

# Device Manager<sup>®</sup>

## for M2M Router devices

# User Manual

## v2.20

The screenshot displays the 'Device Manager' web interface. The top navigation bar includes 'Login', 'System messages (45/8)', 'Alerts (46/3)', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. The main content area is divided into several configuration panels: 'General settings' (Type: 4G, IMEI: 69777048116951, MSIN: 001e049205, Network IP: 10.217.105.81, Port: 22/443, Login name: root, Password: [masked], Description: Stedin test), 'Modem settings' (Watchdog: 0h, Power on delay: 0s, Cyclic sending: 300s, Time window: 120s), 'LAN DHCP settings' (Start: 0, Limit: 0, Lease time: 0h, Alert: RSSI warnings: 12, RSSI error: 8), 'LAN IP settings' (Comm: checked, Local IP: 10.10.0.1, Netmask: 255.255.255.0, Gateway: [empty], Broadcast: [empty], Port forward: [empty], Port route: [empty]), and 'WAN settings' (User name: [empty], Password: [empty]).

Below the configuration panels is a table listing devices. The table has columns for Status, IP, MEID / IMEI, Description, RSSI, ECI0, Diag, Uptime, Last refresh, Modem version, OS version, and HW version. The table contains 20 rows of device data, with the 16th row (IP: 10.217.105.81) highlighted in blue.

Status	IP	MEID / IMEI	Description	RSSI	ECI0	Diag	Uptime	Last refresh	Modem version	OS version	HW version
Online	10.255.228.222	206611075302918	ORT - 11 - vme15 - Csaba	-80 dBm	0	N/A	16:04:08	2021-02-04 20:46:57	LE910-EU1 2...	V2.5.47	W
Offline	10.217.96.88	53529102758043	EASY BACKUP PRODUCTION - BACKU...	-81 dBm	1	N/A	03:10:40	2021-02-27 02:34:34	20.00.405	202011021	BE
Offline	10.217.104.36	356611076822495	ORT - 03 - vme26 - Csaba	-60 dBm	0	N/A	12:01:47	2021-02-04 02:26:04	LE910-EU1 2...	V2.5.55	W
Offline	10.255.228.225	356611075502926	E-test2 - Tdv 01 - vme16 - Csaba	-73 dBm	0	N/A	04:56:20	2020-11-25 15:18:47	LE910-EU1 2...	V2.5.47	W
Offline	10.255.228.224	356611077858409	E-test2 - sm010 - vme26 - Csaba	-75 dBm	0	N/A	16:57:26	2020-11-19 10:02:57	LE910-EU1 2...	V2.5.56	W
Offline	10.255.228.230	356611075499578	E-Test2 - sm106 - vme26 - Csaba	-77 dBm	0	N/A	17:02:19	2020-11-19 10:04:12	LE910-EU1 2...	V2.5.56	W
Online	91.104.150.159	53529102544336	stream pro4	-69 dBm	4	N/A	07:03:19	2021-04-29 15:07:23	20.00.403	202011161	BE
Online	172.31.87.71	51622076472675	EASY BACKUP PRODUCTION - BACKU...	-71 dBm	1	N/A	1:06:04:18	2021-04-29 15:06:03	20.00.405	202012161	BE
Offline	10.217.104.29	53529102716256	Xylem router 02	-79 dBm	4	N/A	16:06:47	2021-04-28 19:00:40	20.00.405	202011021	BE
Online	10.217.104.18	58173054763217	Xylem router 01	-83 dBm	99	N/A	1:04:11:08	2021-04-29 15:06:14	REVISION 0...	201803211	BE
Online	192.168.0.226	53529102568251	Telecom GW	-75 dBm	0	N/A	22:39:37	2021-04-29 15:07:41	20.00.405	202012161	BE
Online	192.168.0.227	51580051968861	Telecom GW	-79 dBm	0	N/A	22:39:48	2021-04-29 15:07:51	12.00.108	202012161	BE
Online	10.217.105.81	69777048116951	Stedin test2	-63 dBm	99	N/A	2:14:31:42	2021-04-29 15:08:38	Revision:15...	20210215...	BE
Online	10.217.105.3	53529102541738	Stedin test2	-57 dBm	1	N/A	1:08:12:08	2021-04-29 15:04:59	20.00.405	202011161	BE
Online	172.31.150.255	53529103780889	EASY BACKUP PRODUCTION - PALFFY...	-89 dBm	1	N/A	57:21:56:29	2021-04-29 15:06:08	20.00.405	202012161	BE
Offline	5.204.109.31	55788110136018	Press Apply to add new device	-57 dBm	3	N/A	05:25:22	2021-04-22 17:59:58	MOF_223001	202104161	BE
Offline	84.224.130.20	69777048116366	Stedin test2	-51 dBm	0	N/A	02:37:43	2021-04-28 19:12:29	Revision:19...	20210428...	BE

At the bottom of the interface, it shows 'Device count: 80', '0 Exec / 0 Queued', 'V7.1.7788.53129', and 'Copyright © WM Systems LLC 2021'.

2021-08-13

## Document specifications

This document was made for the **Device Manager**<sup>®</sup> 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 <sup>®</sup>
<b>Author:</b>	WM Systems LLC
<b>Document version No.:</b>	REV 2.20
<b>Number of pages:</b>	32
<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> .....	4
<b>2. Setup and Configuration</b> .....	5
2.1 Prerequisites .....	5
2.2 System elements.....	5
2.3 Installation.....	5
2.4 TLS protocol communication .....	7
<b>3. System configuration</b> .....	9
3.1 System setup .....	9
3.2 User settings.....	13
<b>4. Device settings</b> .....	17
4.1 Device group configuration .....	17
4.2 Device configuration for modems .....	18
4.3 General settings .....	20
4.4 Location settings .....	23
4.5 Miscellaneous settings .....	23
4.6 Package List.....	23
4.7 2-Factor Authentication settings .....	24
4.8 TLS settings.....	25
<b>5. Device monitoring</b> .....	25
<b>6. Device management</b> .....	27
<b>7. Alerts</b> .....	29
<b>8. System messages</b> .....	30
<b>9. Support</b> .....	31
9.1 Technical Support .....	31
9.2 GPL license .....	31
<b>10. Legal notice</b> .....	32

# 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<sup>®</sup>-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<sup>®</sup> 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.

