**, or you can check it by **download** (from the device) and **upload** (to the device).

**Upload CRL** is the revocation list upload.

A screenshot of a 'Certificate Management' dialog box. It contains three main sections: 'Certificate Signing Request (CSR):' with a checkbox for 'force Private Key re-generation' and buttons for 'Request' and 'Copy CSR'; 'Signed Certificate:' with buttons for 'Download' and 'Upload'; and 'CA Certificate chain:' with buttons for 'Download', 'Upload', and 'Upload CRL'. Each section has a large yellow text area with scrollbars.

**4.7 Certificates & PKI information** Here you can check the certificate information of the device.

### **4.8 SMI settings (Standard Metering Information)**

**Data format for readout:** YYMMDD for example

**Version number of config file:** you can define a version number (not obligatory)

**Type key of AM100:** you define it for the Elster AM100 compatibility (not obligatory)

**Meter Interface init values:** initialization values of meter (not obligatory)

**Meaning of LED1..6:** you can reconfigure the device's LED settings

The screenshot shows the 'Standard Meter Interface' configuration page in the Device Manager. The page is divided into two main sections: 'Standard Meter Interface' and 'Operations'. The 'Standard Meter Interface' section contains the following fields:

- Date format for readout: YMMDD
- Version number of config file:
- Type key of AM100:
- Meter Interface init values:
- Meaning of LED1: GSM / GPRS status
- Meaning of LED2: SIM status ( wrong PIN flashing slow or withoi
- Meaning of LED3: E-meter status
- Meaning of LED4: Not used
- Meaning of LED5: Not used
- Meaning of LED6: Not used

The 'Operations' section on the right contains buttons for New, Delete, CSV export, Import, Download cfg, Upload config, Upload srv cnt, Undo, and Apply.

## 4.9 AMM settings

Here you can configure the AMM/IEC and DLMS settings of the modem.

The screenshot shows the 'IEC' and 'DLMS' configuration pages in the Device Manager. The 'IEC' section contains the following fields:

- Destination IP address or phone number:
- Ei client username: uiname11178
- Ei client password: uipass
- AMM (Ei Server) IP address:
- Ei client authentication mode:
- AMM (Ei Server) port number: 0
- Automatic registration: ☐ Enable
- Poll interval (not deployed): 30
- Poll interval (deployed): 30
- Ei client TCP keep-alive (minutes): 10
- FTP Server IP address:

The 'DLMS' section contains the following fields:

- DLMS host IP address:
- DLMS host port number: 1
- Communication timeout (sec.): 60
- DLMS password:
- List of DLMS authentication mechanisms: 1,5
- Disconnect relay (On/Off): 0
- Start DLMS session when booting: ☐ Enable
- The visibility of the registers 1-0:1.8.0\*255 and 1-0:2.8.0\*255 in the profiles "Daily E billing values" (1-0:99.2.0\*255) and "Monthly billing values" (0-0:98.1.0\*255) is controlled by this parameter: ☐ Visible

The 'Operations' section on the right contains buttons for New, Delete, CSV export, Import, Download cfg, Upload config, Upload srv cnt, Undo, and Apply.

### IEC settings:

**Destination IP address or phone number:** here you can define the remote server's IP address where the data will be transmitted through the wireless network

**EI client username:** for the connection IP address

**EI client password:** if password is also also required, fill in the field

**AMM (EI Server) IP address:** here you can define the remote server's IP address where the data will be transmitted through the wireless network

**EI Client authentication mode:** a remote device can be connected to the modem and readout the data - here you can select authentication mode. Select a value: N - no authentication, E - EI authentication: define the *username* and the *password*.

**AMM (EI Server) port number:** – AMM (EIServer) port (ftp client port), define the port number of the server IP.

**Automatic registration:** Automatic registration to the address - checkbox. In case of data push send automatically or not. You can enable it, if it is necessary to use.

**Poll interval (not deployed):** Value of Poll interval fast (not deployed) in seconds.

**Poll interval (deployed):** Value of Poll-interval slow (deployed) in seconds.

**EI client TCP keep-alive (minutes):** Keeps the EI client connection alive for the defined time range – value in minutes.

**FTP Server IP address:** for defining the Ftp server IP address.

### **DLMS settings:**

The AMM/DLMS parameter group is available here by compatibility reasons with the Elster® AM100 modems. The listed DLMS parameters can be used only with a DLMS / COSEM compatible firmware of the modem.

**DLMS host IP address:** You can define the DLMS AMM server's IP Address. This is mainly used for compatibility with the Elster AM100 modems.

**DLMS host port number:** You can define the port of DLMS AMM server. It is used for compatibility with the Elster AM100 modems.

