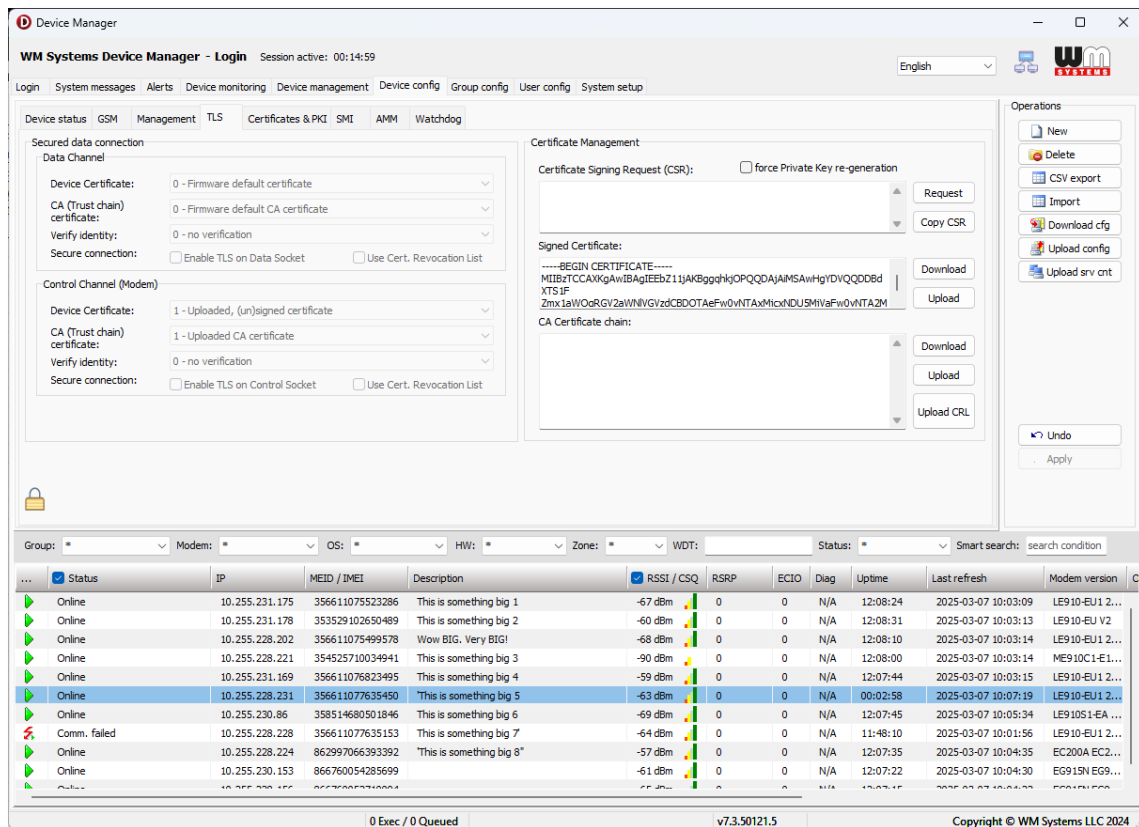


# Device Manager<sup>®</sup>

## for WM-ExS Smart Metering Modems

# User Manual

## v2.5



07-03-2025

# 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 for WM-ExS Smart Metering Modems
<b>Document subject:</b>	Device Manager <sup>®</sup>
<b>Author:</b>	WM Systems LLC
<b>Document version No.:</b>	REV 2.5
<b>Number of pages:</b>	46
<b>Device manager version:</b>	v7.3 50121.5
<b>Document status:</b>	Final
<b>Last modified:</b>	07.03.2025
<b>Approval date:</b>	07.03.2025

# Table of contents

<a href="#">Chapter 1. Introduction</a>	4
<a href="#">Chapter 2. Setup and Configuration</a>	6
<a href="#">2.1 Prerequisites</a>	6
<a href="#">2.2 System elements</a>	6
<a href="#">2.3 Installation</a>	7
<a href="#">2.4 TLS protocol communication</a>	10
<a href="#">Chapter 3. System configuration</a>	11
<a href="#">3.1 System setup</a>	11
<a href="#">3.2 User settings</a>	155
<a href="#">3.3 AD User settings</a>	187
<a href="#">Chapter 4. Device settings</a>	20
<a href="#">4.1 Device group configuration</a>	20
<a href="#">4.2 Device config overview</a>	21
<a href="#">4.3 Add new device</a>	244
<a href="#">4.4 General settings</a>	266
<a href="#">Chapter 5. Device Management</a>	37
<a href="#">5.1 Firmware importing into the system</a>	38
<a href="#">5.2 Firmware upgrade</a>	39
<a href="#">Chapter 6. Device monitoring</a>	41
<a href="#">Chapter 7. Alerts</a>	43
<a href="#">Chapter 8. System messages</a>	44
<a href="#">Chapter 9. Support</a>	45
<a href="#">9.1 Technical Support</a>	45
<a href="#">10. Legal notice</a>	46

# 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 2 and M2M Router PRO4 product families) and smart metering modems (WM-Ex families, and WM-i data loggers).

In this part we will care about only the WM-ExS metering modems.

Our NMT (Network Management Tool) is a remote device management platform which provides continuous monitoring of devices, analytic capabilities, mass firmware updates, reconfiguration.

The software allows you to check the service KPIs of the devices (QoS, life signals), intervene and control the operation, running maintenance tasks on your devices.

It's a cost-effective way of continuous, online monitoring of your connected modems in remote locations.

By receiving info on the device's availability, the monitoring of life signals, and 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 allows installing or replacing 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 smart metering modem 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 can be managed by a Device Manager.

Here we describe the software usage with our smart metering modems such as:

- WM-E1S (for Honeywell/Elster AS meters)
- WM-E1SI (for Itron ACE and SL meters)
- WM-E1SL (for Landis+Gyr E350/E450/E550 meters)
- WM-E1S ISKRA (for Iskra MT830, MT831 meters)
- WM-E1S SAPHIR
- WM-E2S (for Itron ACE and SL meters)
- WM-E2SL (for Landis+Gyr meters E350/E450/E650 meters)
- WM-E2S PME-PMI
- WM-E3S / AM122 / AM322 (for Honeywell AS meters)
- E57C WM LTE (for Landys+Gyr E570 meters)
- WM-E8S (for universal usage)
- Industrial Universal Modem (for universal usage)

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

#### Hardware environment:

- Physical or virtual environment supported
- 4 Core CPU
- 8GB RAM
- 1Gbit LAN connection
- 500MB free disk space

#### Software:

- Windows 10 or Windows 11, 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 controlling the devices.