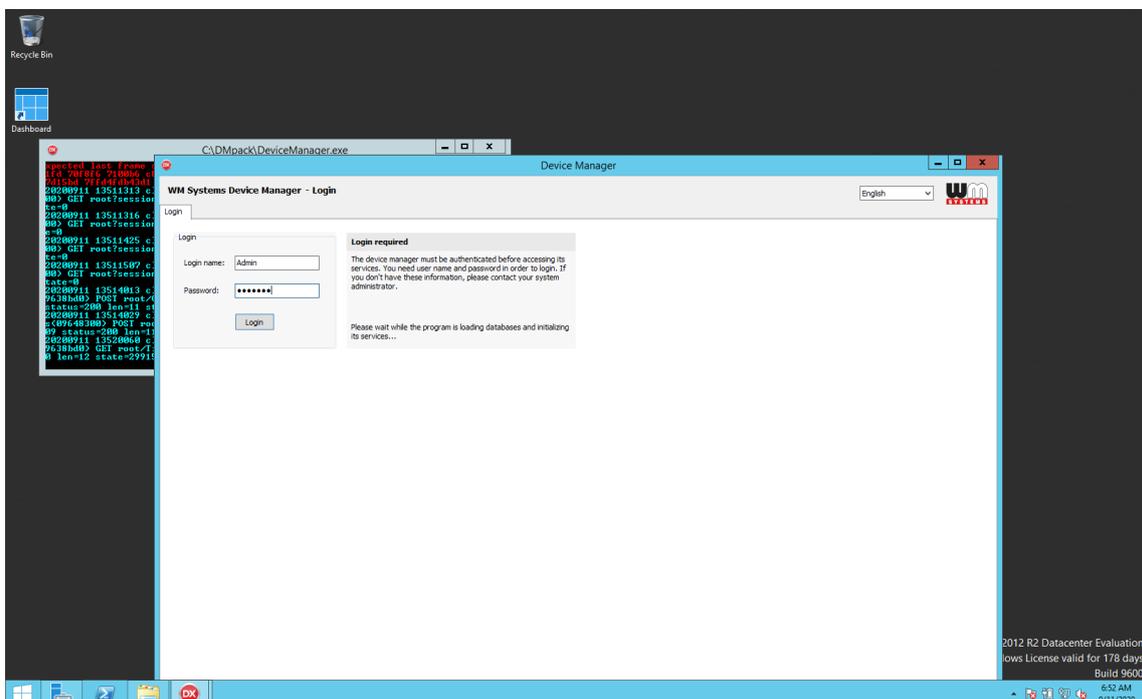
### 3. Modify the configuration file: *DeviceManager.config*

(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.

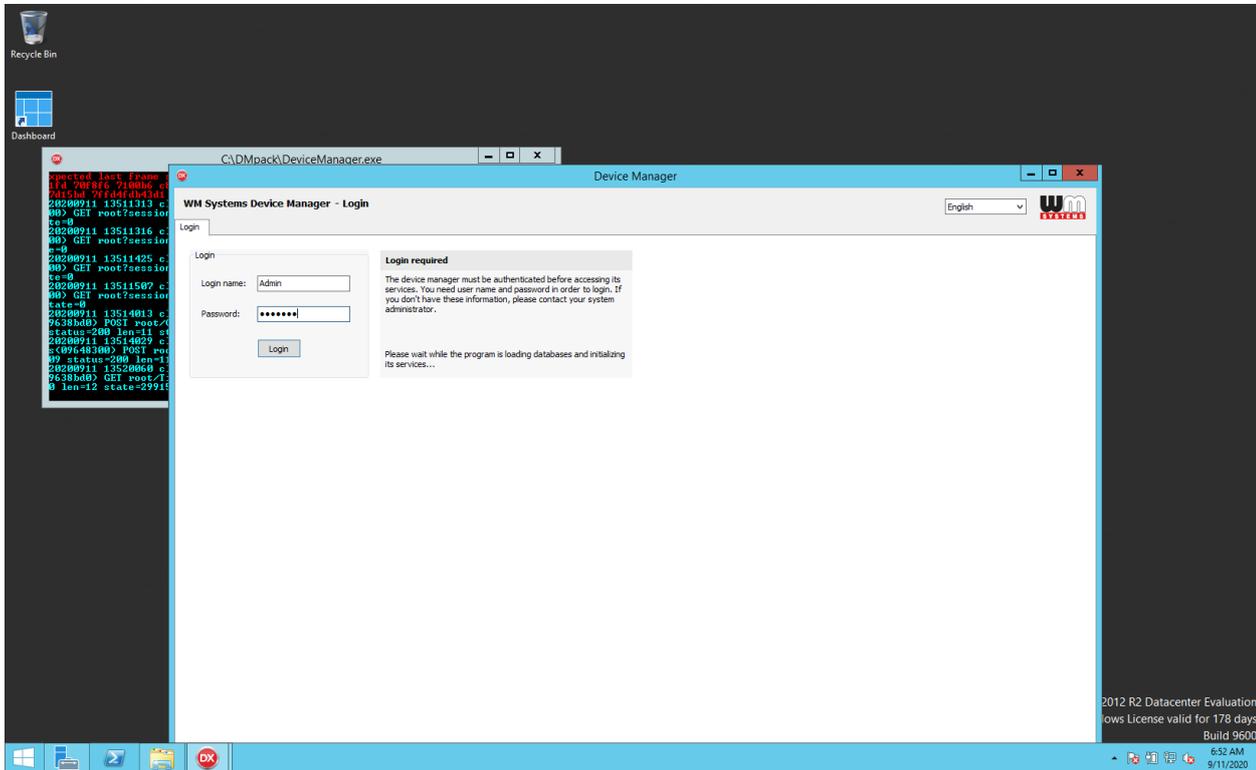


5. You have to **Login** by the following credentials:

- **Login name: Admin - Password: synopsis**

*(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

Remote SNMP (manager)

SNMP level:  v1  v2c  v3

Host:

User name:

Password:

Privacy pass:

Trap mode:  Generic  
 Granular  
 Variable bindings

Enable trap sending

The screenshot shows the 'System setup' tab in the Device Manager application. The interface is divided into several panels:

- Remote SNMP (manager):** Includes fields for SNMP level (v1 selected), Host (192.168.0.202), User name (User), Password, Privacy pass, and Trap mode (Generic selected). A checkbox for 'Enable trap sending' is checked.
- Server settings:** Includes Server name (Device Manager from WMSYSTEM), Server IP address (172.31.112.225), Listening port to modems (57605), Listening port of Web Service (49983), and Proxy Settings.
- Data Broker:** Includes Address (192.168.0.56), Port (888), Supervisor Port (888), and a 'Check' button.
- Miscellaneous:** Includes Zone limit, Comm (0), Update (0), Modem upgrade path (/var/fw), Chunk (32), Block (512), and 'Enable Active Directory' checked.
- Security (AES 256):** Includes 'Encrypted' and 'Random IV' checked, 'Authenticated' checked, and 'Save keys' button.
- Quick Login:** Includes 'Remember login name and password' checked.
- Automatic data maintenance:** Includes 'Keep data of the last: 6 months'.
- External alarm server:** Includes 'Not used' selected, OS Event Viewer, and SysLog Server options.
- Remote LogView Server:** Includes 'Enable remote logging' unchecked, Server (127.0.0.1), and Port (8091).
- DM Service Management:** Includes buttons for 'Start DM service', 'Stop DM service', 'Restart service', 'Apply settings', and 'Undo'.