**Communication timeout (sec):** You can define the max. time interval without DLMS communication (timeout) – value in seconds

**DLMS password:** define password for the DLMS connection

**List of DLMS authentication mechanisms:**

**Disconnect relay (On/Off):** not implemented yet for the modems

**Start DLMS session when booting:** you can enable

**The visibility of registers:** You can define the registers to be visible or not. You can set it to **Visible**

Meaning of groups:

- (1-0:1.8.0\*255 and 1-0:2.8.0\*255) in the profiles Daily E-billing values
- (1-0:99.2.0\*255) and Monthly billing values
- (0-0:98.1.0\*255) is controlled by this parameter

## 4.10 Watchdog settings

Here you can configure the watchdog behavior of the device.

The screenshot shows the 'Device Manager' application window. The title bar reads 'Device Manager'. Below the title bar, there is a navigation bar with tabs: 'Login', 'System messages (10438)', 'Alerts (1115)', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. The 'Device config' tab is selected. Within this tab, there are sub-tabs: 'Device status', 'GSM', 'Management', 'TLS', 'Certificates & PKI', 'SMI', 'AMM', and 'Watchdog'. The 'Watchdog' sub-tab is active. The main area displays 'Watchdog function parameters' with the following fields:

Ping IP address:	<input type="text"/>
Number of ping-retries:	<input type="text" value="3"/>
Ping timeout:	<input type="text" value="15000"/>
Ping interval:	<input type="text" value="65535"/>
GPRS login-fail timeout:	<input type="text" value="30"/>
Module-reset timeout:	<input type="text" value="24"/>
Daily restart at time (hh:mm):	<input type="text"/>
GPRS reconnect interval:	<input type="text" value="0"/>
Cellular network access technology:	<input type="text" value="All available access technology (default)"/>

On the right side of the window, there is an 'Operations' panel with buttons: 'New', 'Delete', 'CSV export', 'Import', 'Download cfg', 'Upload config', and 'Upload srv cnt'. At the bottom right, there are 'Undo' and 'Apply' buttons.

**Ping IP address:** add an IP address which can be accessed from the IP zone of the SIM card. This will be used for continuous checking of the network availability.

**Number of ping-retries:** how many times to try to ping the devices

**Ping timeout:** delay between ping cycles

**Ping interval:** length of a pinging cycle (in seconds)

**GPRS login-fail timeout:** you can set a timeout (tolerance) value (in second) in case of unnecessary login

**Module-reset timeout:** You can also configure length of GPRS connection trial in hours

**Daily restart at time (hh:mm):** you can define an exact daily time for restarting the remote device

**GPRS reconnect interval:** length of GPRS reconnection (in seconds)

**Cellular network access technology:** by dropdown selection. The device has the ability to manually force the refresh of the firmware remotely (FOTA) by selecting only the GPRS or only 3G or only the LTE 4G standard. Check the Cellular Network Access Technology selection (LTE, 3G, 2G mode) for FOTA field's value and choose the required option here.

## 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.

WM Systems Device Manager - Login

Session active: 00:14:59

English

WM SYSTEMS

Login

System messages (4403)

Alerts (6768)

Device monitoring

Device management

Device config

Group config

User config

System setup

Modem versions

File	Size	Hash
No available packages		

OS / Firmware versions

File	Size	Hash
<input type="checkbox"/> fwos-E2EFL_FW_2536.dwl	413952	F1829C08
<input type="checkbox"/> fwos-E2EFL_FW_2_5_351.dwl	131840	63D6B293
<input type="checkbox"/> fwos-BE0077B_CDMA450_Router-Standard....	7640376	019EE57
<input type="checkbox"/> yfwos-E1EFL_FW_2530-old-bl.dwl	264960	059107EE
<input type="checkbox"/> fwos-BE0077B_CDMA450_Router-DCU-1s.2...	5608685	2ACB6277
<input type="checkbox"/> fwos-E2EFL_FW_2535.dwl	413952	560355CC
<input type="checkbox"/> fwos-E2EFL_FW_2_5_361.dwl	134144	CCB3438B
<input type="checkbox"/> fwos-BE0041E_MG_Main_Router-Pro.20180...	8799681	0B7C18BD
<input type="checkbox"/> fwos-BE0077B_CDMA450_Router-DCU-1s.2...	5608480	D6194E5
<input type="checkbox"/> fwos-E1EFL_FW_2534.dwl	280320	B11271CC
<input type="checkbox"/> fwos-E1EFL_FW_2530-new-bl.dwl	279296	4823D719
<input type="checkbox"/> fwos-E1EFL_FW_2_5_281.dwl	137600	B5E56786
<input type="checkbox"/> fwos-E1EFL_FW_2_5_281-up20200622.dwl	137216	96748698