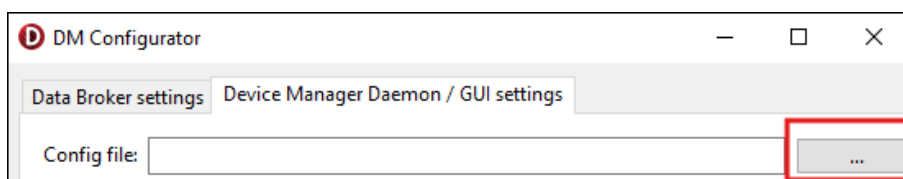
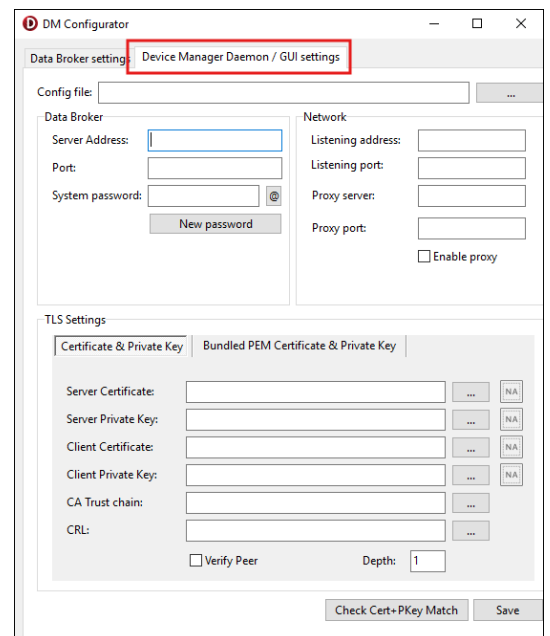
## Device Manager UI

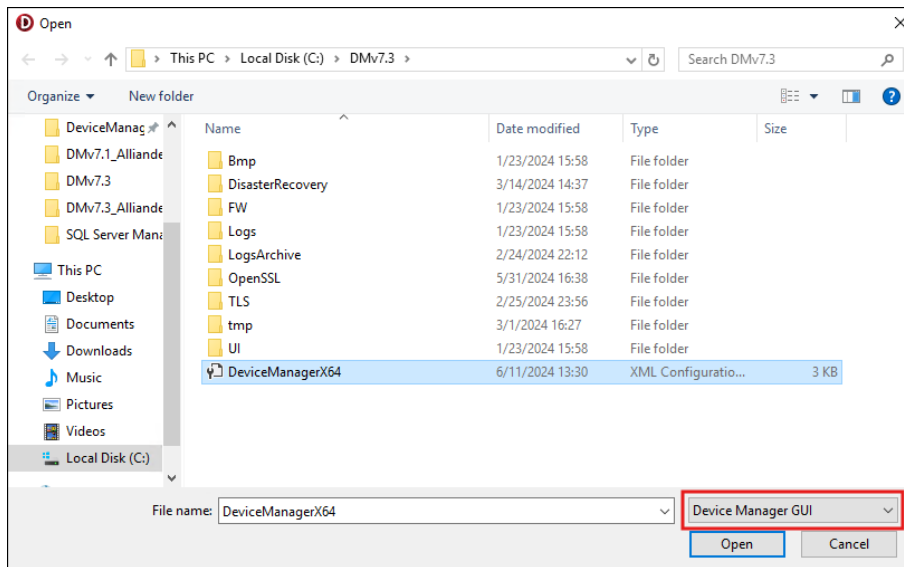
This is the device management user interface-, and business logic. It communicates with the Data Broker via a REST API, and with the modem devices through WM Systems' proprietary device management protocol.

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' partition. eg. **C:\DMv7.3**
2. Unzip the Device Manager compressed software package into the folder.
3. Execute the **DMConfigurator.exe** file. The DM will be starting and the following window appears.
4. Select the **Device Manager Daemon / GUI Settings** tab.
5. Browse the **DeviceManagerX64.config** template file from the program folder and press the right **Open** button.





- Set the parameters of the **Data Broker** and also set the password for the **Device Manager Daemon**.

The screenshot shows the 'Data Broker' configuration window. It has three input fields: 'Server Address' with the value '192.168.30.202', 'Port' with the value '888', and 'System password' with the value 'tDRqhNCKJLTg7pRQ'. There is a small icon to the right of the password field.

- Set the external target IP address (**Listening address**) of the devices and the communication port (**Listening Port**).

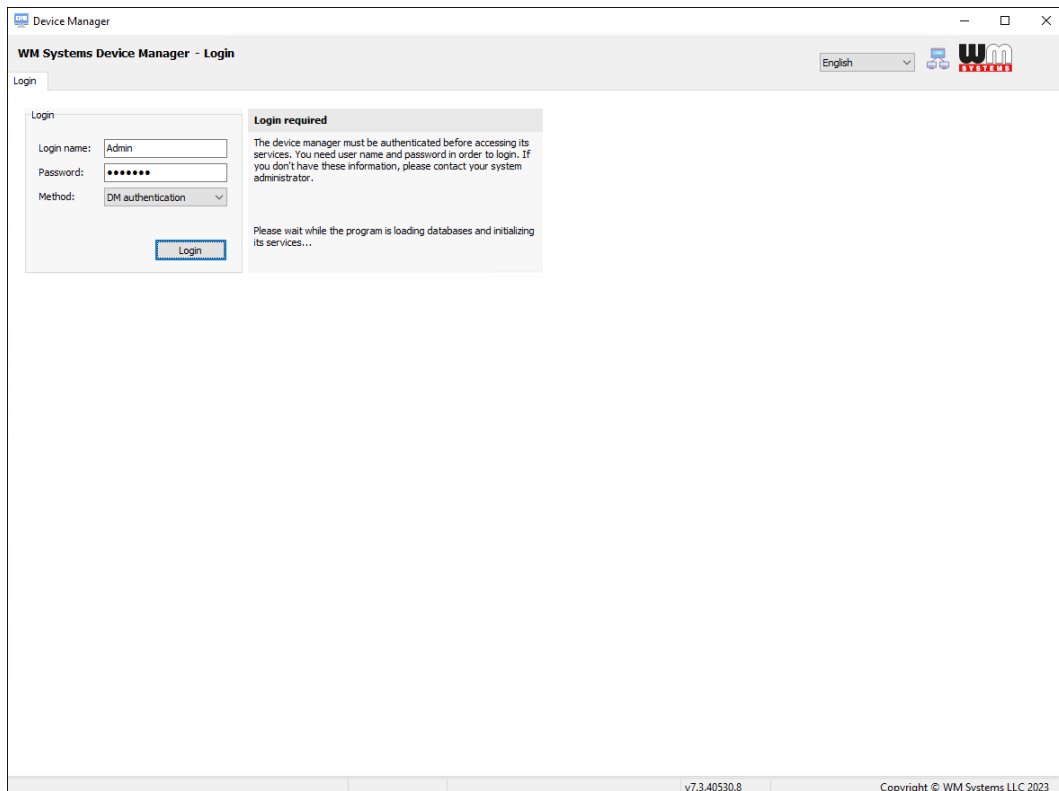
The screenshot shows the 'Network' configuration window. It has two input fields: 'Listening address' with the value '10.202.172.109' and 'Listening port' with the value '57610'.