- 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

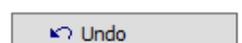
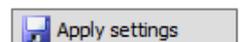
**Privacy pass:** Required when the v3 SNMP level is selected. The authentication is possible by any of the SNMP-enabled users plus the privacy pass specified here. Of course, this setting must be the same as that of the SNMP manager.

**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

Default security key

Specific security key (32 char):

Quick Login

Remember login name and password

Automatic data maintenance

Keep data of the last:  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:

Port:

Supervisor Port:

Miscellaneous

Zone limit: Comm:  Update:

Limit the number of devices per zone processing upgrade

Modem upgrade path: /var/fw

Chunk:  Block:

Enable Active Directory

Time format:

Max. parallel threads:

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

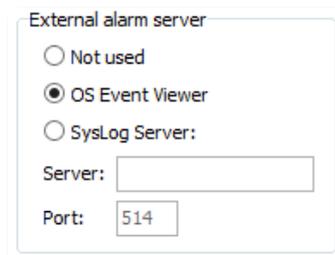
**Time format:** can be *Local time* or *UTC*

**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



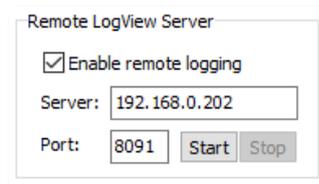
The screenshot shows a window titled "External alarm server". It contains three radio button options: "Not used", "OS Event Viewer" (which is selected), and "SysLog Server:". Below the "SysLog Server:" option, there are two input fields: "Server:" and "Port:". The "Port:" field contains the value "514".

### 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

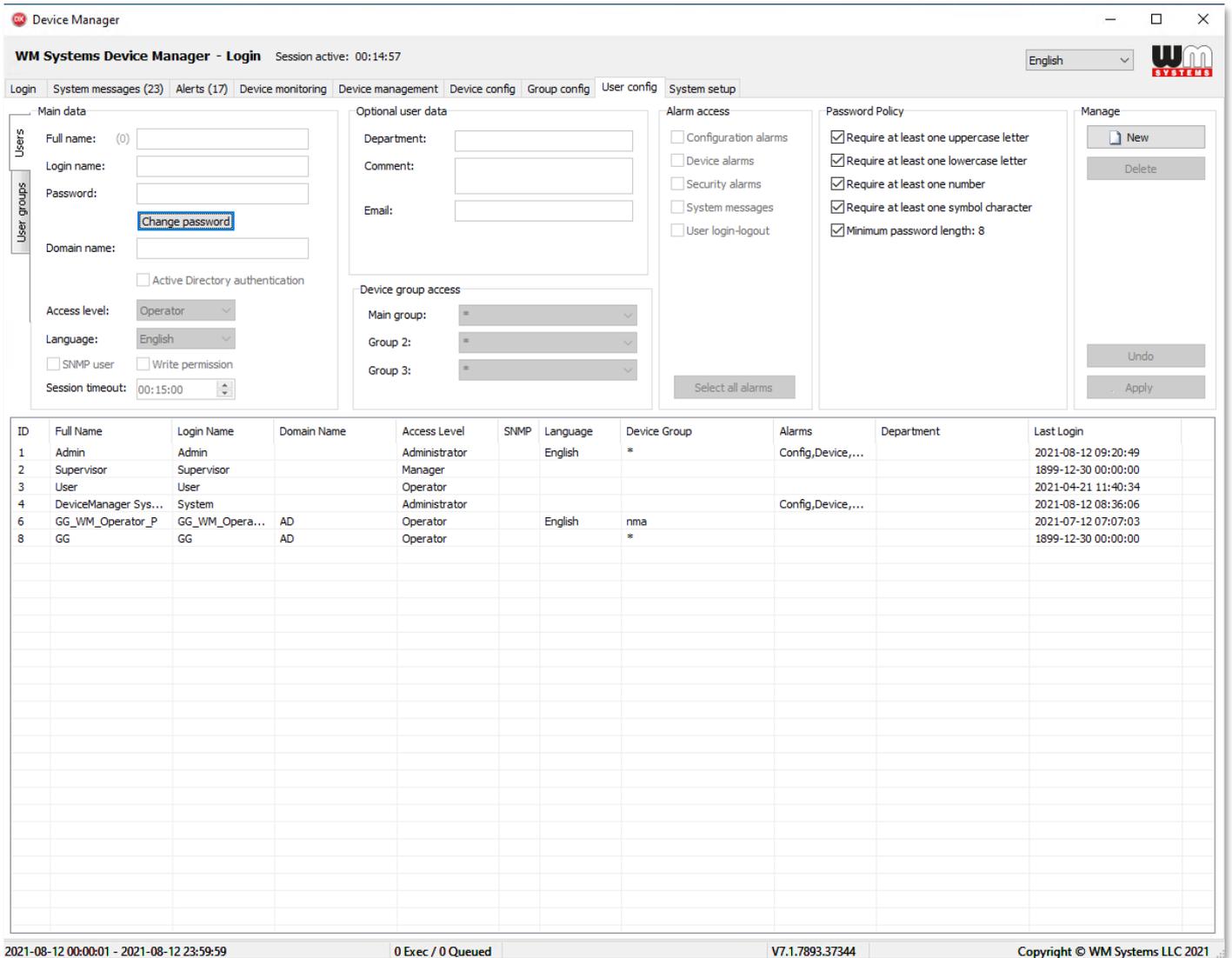


The screenshot shows a window titled "Remote LogView Server". It contains a checked checkbox labeled "Enable remote logging". Below this, there are two input fields: "Server:" containing "192.168.0.202" and "Port:" containing "8091". To the right of the "Port:" field are two buttons labeled "Start" and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