Filter

Group:

\*

Modem version (to selected):

\*

OS version (to selected):

\*

HW version:

\*

Smart search:

Scope of control

☐ All listed devices

☒ Selected device(s) only

Manage

Upload config

Download config

Upload server data

Set real-time clock

Factory reset

Reboot device

Upgrade OS

Upgrade modem

Remote WIPE

...	Status	IP	MEID / IMEI	Description	RSSI	ECIO	Diag	Uptime	Last refresh	Modem version	OS version	HW version	Zon
	Online	94.44.14.191	51622075254058	4G	-77 dBm	0	N/A	16 20:05:23	2021-04-30 13:07:15	20.00.406	20210219...	BE0077	
	Online	84.224.74.241	53529102558732	LE910-EUG, DDNS, DVR	-65 dBm	3	N/A	1 20:39:18	2021-04-30 13:07:24	20.00.405	20210219...	BE0077	
	Online	172.31.14.25	59852054133815	EASY BACKUP PRODUCTI...	-67 dBm	0	N/A	2 22:46:51	2021-04-30 13:06:53	17.01.522	202012161	BE0077	
	Online	84.224.36.34	59852053517018	Test2 ELS_16-1...	-75 dBm	99	N/A	51 02:03:19	2021-04-30 13:06:41	17.00.523	20210219...	BE0077	
	Online	94.44.7.107	59852054121349	Test3 ELS_1...	-67 dBm	3	N/A	11 22:14:23	2021-04-30 13:06:17	17.01.522	20210219...	BE0077	
	Online	10.202.177.161	58173054771236	EASY BACKUP PRODUCTI...	-77 dBm	99	N/A	36 08:22:04	2021-04-30 13:10:33	REVISION 0...	201803211	BE0041	
	Online	10.202.162.212	51580051015341	EASY BACKUP PRODUCTI...	-89 dBm	0	N/A	29 01:15:17	2021-04-30 13:10:25	12.00.106	201907102	BE0077	
	Online	172.31.86.48	51580050852538	EASY BACKUP PRODUCTI...	-77 dBm	0	N/A	79 13:08:03	2021-04-30 13:09:39	12.00.106	201907102	BE0077	
	Online	172.31.13.182	58173054767267	EASY BACKUP PRODUCTI...	-75 dBm	99	N/A	218 15:18:29	2021-04-30 13:07:45	REVISION 0...	201803211	BE0041	
	Online	10.202.170.16	58173051643651	EASY BACKUP PRODUCTI...	-103 dBm	99	N/A	40 05:04:14	2021-04-30 13:10:47	REVISION 0...	201803211	BE0041	
	Online	172.31.14.233	59852053963238	EASY BACKUP PRODUCTI...	-51 dBm	3	N/A	105 02:41:29	2021-04-30 13:08:44	17.01.522	202012161	BE0077	
	Online	172.31.152.58	51580050846902	EASY BACKUP PRODUCTI...	-87 dBm	0	N/A	17 01:12:16	2021-04-30 13:07:04	12.00.106	201907102	BE0077	
	Online	172.31.158.212	51580051074991	EASY BACKUP PRODUCTI...	-79 dBm	0	N/A	43 02:24:46	2021-04-30 13:07:17	12.00.106	201907102	BE0077	
	Online	172.31.14.193	58173052233528	EASY BACKUP PRODUCTI...	-79 dBm	99	N/A	191 03:27:10	2021-04-30 13:09:42	REVISION 0...	201803211	BE0041	
	Online	172.31.13.178	51580051877385	EASY BACKUP PRODUCTI...	-89 dBm	0	N/A	23 03:21:36	2021-04-30 13:07:20	12.00.108	201907102	BE0077	
	Online	172.31.155.82	59852053963287	EASY BACKUP PRODUCTI...	-75 dBm	1	N/A	1 12:09:47	2021-04				

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 columns: **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.

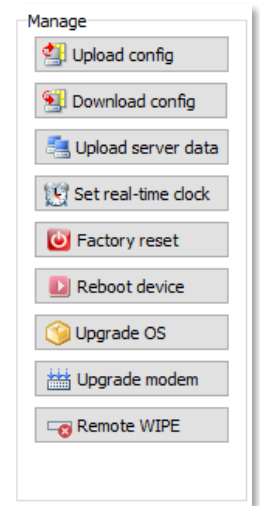
The validity of the data valid for the device can be checked in the **Last refresh** column.