- Locate and set all certificate files (with \*.pem file extension) from the directory.

The screenshot shows the 'TLS Settings' window. It has two tabs: 'Certificate & Private Key' (selected) and 'Bundled PEM Certificate & Private Key'. There are six input fields for certificates and keys, each with a browse button ('...') and a lock icon. The fields are: 'Server Certificate', 'Server Private Key', 'Client Certificate', 'Client Private Key', 'CA Trust chain', and 'CRL'. The 'Verify Peer' checkbox is unchecked, and the 'Depth' field is set to '0'.

After saving the modifications of the config file, please execute the file **DeviceManagerX64.exe** again.

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



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

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

*(The login data are case-sensitive!)*

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

Normally the authentication method is a local DM authentication, but you can also choose between local and LDAP authentication (if it is already set on the AD server, and previously set in the DM).

### **Important!**

*Consequently, only those services, views, and data are visible to the user who is currently logged in and has access/permission to. These can be limited by configuring the user rights.*

*Note, that in case of using Active Directory, the current rights and access levels of those Active Directory 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 TLS solution can use a mutual authentication method as an option to identify the two parties involved in a communication.

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

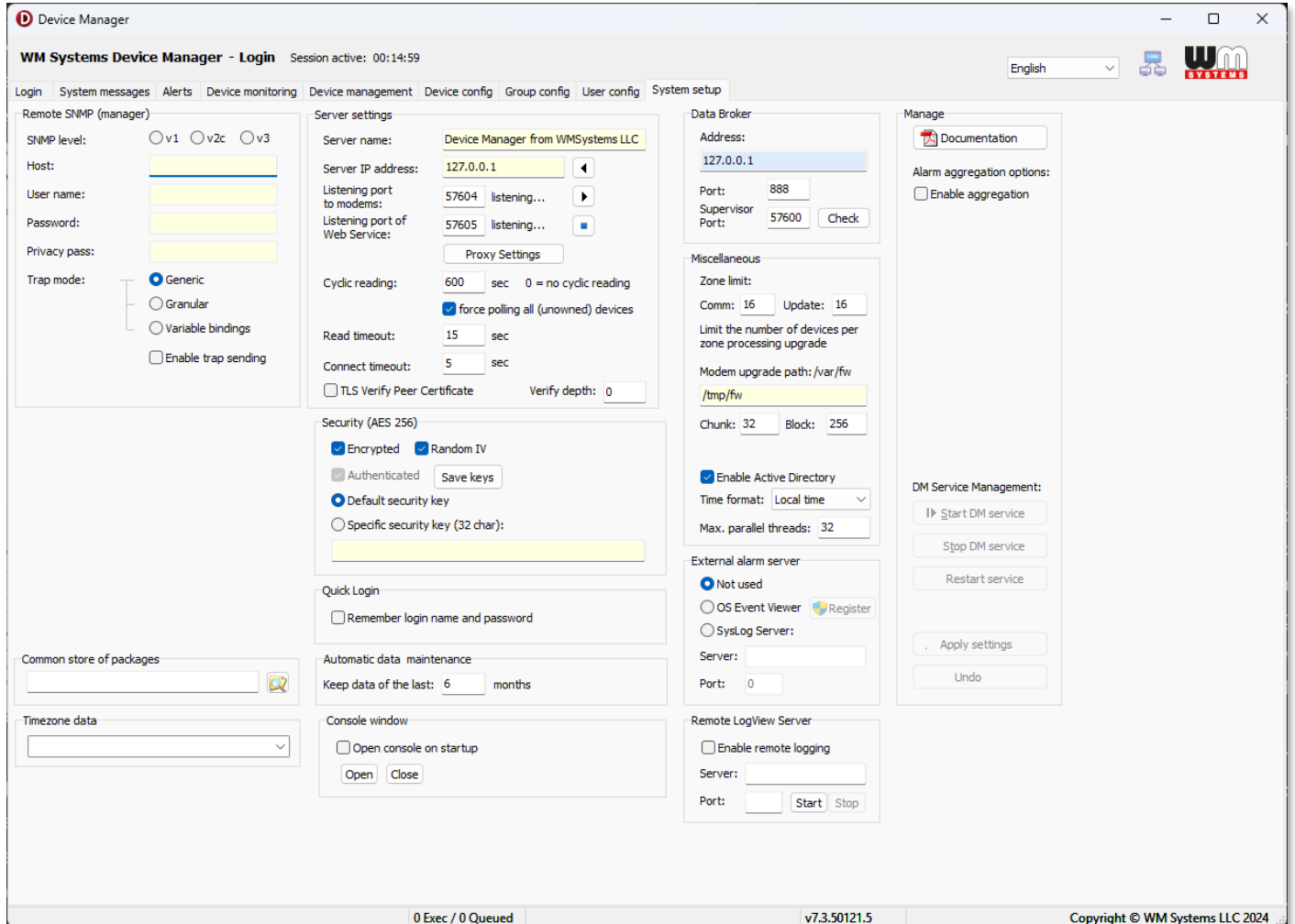
Only a factory default setting is implemented on the modem, so the device does not check whether the certificate presented of a connected party is signed by a trusted party. Any TLS connection to the modem can be established with any certificate, even if its self-signed.