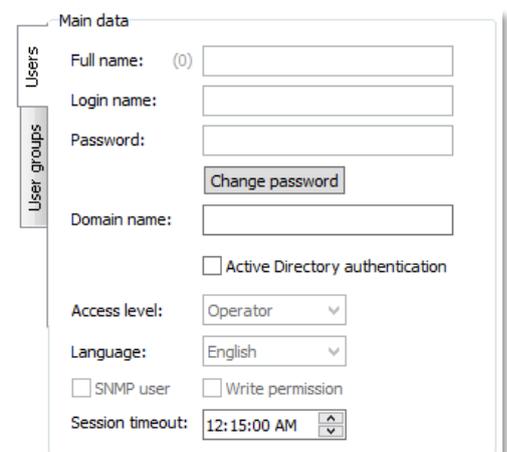
**Full name:** User real name

**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.

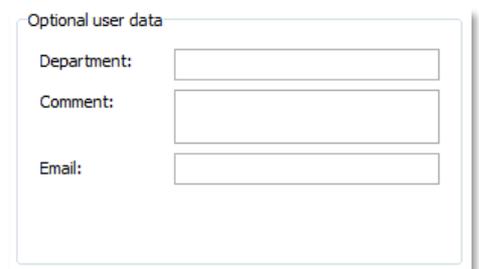
**Session timeout:** automatic logout can be also defined.

### **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!)



Optional user data

Department:	<input type="text"/>
Comment:	<input type="text"/>
Email:	<input type="text"/>

### **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)



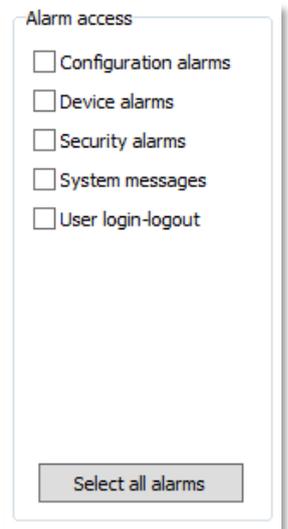
Device group access

Main group:	<input type="text" value="*"/>	▼
Group 2:	<input type="text" value="*"/>	▼
Group 3:	<input type="text" value="*"/>	▼

## **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.



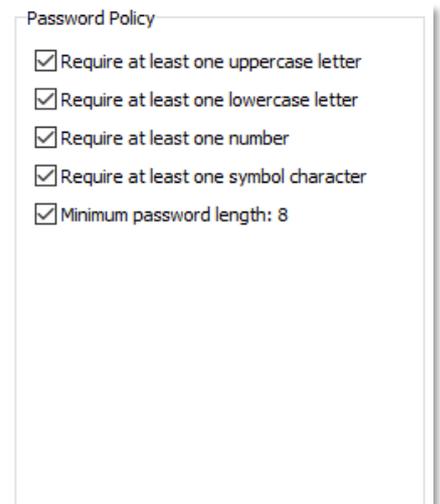
Alarm access

- 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.



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.

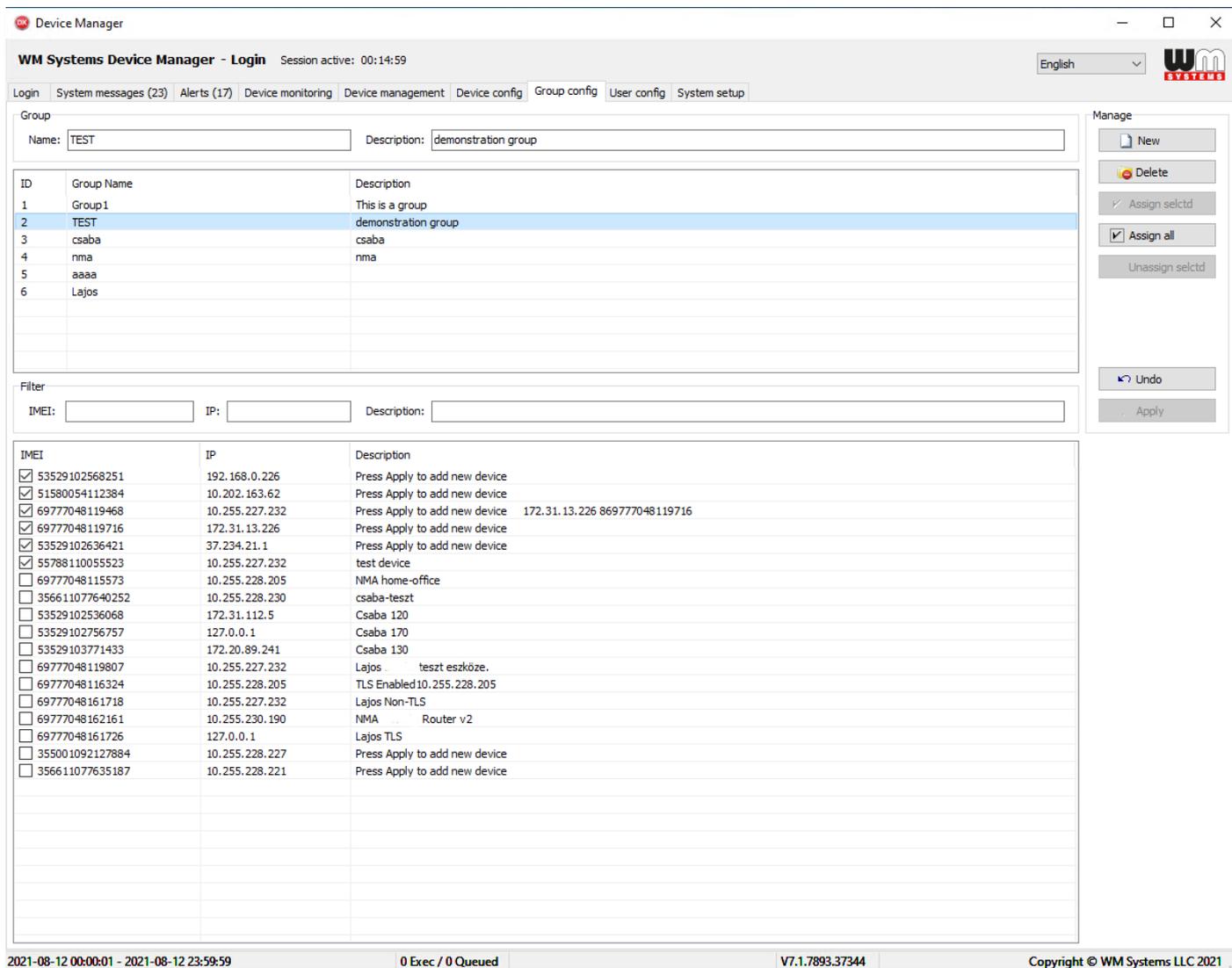
If you want to add more devices for an existing group, just check in the new device(s).