**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 configuration 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



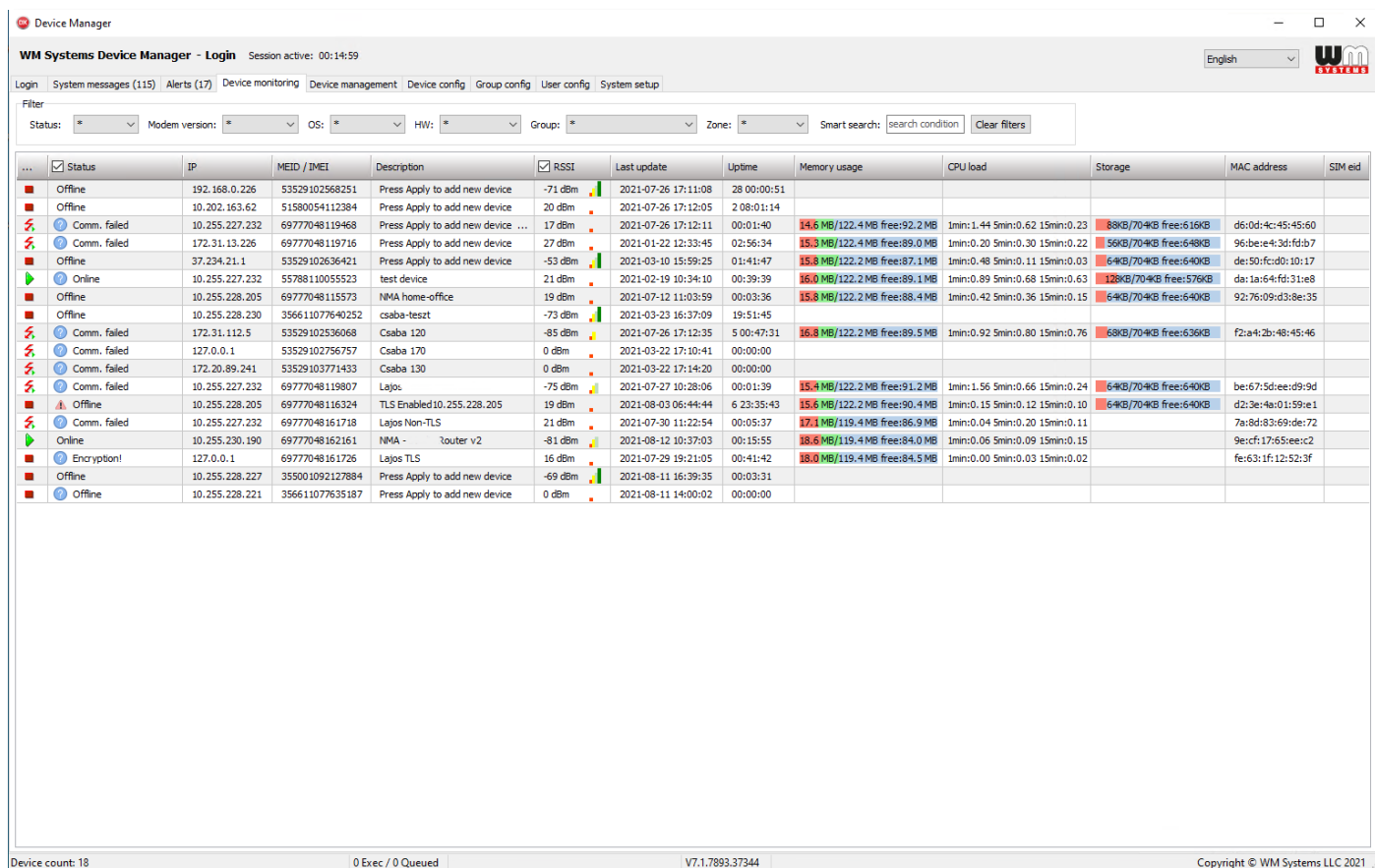
## Chapter 6. Device monitoring

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 columns 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.



The screenshot displays the 'Device Manager' window of the 'WM Systems Device Manager' application. The interface includes a top navigation bar with tabs for 'Login', 'System messages (115)', 'Alerts (17)', 'Device monitoring' (selected), 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. Below the navigation bar is a filter section with dropdown menus for 'Status', 'Modem version', 'OS', 'HW', and 'Group', along with a 'Smart search' field and 'Clear filters' button. The main area contains a table with 13 columns: Status, IP, MEID / IMEI, Description, RSSI, Last update, Uptime, Memory usage, CPU load, Storage, MAC address, and SIM eid. The table lists 18 devices with various statuses including 'Offline', 'Comm. failed', 'Online', and 'Encryption!'. Each row provides detailed information about the device's current state and performance metrics.