# Chapter 3. System configuration

## 3.1 System setup

After login to the system, first choose **System setup** tab. Each part of the screen listed here with the relevant fields.

The Device Manager application has some default parameters of operation, but it must be checked before using the DM. If it is necessary settings should be modified.



### **Remote SNMP (manager)**

The Device Manager uses an 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
- 1.3.6.1.6.3.1.1.5.5 – Authentication failure (unauthorized login attempt or wrong password)

The SNMP trap contain: 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 also.

**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 and the privacy pass specified here. Of course, this setting must be the same as it is at the SNMP Manager side.

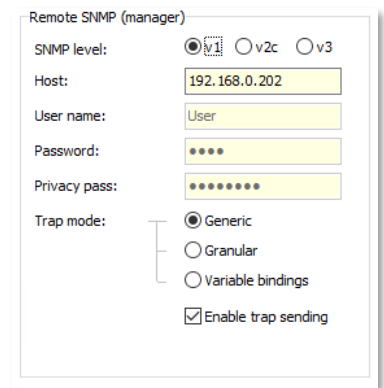
**Trap mode:** depending on the manager's capabilities, the program can send traps with the so-called variable bindings providing detailed information about the event and the relevant node.

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 a 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 is 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".

In case of failure, changed settings can be revoked by the **Undo** button.

When you want to save the settings, press the **Apply settings** button.



Remote SNMP (manager)

SNMP level:  v1  v2c  v3

Host:


User name:


Password:

Privacy pass:

Trap mode:  Generic  Granular  Variable bindings

Enable trap sending

 Apply settings

 Undo

## 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 can send their data.

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

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

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

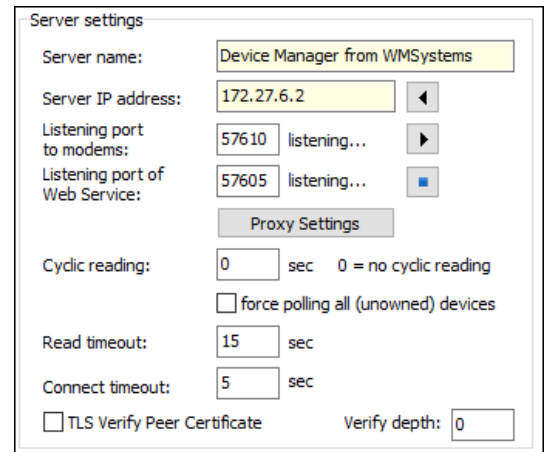
**Cyclic reading (sec):** you can define a periodic reading of the devices. The Device Manager can cyclically poll devices when configured to do so. We don't offer to configure smaller periodic than 600 seconds.

- The zero value equals no polling.

- The default value is "0" because the server does not initiate any communication, the devices do it.

**Force polling all (unowned) devices:** In normal case this feature is disabled. If you want to request the DM to check device vital signals with the Data Broker, then allow this option and the DM will be getting last known vital information of modems, current configuration and encryption files of the listed devices within minutes.

**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.



The screenshot shows a 'Server settings' window with the following fields and options:

- Server name: Device Manager from WMSystems
- Server IP address: 172.27.6.2
- Listening port to modems: 57610 listening...
- Listening port of Web Service: 57605 listening...
- Proxy Settings button
- Cyclic reading: 0 sec 0 = no cyclic reading
- force polling all (unowned) devices
- Read timeout: 15 sec
- Connect timeout: 5 sec
- TLS Verify Peer Certificate
- Verify depth: 0

**Connect timeout (sec):** here you can define the connection timeout for devices.

## Security (AES 256)

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

**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):** you can specify a special security key here.

## Quick Login

**Remember login name and password:** to save your login credentials. There is no need to type username and password at the login screen.

## Automatic data maintenance

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

## Data broker

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

**Port:** port number of the Data Broker.

**Supervisor port:** supervision port number. Not used in this application version.

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

The screenshot shows two configuration panels. The top panel, titled "Data Broker", includes an "Address" field with the value "192.168.0.56", a "Port" field with "888", and a "Supervisor Port" field with "888" and a "Check" button. The bottom panel, titled "Miscellaneous", includes a "Zone limit" section with "Comm" and "Update" fields both set to "0", a note "Limit the number of devices per zone processing upgrade", a "Modem upgrade path" field with "/var/fw", "Chunk" and "Block" fields set to "32" and "512" respectively, a checked "Enable Active Directory" checkbox, a "Time format" dropdown menu set to "Local time", and a "Max. parallel threads" field set to "64".

## Miscellaneous

**Zone limit:** Restricts the number of simultaneous uploads to modems in the same zone. 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.

The screenshot shows three configuration panels. The top panel, titled "Security (AES 256)", has checkboxes for "Encrypted", "Random IV", and "Authenticated", all of which are checked. There is a "Save keys" button, a radio button selected for "Default security key", and a text input field for "Specific security key (32 char)". The middle panel, titled "Quick Login", has a checked checkbox for "Remember login name and password". The bottom panel, titled "Automatic data maintenance", has a "Keep data of the last:" field set to "6" months.

- **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 temporarily on the device. The default directory path is: **/tmp/fw**

**Enable Active Directory:** you can enable or disable the Active Directory service for the Device Manager here.

**Time format:** can be chosen from *Local time* or *UTC*.

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

### External alarm server

The client can send device alarm messages to the event log from the operating system or the external syslog server. Here you can configure these by the following parameter options:

- **Not used**
- **OS Event Viewer**
- **SysLog Server:** this feature currently not works
  - **Server:** Syslog server IP address
  - **Port:** Syslog server port number