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

A new device group can be also defined here.

Press the  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.



**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

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 be 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 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 'Device Manager' interface for 'WM Systems Device Manager - Login'. The top navigation bar includes tabs for 'System messages (115)', 'Alerts (17)', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. The 'Device config' tab is active, showing various configuration sections: General settings (Type: 4G, Enabled), Modem settings (Watchdog: 0h, Power on delay: 0s, rmd: 10s, Cyclic sending: 3600s, Time window: 60s), LAN DHCP settings (Enabled, Start: 100, Limit: 150, Lease time: 12h), Alert settings (RSSI warning: 0, RSSI error: 0), LAN IP settings (Comm: Disabled, Ping enabled, Local IP: 192.168.127.1, Netmask: 255.255.255.0), WAN settings (User name, Password, Enable), and APN settings (Name: wim2m).

Below the configuration panels is a table of managed devices with the following columns: Status, IP, MEID / IMEI, Description, RSSI / CSQ, ECTO, Diag, Uptime, Last refresh, Modem version, OS version, HW version, Zone, FWSTM32, and wdt-ctr. The table contains 20 rows of device data, with the last row (IP: 10.255.228.205, MEID/IMEI: 69777048161726) highlighted in blue. The status of devices varies, including 'Offline', 'Comm. failed', and 'Online'.

At the bottom of the interface, there is a 'Device count: 18' indicator, a '0 Exec / 0 Queued' status, a version number 'V7.1.7893.37344', and a copyright notice 'Copyright © WM Systems LLC 2021'.

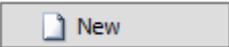
You can check the device- and network properties (**IP** address, **IMEI/MEID**), their availability by analysing the **Last Refresh** information (date/time of last known status) with the **Uptime** (when the device was rebooted / started last time).

The cellular network performance indexes are also available at **RSSI / CSQ** (signal strength), **ECIO**.

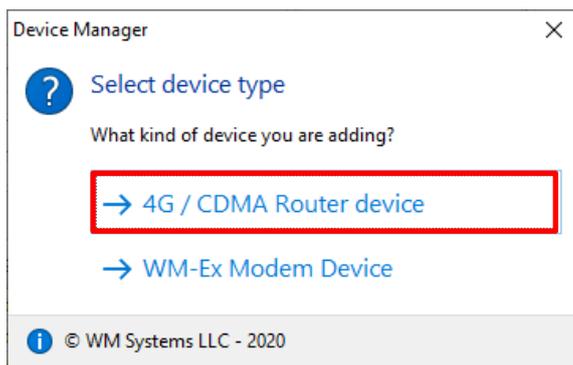
The **Modem version**, **OS version** (date of the build), **HW version** (PCB identifier), **FWSTM32** (Microcontroller firmware version) are also available here.

	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

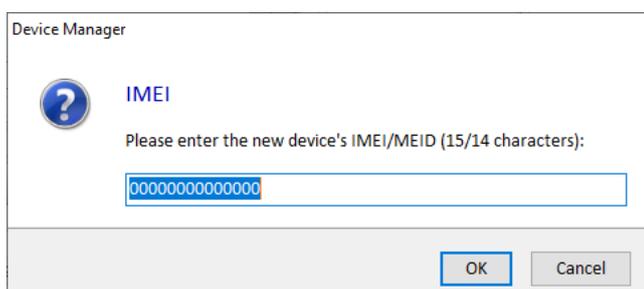
When you've selected a device from the list, you can click with right mouse button to the element, and the following right submenu appears, where you can choose from the available features to perform an interaction on the device.

You can also add further new devices by the  button.

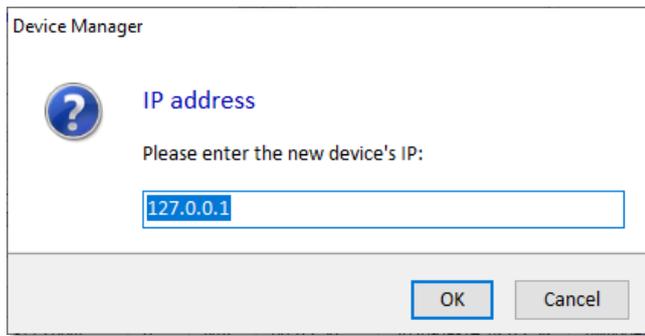
For routers you have to first select the device type: **4G / CDMA Router device**.



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

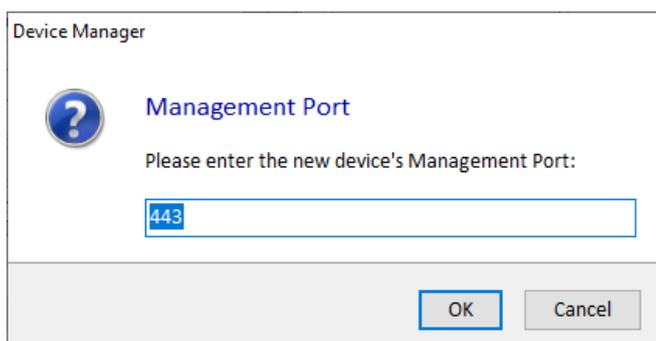


Add the **IP address** of the device.



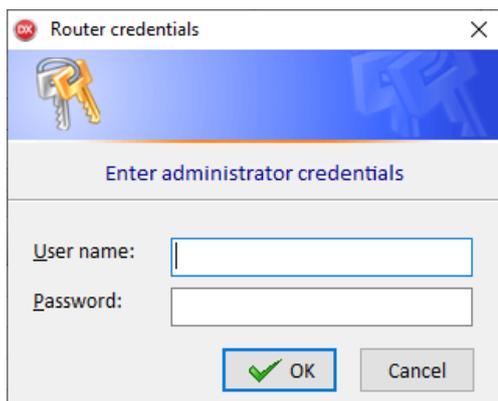
The image shows a 'Device Manager' dialog box with a question mark icon. The title is 'IP address'. Below the icon, it says 'Please enter the new device's IP:'. There is a text input field containing '127.0.0.1'. At the bottom, there are 'OK' and 'Cancel' buttons.