Status	IP	MEID / IMEI	Description	RSSI	Last update	Uptime	Memory usage	CPU load	Storage	MAC address	SIM eid
Offline	192.168.0.226	53529102568251	Press Apply to add new device	-71 dBm	2021-07-26 17:11:08	28 00:00:51					
Offline	10.202.163.62	51580054112384	Press Apply to add new device	20 dBm	2021-07-26 17:12:05	2 08:01:14					
Comm. failed	10.255.227.232	69777048119468	Press Apply to add new device ...	17 dBm	2021-07-26 17:12:11	00:01:40	14.6 MB / 122.4 MB free:92.2 MB	1min:1.44 5min:0.62 15min:0.23	88KB / 704KB free:616KB	d6:0d:4c:45:45:60	
Comm. failed	172.31.13.226	69777048119716	Press Apply to add new device	27 dBm	2021-01-22 12:33:45	02:56:34	15.3 MB / 122.4 MB free:89.0 MB	1min:0.20 5min:0.30 15min:0.22	56KB / 704KB free:648KB	96:bce:4:3d:fd:b7	
Online	37.234.21.1	53529102636421	Press Apply to add new device	-53 dBm	2021-03-10 15:59:25	01:41:47	15.8 MB / 122.2 MB free:87.1 MB	1min:0.48 5min:0.11 15min:0.03	64KB / 704KB free:640KB	de:50:fc:d0:10:17	
Online	10.255.227.232	55788110055523	test device	21 dBm	2021-02-19 10:34:10	00:39:39	16.0 MB / 122.2 MB free:89.1 MB	1min:0.89 5min:0.68 15min:0.63	128KB / 704KB free:576KB	da:1a:64:fd:31:e8	
Offline	10.255.228.205	69777048115573	NMA home-office	19 dBm	2021-07-12 11:03:59	00:03:36	15.8 MB / 122.2 MB free:88.4 MB	1min:0.42 5min:0.36 15min:0.15	64KB / 704KB free:640KB	92:76:09:d3:8e:35	
Offline	10.255.228.230	356611077640252	csaba-teszt	-73 dBm	2021-03-23 16:37:09	19:51:45					
Comm. failed	172.31.112.5	53529102536068	Csaba 120	-85 dBm	2021-07-26 17:12:35	5 00:47:31	16.8 MB / 122.2 MB free:89.5 MB	1min:0.92 5min:0.80 15min:0.76	68KB / 704KB free:636KB	f2:a4:2b:48:45:46	
Comm. failed	127.0.0.1	53529102756757	Csaba 170	0 dBm	2021-03-22 17:10:41	00:00:00					
Comm. failed	172.20.89.241	53529103771433	Csaba 130	0 dBm	2021-03-22 17:14:20	00:00:00					
Comm. failed	10.255.227.232	69777048119807	Lajos	-75 dBm	2021-07-27 10:28:06	00:01:39	15.4 MB / 122.2 MB free:91.2 MB	1min:1.56 5min:0.66 15min:0.24	64KB / 704KB free:640KB	be:67:5d:ee:d9:9d	
Offline	10.255.228.205	69777048116324	TLS Enabled 10.255.228.205	19 dBm	2021-08-03 06:44:44	6 23:35:43	15.6 MB / 122.2 MB free:90.4 MB	1min:0.15 5min:0.12 15min:0.10	64KB / 704KB free:640KB	d2:3e:4a:01:59:e1	
Comm. failed	10.255.227.232	69777048161718	Lajos Non-TLS	21 dBm	2021-07-30 11:22:54	00:05:37	17.1 MB / 119.4 MB free:86.9 MB	1min:0.04 5min:0.20 15min:0.11		7a:8d:83:69:de:72	
Online	10.255.230.190	69777048162161	NMA - router v2	-81 dBm	2021-08-12 10:37:03	00:15:55	18.6 MB / 119.4 MB free:84.0 MB	1min:0.06 5min:0.09 15min:0.15		9e:cf:17:65:ee:c2	
Encryption!	127.0.0.1	69777048161726	Lajos TLS	16 dBm	2021-07-29 19:21:05	00:41:42	18.0 MB / 119.4 MB free:84.5 MB	1min:0.00 5min:0.03 15min:0.02		fe:63:1f:12:52:3f	
Offline	10.255.228.227	355001092127884	Press Apply to add new device	-69 dBm	2021-08-11 16:39:35	00:03:31					
Offline	10.255.228.221	356611077635187	Press Apply to add new device	0 dBm	2021-08-11 14:00:02	00:00:00					