### Remote LogView Server

**Enable remote logging** – you can enable or disable the feature (for debugging only)

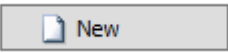
**Server:** IP of the LogView server

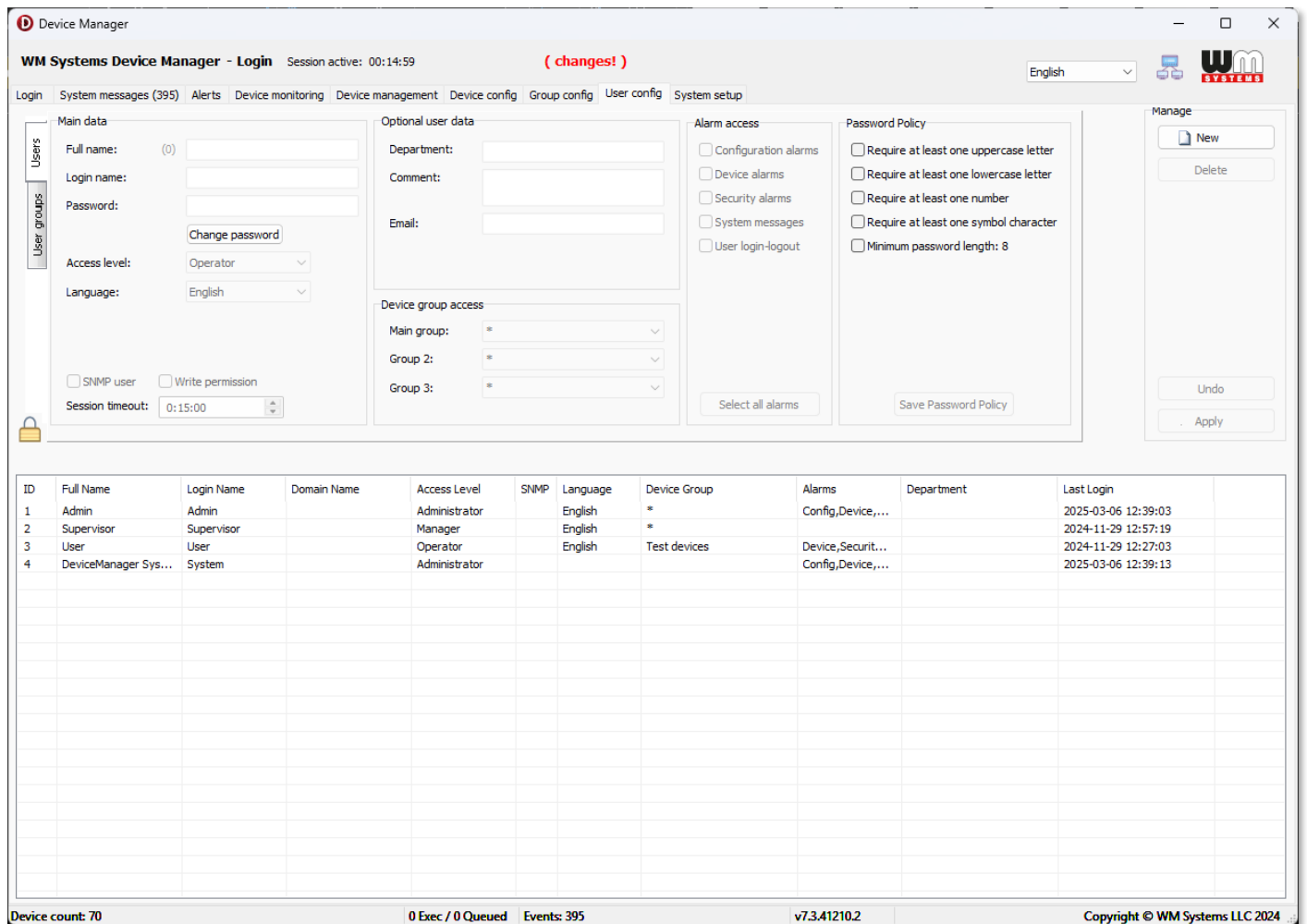
**Port:** port number of the LogView logging server

## 3.2 User settings

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

In this screen, you can see the existing users and groups. By selecting one, you can modify its data.


Or you can create a new by pressing the  button at the right of the screen.



The screenshot shows the 'WM Systems Device Manager - Login' window. The top navigation bar includes 'Login', 'System messages (395)', 'Alerts', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. The 'User config' tab is active, showing fields for 'Main data' (Full name, Login name, Password, Access level, Language), 'Optional user data' (Department, Comment, Email), 'Alarm access' (Configuration alarms, Device alarms, Security alarms, System messages, User login-logout), and '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). A 'Change password' button is visible. The 'Manage' section on the right has 'New', 'Delete', 'Undo', and 'Apply' buttons. Below the form is a table with columns: ID, Full Name, Login Name, Domain Name, Access Level, SNMP, Language, Device Group, Alarms, Department, and Last Login.

ID	Full Name	Login Name	Domain Name	Access Level	SNMP	Language	Device Group	Alarms	Department	Last Login
1	Admin	Admin		Administrator		English	*	Config,Device,...		2025-03-06 12:39:03
2	Supervisor	Supervisor		Manager		English	*			2024-11-29 12:57:19
3	User	User		Operator		English	Test devices	Device,Securit...		2024-11-29 12:27:03
4	DeviceManager Sys...	System		Administrator				Config,Device,...		2025-03-06 12:39:13

Device count: 70      0 Exec / 0 Queued      Events: 395      v7.3.41210.2      Copyright © WM Systems LLC 2024

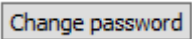
If you want to edit existing parameters, press the  button. This solution prevents accidental modification.

## Main data

**Full name:** User name

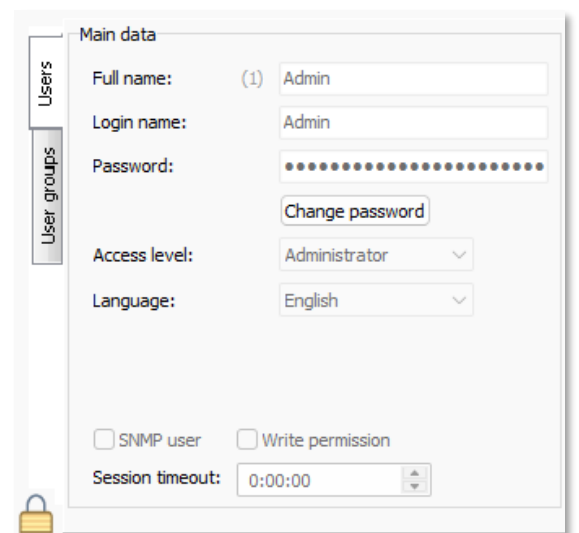
**Login name:** Name for login access

**Password:** Authenticating for login name

If you want to change the password, select the user and press the  button.