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.



The image shows a 'Device Manager' dialog box with a question mark icon. The title is 'Management Port'. Below the icon, it says 'Please enter the new device's Management Port:'. There is a text input field containing '443'. At the bottom, there are 'OK' and 'Cancel' buttons.

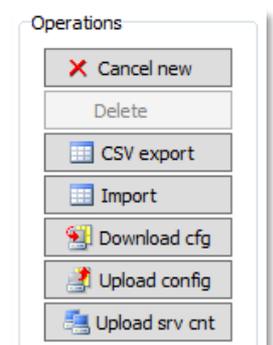
Then you have to fill the administrator credentials (**user name, password**) to add the new device to the Device Manager.



The image shows a 'Router credentials' dialog box with a key icon. The title is 'Router credentials'. Below the icon, it says 'Enter administrator credentials'. There are two text input fields: 'User name:' and 'Password:'. At the bottom, there are 'OK' and 'Cancel' buttons.

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



The image shows a vertical sidebar titled 'Operations'. It contains several buttons: 'Cancel new' (with a red X icon), 'Delete', 'CSV export' (with a grid icon), 'Import' (with a grid icon), 'Download cfg' (with a download icon), 'Upload config' (with an upload icon), and 'Upload srv cnt' (with an upload icon).

- **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

The screenshot shows the 'Device Manager' application window. The title bar reads 'WM Systems Device Manager - Login' with a session active for 00:14:59. The interface includes a navigation menu with tabs: Login, System messages (115), Alerts (17), Device monitoring, Device management, Device config (selected), Group config, User config, and System setup. The 'Device config' tab is active, displaying various configuration sections:

- General settings:** Type: 4G, Enabled, IMEI: 69777048162161, ICC: 8936200003171059925f, Network IP: 10.255.230.190, Port (SSH/SRV): 22 / 443, Login name: root, Password: [masked], Description: NMA - Router v2, Group: [empty].
- Modem settings:** Watchdog: 0 h, Power on delay: 0 s rnd: 10 s, Cyclic sending (by modem): 3600 s, Time window: 60 s.
- LAN DHCP settings:** Enabled, Start: 100, Limit: 150, Lease time: 12 h.
- Alert:** Enable, RSSI warning: 0, RSSI error: 0.
- Timezone:** Name: Europe/Budapest.
- LAN IP settings:** Comm: [Nat] [Disabled] [Ping enabled], Local IP: 192.168.127.1, Netmask: 255.255.255.0, Gateway: [empty], Broadcast: [empty], Port forward: [empty], Port route: [empty].
- WAN settings:** Edit, User name: [empty], Password: [masked], Enable, Change password.
- APN:** Name: wm2m.
- Operations:** New, Delete, CSV export, Import, Download cfg, Upload config, Upload srv cnt, Undo, Apply.

**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).

The screenshot shows the 'WM Systems Device Manager - Login' interface. The 'Location' tab is selected in the left sidebar. The main content area is divided into three sections: 'Contact', 'Location', and 'GPS'. The 'Contact' section has fields for 'Name' and 'Phone'. The 'Location' section has fields for 'Street', 'District', 'City', and 'Postal code'. The 'GPS' section has fields for 'Long' and 'Lat', with a note: 'Set GPS coordinates simply by clicking on the map'. Below these sections is a 'Description' field containing 'NMA - Router v2'. On the right side, there is an 'Operations' panel with buttons for 'New', 'Delete', 'CSV export', 'Import', 'Download cfg', 'Upload config', and 'Upload srv cnt'. At the bottom right, there are 'Undo' and 'Apply' buttons.

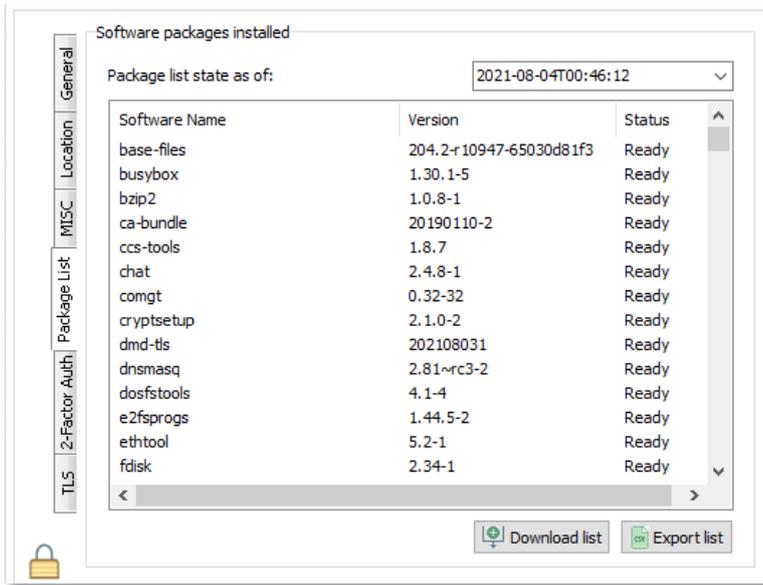
## 4.5 Miscellaneous settings

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

The screenshot shows the 'WM Systems Device Manager - Login' interface with the 'MISC' tab selected. The main content area is divided into three sections: 'GRE', 'Periodic reboot', and 'Periodic ping'. The 'GRE' section has an 'Enable' checkbox, 'Remote address', and 'Pipe address' fields. The 'Periodic reboot' section has an 'Enable' checkbox and an 'HH:MM' field. The 'Periodic ping' section has an 'Enable' checkbox, 'IP', 'Ping failure', and 'Ping interval' fields. Below these sections are 'Route net' and 'Route masklen' fields, with a 'DMVPN' checkbox. On the right side, there is an 'Operations' panel with buttons for 'New', 'Delete', 'CSV export', 'Import', 'Download cfg', 'Upload config', and 'Upload srv cnt'. At the bottom right, there are 'Undo' and 'Apply' buttons.