### IMPORTANT!

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

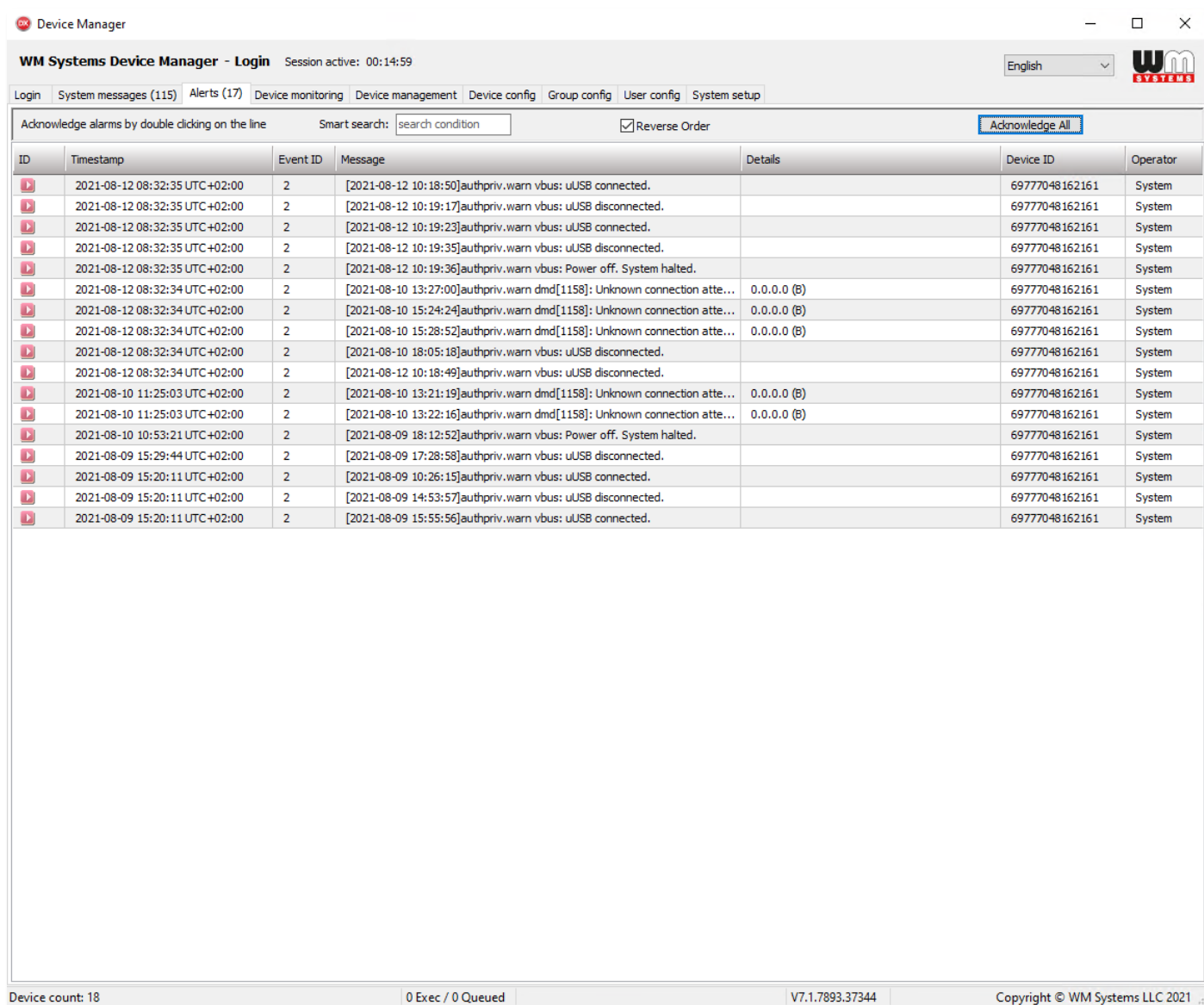
## Chapter 7. Alerts

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.



Device Manager

WM Systems Device Manager - Login Session active: 00:14:59

English

Login System messages (115) Alerts (17) Device monitoring Device management Device config Group config User config System setup

Acknowledge alarms by double clicking on the line Smart search: search condition ☐ Reverse Order [Acknowledge All](#)