Here you can enable the **Active Directory authentication** also.

**Access level:**



This close-up shows the 'Main data' section of the user configuration form. It includes fields for 'Full name' (Admin), 'Login name' (Admin), and 'Password' (masked with dots). A 'Change password' button is present. Below are 'Access level' (Administrator) and 'Language' (English) dropdown menus. At the bottom, there are checkboxes for 'SNMP user' and 'Write permission', and a 'Session timeout' dropdown set to 0:00:00.

- **Disabled** – with this access level, you can disable the selected user. The selected user will be not able to access the DM.
- **Administrator** – full access to all services including user config, 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:

Comment:

Email:

### Device group access

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

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

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

Device group access

Main group:

Group 2:

Group 3:

### 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

## 3.3 AD User settings

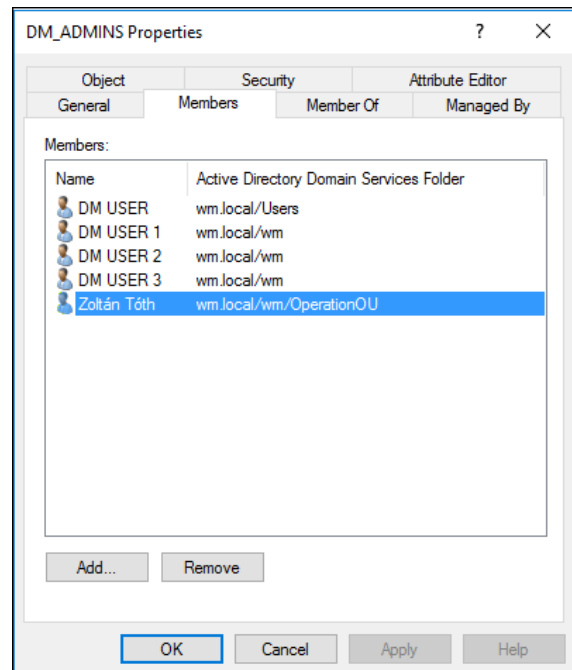
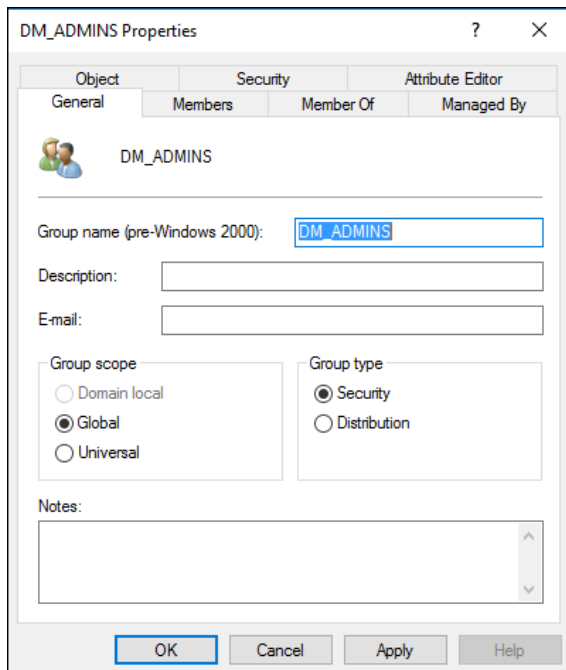
If you want to use LDAP authentication, you can set the parameters in the **User groups** tab.

The screenshot shows the configuration interface for a user group named 'DM\_ADMINS'. The interface is divided into several sections:

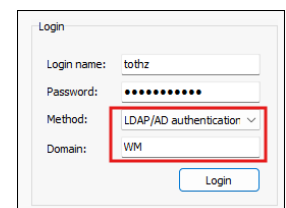
- Main data:** Group Name (DM\_ADMINS), Domain name (WM), Access level (Administrator), Language (English), and Session timeout (0:00:00).
- Optional user data:** Department and Comment fields.
- Device group access:** Main group, Group 2, and Group 3, all set to '\*'. There is a 'Select all alarms' button.
- Alarm access:** Configuration alarms, Device alarms, Security alarms, System messages, and User login-logout are all checked.
- 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, and Minimum password length: 8 are all unchecked.
- Manage:** New, Delete, Undo, and Apply buttons.

ID	Group Name	Login Name	Domain Name	Access Level	SNMP	Language	Device Group	Alarms	Department	Last Login
5	DM_ADMINS	DM_ADMINS	WM	Administrator			*	Config,Device,...		2024-02-24 07:54:18

1. Create an Active Directory group in Device Manager. Press **New** button, and set the **Group Name**, **Domain name**, **Access level** and select the **AD auth.** option.
2. Set the **Alarm access** for this user group.
3. When all settings are done, press the **Apply** button.
4. Create the same AD group in the Active Directory, and assign the related users to it.



5. On the DM login screen, change the **Method** to **LDAP** and set the **Domain**.



6. Enter the **domain user name** and **password** and press the **Login** button. If all settings correct, then you can login into the DM with the AD user.