## 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).

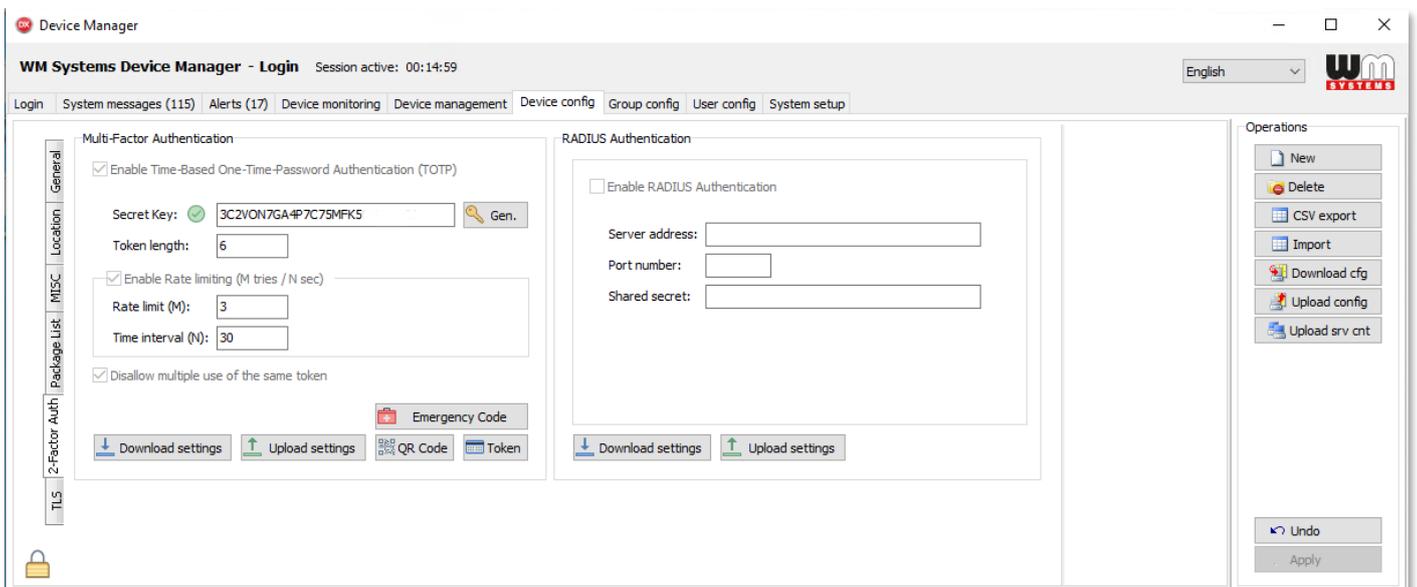


## 4.7 2-Factor Authentication settings

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.

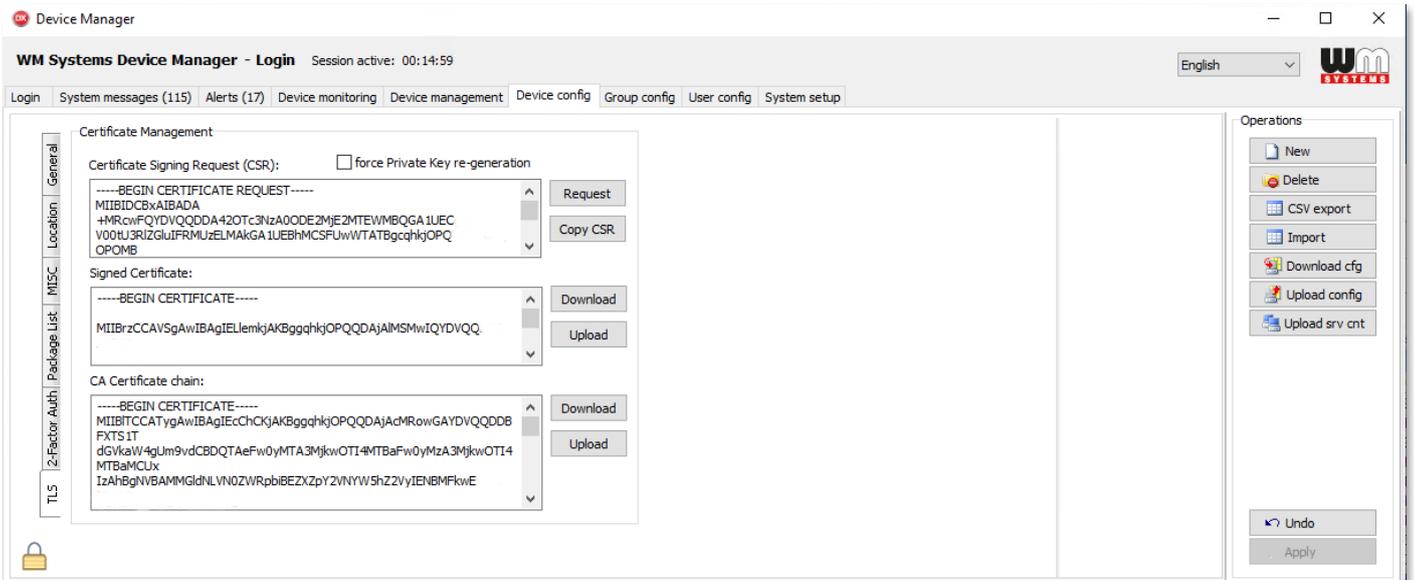
Here you can also select the **Download settings** or **Upload settings** by its buttons for the easier configuration.



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.

The screenshot shows the 'Device Manager' interface with the 'Device management' tab selected. It features a table of devices with columns for status, IP, MEID/IMEI, description, RSSI, ECIO, Diag, Uptime, Last refresh, Modem version, OS version, HW version, and Zone. The status column uses pictograms: a red 'X' for 'Comm. failed', a green 'G' for 'Online', and a red square for 'Encryption!'. The table contains 12 rows of device data.