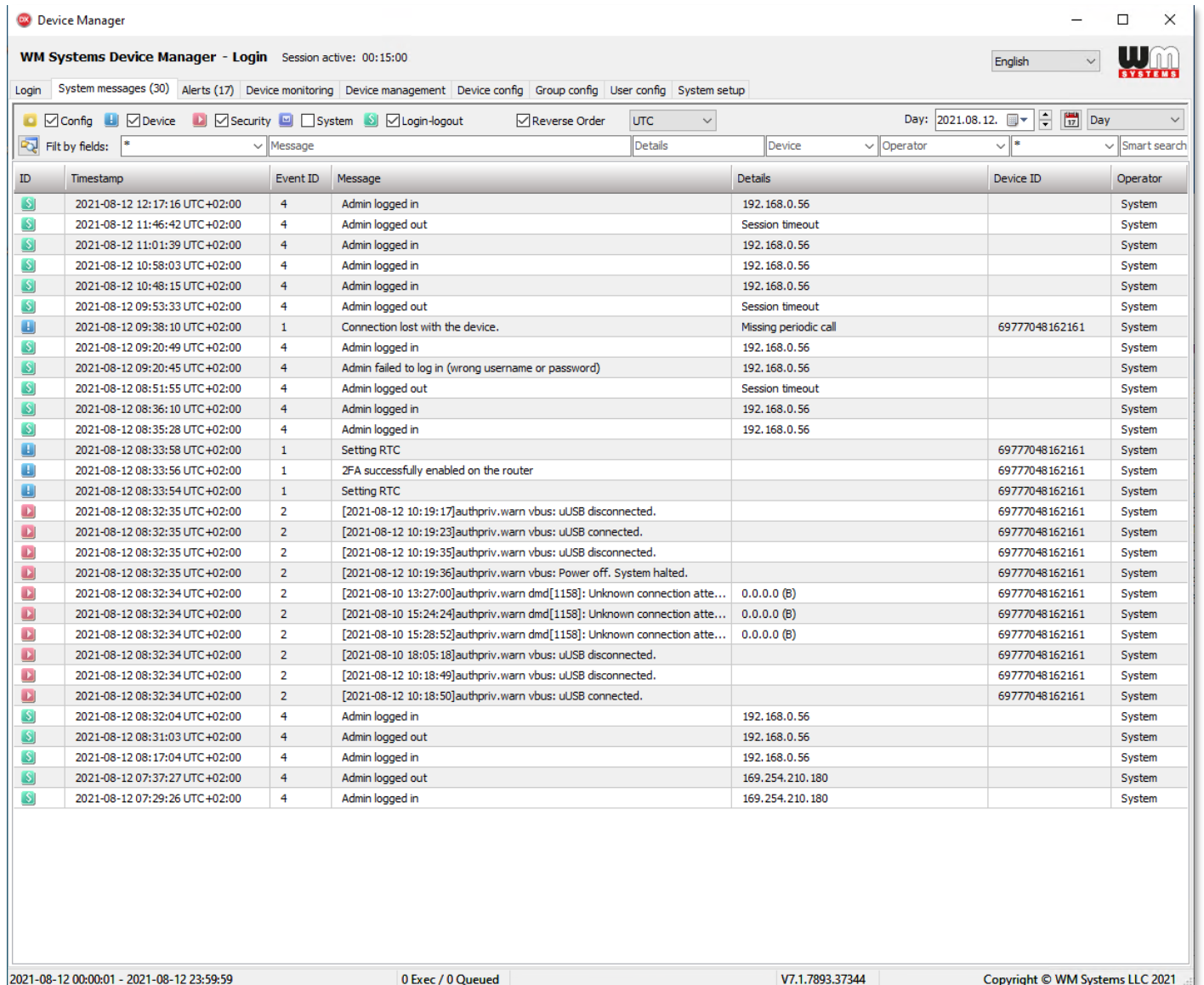
ID	Timestamp	Event ID	Message	Details	Device ID	Operator
	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:18:50]authpriv.warn vbus: uUSB connected.		69777048162161	System
	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:19:17]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:19:23]authpriv.warn vbus: uUSB connected.		69777048162161	System
	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:19:35]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:19:36]authpriv.warn vbus: Power off. System halted.		69777048162161	System
	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-10 13:27:00]authpriv.warn dmd[1158]: Unknown connection atte...	0.0.0.0 (B)	69777048162161	System
	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-10 15:24:24]authpriv.warn dmd[1158]: Unknown connection atte...	0.0.0.0 (B)	69777048162161	System
	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-10 15:28:52]authpriv.warn dmd[1158]: Unknown connection atte...	0.0.0.0 (B)	69777048162161	System
	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-10 18:05:18]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-12 10:18:49]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
	2021-08-10 11:25:03 UTC+02:00	2	[2021-08-10 13:21:19]authpriv.warn dmd[1158]: Unknown connection atte...	0.0.0.0 (B)	69777048162161	System
	2021-08-10 11:25:03 UTC+02:00	2	[2021-08-10 13:22:16]authpriv.warn dmd[1158]: Unknown connection atte...	0.0.0.0 (B)	69777048162161	System
	2021-08-10 10:53:21 UTC+02:00	2	[2021-08-09 18:12:52]authpriv.warn vbus: Power off. System halted.		69777048162161	System
	2021-08-09 15:29:44 UTC+02:00	2	[2021-08-09 17:28:58]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
	2021-08-09 15:20:11 UTC+02:00	2	[2021-08-09 10:26:15]authpriv.warn vbus: uUSB connected.		69777048162161	System
	2021-08-09 15:20:11 UTC+02:00	2	[2021-08-09 14:53:57]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
	2021-08-09 15:20:11 UTC+02:00	2	[2021-08-09 15:55:56]authpriv.warn vbus: uUSB connected.		69777048162161	System