# Chapter 4. Device settings


## 4.1 Device group configuration

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

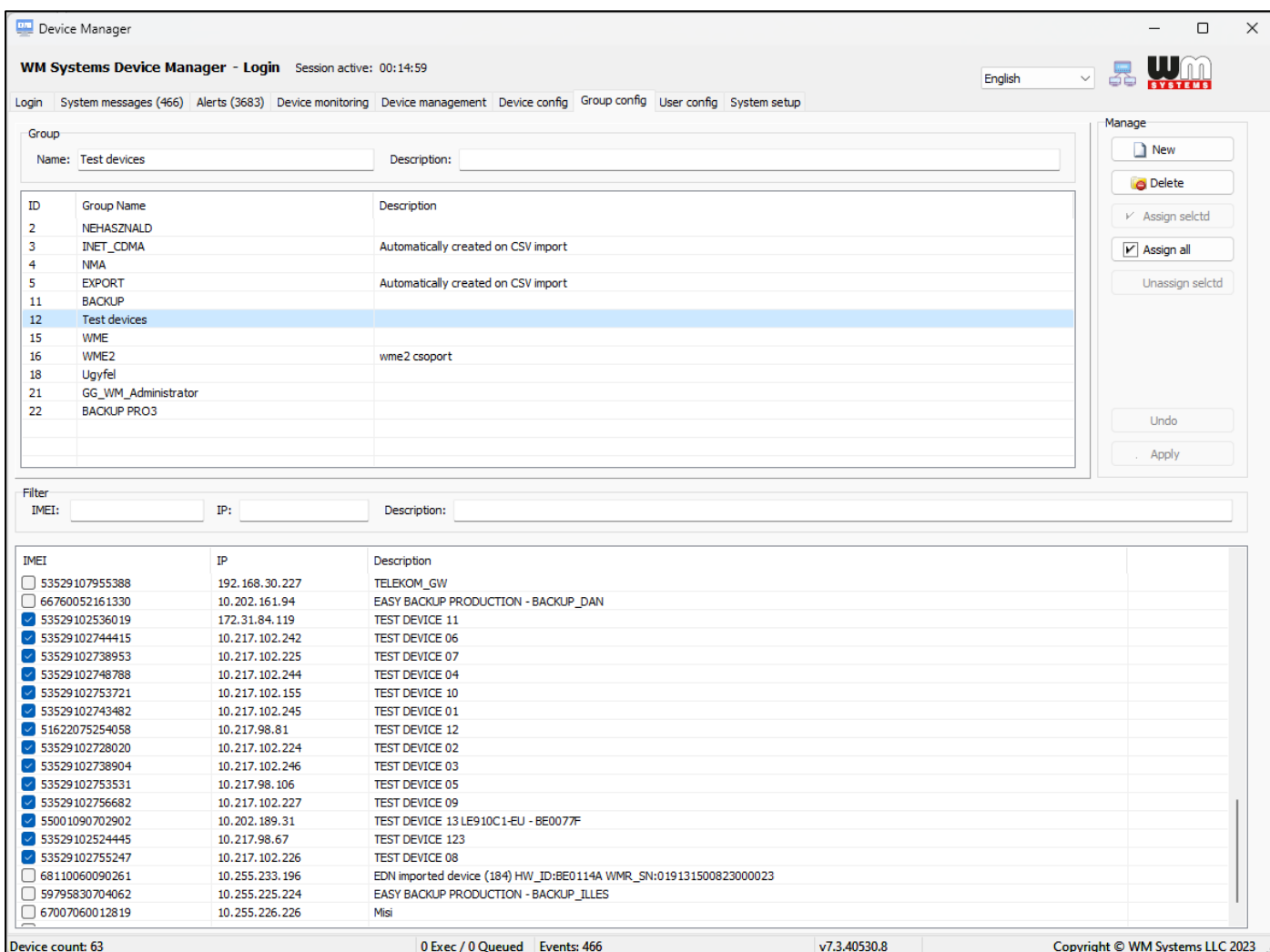
Choose a **Group name** and see the marked devices below.

If you want to add more devices for an existing group, just check 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 to create a new group and fill in the **Name** field (mandatory) and the **description** (optional).

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



Device Manager

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

English

Login System messages (466) Alerts (3683) Device monitoring Device management Device config **Group config** User config System setup

Group

Name: Test devices Description:

ID	Group Name	Description
2	NEHASZNALD	
3	INET_CDMA	Automatically created on CSV import
4	NMA	
5	EXPORT	Automatically created on CSV import
11	BACKUP	
12	Test devices	
15	WME	
16	WME2	wme2 csport
18	Ugyfel	
21	GG_WM_Administrator	
22	BACKUP PRO3	

Manage

New

Delete

Assign selectd

Assign all

Unassign selectd

Undo

Apply

Filter

IMEI: IP: Description:

IMEI	IP	Description
<input type="checkbox"/> 53529107955388	192.168.30.227	TELEKOM_GW
<input type="checkbox"/> 66760052161330	10.202.161.94	EASY BACKUP PRODUCTION - BACKUP_DAN
<input checked="" type="checkbox"/> 53529102536019	172.31.84.119	TEST DEVICE 11
<input checked="" type="checkbox"/> 53529102744415	10.217.102.242	TEST DEVICE 06
<input checked="" type="checkbox"/> 53529102738953	10.217.102.225	TEST DEVICE 07
<input checked="" type="checkbox"/> 53529102748788	10.217.102.244	TEST DEVICE 04
<input checked="" type="checkbox"/> 53529102753721	10.217.102.155	TEST DEVICE 10
<input checked="" type="checkbox"/> 53529102743482	10.217.102.245	TEST DEVICE 01
<input checked="" type="checkbox"/> 51622075254058	10.217.98.81	TEST DEVICE 12
<input checked="" type="checkbox"/> 53529102728020	10.217.102.224	TEST DEVICE 02
<input checked="" type="checkbox"/> 53529102738904	10.217.102.246	TEST DEVICE 03
<input checked="" type="checkbox"/> 53529102753531	10.217.98.106	TEST DEVICE 05
<input checked="" type="checkbox"/> 53529102756682	10.217.102.227	TEST DEVICE 09
<input checked="" type="checkbox"/> 55001090702902	10.202.189.31	TEST DEVICE 13 LE910C 1-EU - BE007F
<input checked="" type="checkbox"/> 53529102524445	10.217.98.67	TEST DEVICE 123
<input checked="" type="checkbox"/> 53529102755247	10.217.102.226	TEST DEVICE 08
<input type="checkbox"/> 68110060090261	10.255.233.196	EDN imported device (184) HW_ID:BE01144 WMR_SN:019131500823000023
<input type="checkbox"/> 59795830704062	10.255.225.224	EASY BACKUP PRODUCTION - BACKUP_ILLES
<input type="checkbox"/> 67007060012819	10.255.226.226	Misi

Device count: 63 0 Exec / 0 Queued Events: 466 v7.3.40530.8 Copyright © WM Systems LLC 2023

After the group creation, you can select even more devices for a group. You can see the managed devices of Device Manager at the bottom side of the screen. The selected

devices will be automatically assigned to the designated group. Creating groups makes it easier to use and manage devices with DM.

## 4.2 Device config overview

At the **Device config** tab, you can check the current settings of a device. This screen is available only for these access levels: *Administrators, Managers*.