...	Status	IP	MEID / IMEI	Description	RSSI	ECIO	Diag	Uptime	Last refresh	Modem version	OS version	HW version	Zone
	Comm. failed	10.255.227.232	69777048119468	Press Apply to add new d...	17 dBm	99	N/A	00:01:40	2021-07-26 17:12:11	Revision:19...	202101211	BE0077	1
	Comm. failed	172.31.13.226	69777048119716	Press Apply to add new d...	27 dBm	99	N/A	02:56:34	2021-01-22 12:33:45	Revision:19...	202101211	BE0077	1
	Online	10.255.227.232	55788110055523	test device	21 dBm	3	N/A	00:39:39	2021-02-19 10:34:10	MOF.223001	202102181	BE0077	2
	Comm. failed	172.31.112.5	53529102536068	Csaba 120	-85 dBm	1	N/A	5 00:47:31	2021-07-26 17:12:35	20.00.405	20210318...	BE0077	2
	Comm. failed	127.0.0.1	53529102756757	Csaba 170	0 dBm	0	N/A	00:00:00	2021-03-22 17:10:41				1
	Comm. failed	172.20.89.241	53529103771433	Csaba 130	0 dBm	0	N/A	00:00:00	2021-03-22 17:14:20				1
	Comm. failed	10.255.227.232	69777048119807	Lajos	-75 dBm	5	N/A	00:01:39	2021-07-27 10:28:06	Revision:19...	20210429...	BE0104	2
	Comm. failed	10.255.227.232	69777048161718	Lajos Non-TLS	21 dBm	0	N/A	00:05:37	2021-07-30 11:22:54	Revision:19...	202107291	BE0106	0
	Online	10.255.230.190	69777048162161	NMA - Router v2	-81 dBm	99	N/A	00:15:55	2021-08-12 10:37:03	Revision:19...	202108042	BE0106	0
	Encryption!	127.0.0.1	69777048161726	Lajos TLS	16 dBm	99	N/A	00:41:42	2021-07-29 19:21:05	Revision:19...	202107291	BE0106	0

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.

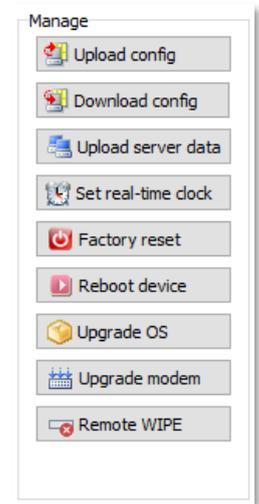
The validity of the data valid for the device can be checked in the **Last refresh** column.

**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

## 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 (**RSST**), 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 shows the 'Device Manager' window with the 'Device monitoring' tab selected. The table below represents the data shown in the interface.

...	Status	IP	MEID / IMEI	Description	RSST	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:be:e4:3d:fd:b7	
	Offline	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					

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

### 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.

The screenshot shows the 'Alerts' tab in the WM Systems Device Manager interface. The window title is 'WM Systems Device Manager - Login' with a session active for 00:14:59. The interface includes a navigation menu with options like 'Login', 'System messages (115)', 'Alerts (17)', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. The 'Alerts (17)' tab is selected. Below the navigation, there is a search bar with the text 'Smart search: search condition' and a checked 'Reverse Order' option. An 'Acknowledge All' button is visible in the top right of the alert list area. The main area contains a table with 7 columns: ID, Timestamp, Event ID, Message, Details, Device ID, and Operator. The table lists 17 alerts, each with a red play button icon in the ID column. The messages include events such as 'uUSB connected', 'uUSB disconnected', 'Power off. System halted', and 'Unknown connection attempt'. The bottom status bar shows 'Device count: 18', '0 Exec / 0 Queued', 'V7.1.7893.37344', and 'Copyright © WM Systems LLC 2021'.

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

## 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.

The screenshot shows the 'WM Systems Device Manager - Login' interface. The 'System messages (30)' tab is active. The interface includes a navigation bar with tabs like 'Login', 'System messages (30)', 'Alerts (17)', etc. Below the navigation bar, there are filter options for event types (Config, Device, Security, System, Login-logout) and a 'Reverse Order' checkbox. The main area displays a table of system messages.

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 09:38:15 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

At the bottom of the interface, there is a status bar showing: 2021-08-12 00:00:01 - 2021-08-12 23:59:59, 0 Exec / 0 Queued, V7.1.7893.37344, and Copyright © WM Systems LLC 2021.

## 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/>

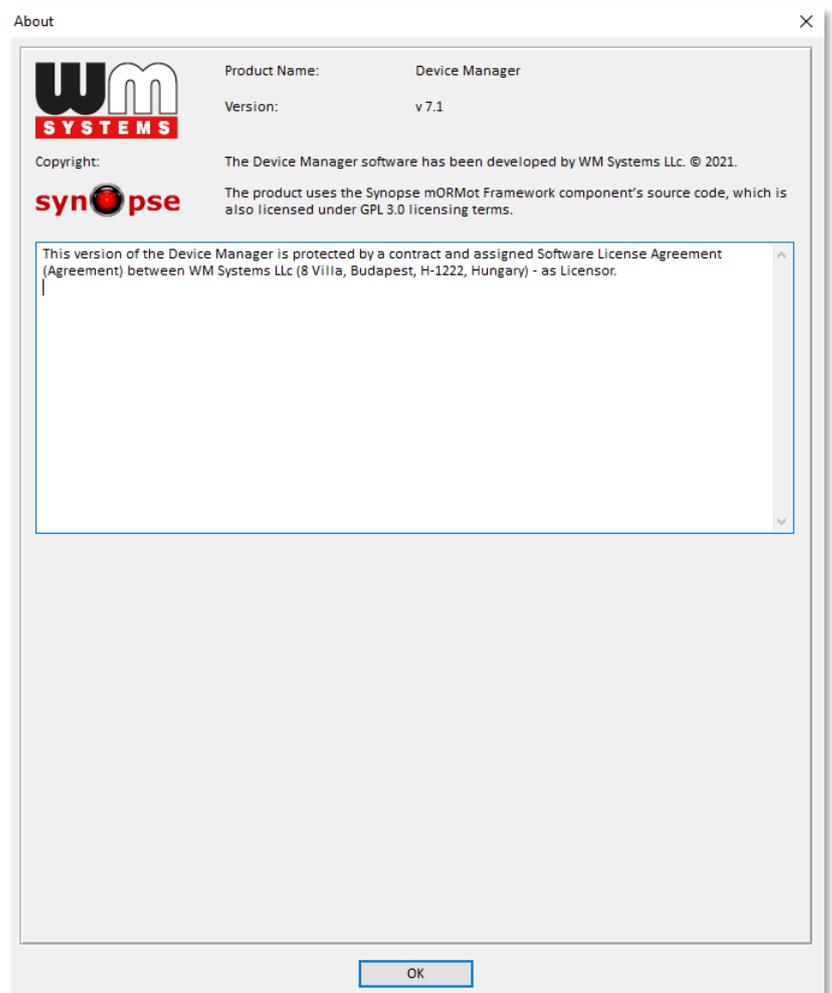
The documentation and software release for this product can be accessed via the following link:

<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

©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.