Device count: 18 0 Exec / 0 Queued V7.1.7893.37344 Copyright © WM Systems LLC 2021

## Chapter 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.



Device Manager

WM Systems Device Manager - Login Session active: 00:15:00 English

Login System messages (30) Alerts (17) Device monitoring Device management Device config Group config User config System setup

Filter by fields: \* Message Details Device Operator \* Smart search

ID	Timestamp	Event ID	Message	Details	Device ID	Operator
[S]	2021-08-12 12:17:16 UTC+02:00	4	Admin logged in	192.168.0.56		System
[S]	2021-08-12 11:46:42 UTC+02:00	4	Admin logged out	Session timeout		System
[S]	2021-08-12 11:01:39 UTC+02:00	4	Admin logged in	192.168.0.56		System
[S]	2021-08-12 10:58:03 UTC+02:00	4	Admin logged in	192.168.0.56		System
[S]	2021-08-12 10:48:15 UTC+02:00	4	Admin logged in	192.168.0.56		System
[S]	2021-08-12 09:53:33 UTC+02:00	4	Admin logged out	Session timeout		System
[!]	2021-08-12 09:38:10 UTC+02:00	1	Connection lost with the device.	Missing periodic call	69777048162161	System
[S]	2021-08-12 09:20:49 UTC+02:00	4	Admin logged in	192.168.0.56		System
[S]	2021-08-12 09:20:45 UTC+02:00	4	Admin failed to log in (wrong username or password)	192.168.0.56		System
[S]	2021-08-12 08:51:55 UTC+02:00	4	Admin logged out	Session timeout		System
[S]	2021-08-12 08:36:10 UTC+02:00	4	Admin logged in	192.168.0.56		System
[S]	2021-08-12 08:35:28 UTC+02:00	4	Admin logged in	192.168.0.56		System
[!]	2021-08-12 08:33:58 UTC+02:00	1	Setting RTC		69777048162161	System
[!]	2021-08-12 08:33:56 UTC+02:00	1	2FA successfully enabled on the router		69777048162161	System
[!]	2021-08-12 08:33:54 UTC+02:00	1	Setting RTC		69777048162161	System
[!]	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:19:17]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
[!]	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:19:23]authpriv.warn vbus: uUSB connected.		69777048162161	System
[!]	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:19:35]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
[!]	2021-08-12 08:32:35 UTC+02:00	2	[2021-08-12 10:19:36]authpriv.warn vbus: Power off. System halted.		69777048162161	System
[!]	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-10 13:27:00]authpriv.warn dmd[1158]: Unknown connection atte...	0.0.0.0 (B)	69777048162161	System
[!]	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-10 15:24:24]authpriv.warn dmd[1158]: Unknown connection atte...	0.0.0.0 (B)	69777048162161	System
[!]	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-10 15:28:52]authpriv.warn dmd[1158]: Unknown connection atte...	0.0.0.0 (B)	69777048162161	System
[!]	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-10 18:05:18]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
[!]	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-12 10:18:49]authpriv.warn vbus: uUSB disconnected.		69777048162161	System
[!]	2021-08-12 08:32:34 UTC+02:00	2	[2021-08-12 10:18:50]authpriv.warn vbus: uUSB connected.		69777048162161	System
[S]	2021-08-12 08:32:04 UTC+02:00	4	Admin logged in	192.168.0.56		System
[S]	2021-08-12 08:31:03 UTC+02:00	4	Admin logged out	192.168.0.56		System
[S]	2021-08-12 08:17:04 UTC+02:00	4	Admin logged in	192.168.0.56		System
[S]	2021-08-12 07:37:27 UTC+02:00	4	Admin logged out	169.254.210.180		System
[S]	2021-08-12 07:29:26 UTC+02:00	4	Admin logged in	169.254.210.180		System

2021-08-12 00:00:01 - 2021-08-12 23:59:59 0 Exec / 0 Queued V7.1.7893.37344 Copyright © WM Systems LLC 2021

# Chapter 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.



## Chapter 10. Legal notice

©2021. WM Systems LLC.

The content of this documentation (all information, pictures, tests, descriptions, guides, logos) is under copyright protection. Copying, using, distributing and publishing is only permitted with the consent of WM Systems LLC., with clear indication of the source.

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.