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 → currently not used here
- WDT → currently not used here
- Status → device status filtering
- Smart search → the filled characters will be searched in entire the database

The screenshot displays the 'Device Manager' interface. At the top, it shows 'WM Systems Device Manager - Login' with a session active for 00:15:00. The navigation menu includes 'Login', 'System messages', 'Alerts', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. The 'Device config' tab is active, showing 'Device information' for a selected device. The information includes RSSI (-68dBm), Generation (4G), Access Technology (E-UTRAN), Last refresh (2025-03-07 09:23:47), Device Enabled (checked), Description (Wow BIG. Very BIG!), Serial No. of the Modem Chip, Operating System Revision ID (WM-E2S E2S\_EFL\_BL B2.60), Firmware version (V2.5.60), GSM module and firmware version (LE910-EU1 20.00.416), Network Operator (21601), IMEI (356611075499578), ICC (8936200003150893591), IP address (10.255.228.202), and Management port (9001). A 'No automatic IP update' checkbox is also present. On the right, there are 'Operations' buttons: New, Delete, CSV export, Import, Download cfg, Upload config, Upload srv cnt, Undo, and Apply. Below the configuration details is a filter bar with dropdowns for Group, Modem, OS, HW, Zone, WDT, Status, and a Smart search field. A table below shows a list of devices with columns for Status, IP, MEID / IMEI, Description, RSSI / CSQ, RSRP, ECIO, Diag, Uptime, Last refresh, and Modem version. The third device is selected, showing a 33% battery level. At the bottom, it indicates 'Device count: 11', '0 Exec / 0 Queued', version 'v7.3.50121.5', and 'Copyright © WM Systems LLC 2024'.

...	Status	IP	MEID / IMEI	Description	RSSI / CSQ	RSRP	ECIO	Diag	Uptime	Last refresh	Modem version
▶	Online	10.255.231.175	356611075523286	This is something big 1	-61 dBm	0	0	N/A	12:36:16	2025-03-07 10:29:46	LE910-EU1 2...
▶	Online	10.255.231.178	353529102650489	This is something big 2	-63 dBm	0	0	N/A	12:36:36	2025-03-07 10:30:03	LE910-EU1 V2
▶	33%	10.255.228.202	356611075499578	Wow BIG. Very BIG!	-68 dBm	0	0	N/A	12:29:58	2025-03-07 10:23:47	LE910-EU1 2...
▶	Online	10.255.228.221	354525710034941	This is something big 3	-90 dBm	0	0	N/A	12:29:47	2025-03-07 10:23:43	ME910C1-E1...
▶	Online	10.255.231.169	356611076823495	This is something big 4	-65 dBm	0	0	N/A	12:29:45	2025-03-07 10:24:01	LE910-EU1 2...
▶	Online	10.255.228.231	356611077635450	This is something big 5	-63 dBm	0	0	N/A	00:23:00	2025-03-07 10:27:56	LE910-EU1 2...
▶	Online	10.255.230.86	358514680501846	This is something big 6	-67 dBm	0	0	N/A	12:32:21	2025-03-07 10:26:40	LE910S1-EA...
▶	Online	10.255.228.228	356611077635153	This is something big 7	-63 dBm	0	0	N/A	00:17:43	2025-03-07 10:22:24	LE910-EU1 2...
▶	Online	10.255.228.224	862997066393392	This is something big 8"	-61 dBm	0	0	N/A	12:30:46	2025-03-07 10:25:11	EC200A EC2...
▶	Online	10.255.230.153	866760054285699		-61 dBm	0	0	N/A	12:30:25	2025-03-07 10:24:58	EG915N EG9...

On this screen, you can see all devices listed with their current known **Status** – such as *Online, Offline, Disabled, Never Plugged in, Connecting, etc.*

If you see percentage there, that means the device information is currently under updating.

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

If you want to refresh the vital signals of a device manually, click on the device from the listed ones and push right click on and choose **Read Device Status** option there. Soon, the last known information of the device will be requested and soon refreshed on the screen. This can take up half a minute for a device.

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

*\* Note, that these are not valid status values for smart metering modems.*

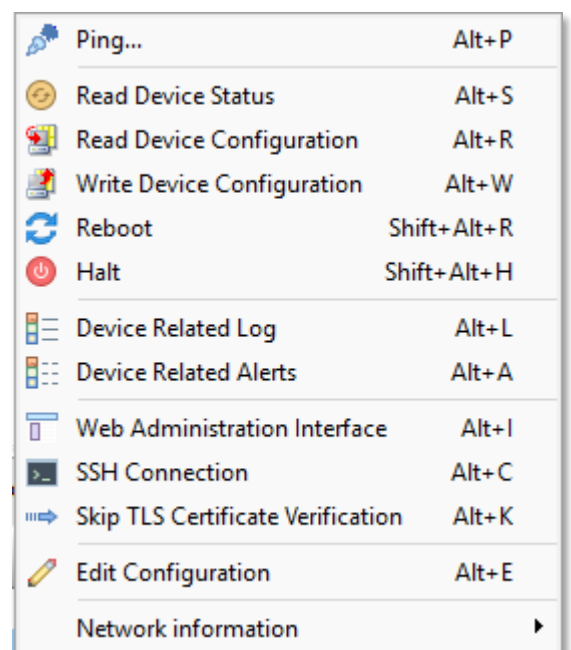
The **Modem version**, **OS version** (date of the build), **HW version** (PCB identifier), **FWSTM32** (Microcontroller firmware version) are also available here.

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

**Ping:** you can ping the selected device from the GUI.

**Read Device Status:** the GUI attempts to connect directly to the device to read the status of the modem.

**Read Device Configuration:** the GUI attempts to connect directly to the device to read the current configuration of the modem.



**Write Device Configuration:** the GUI attempts to connect directly to the device to write the device configuration from the DM. Before you want to modify the configuration of the WM-ExS modem, try to read out its settings.

Modify the configuration, then write the new configuration to the device.

Then read out the configuration again.

The configuration will be updated in the database.

**Reboot:** with this, you can reboot the device (reboot the OS only).

**Halt:** with this, you can reboot the modem with a full power cycle.

**Device Related log:** here the screen will be redirected to the **System messages** with filtering the selected device events.

**Device Related Alerts:** here the screen will be redirected to the **Alerts** with filtering the selected device alerts.

**Web Administration Interface:** it will open the device web admin interface of the selected device in your internet browser. This function depends on the modem firmware.

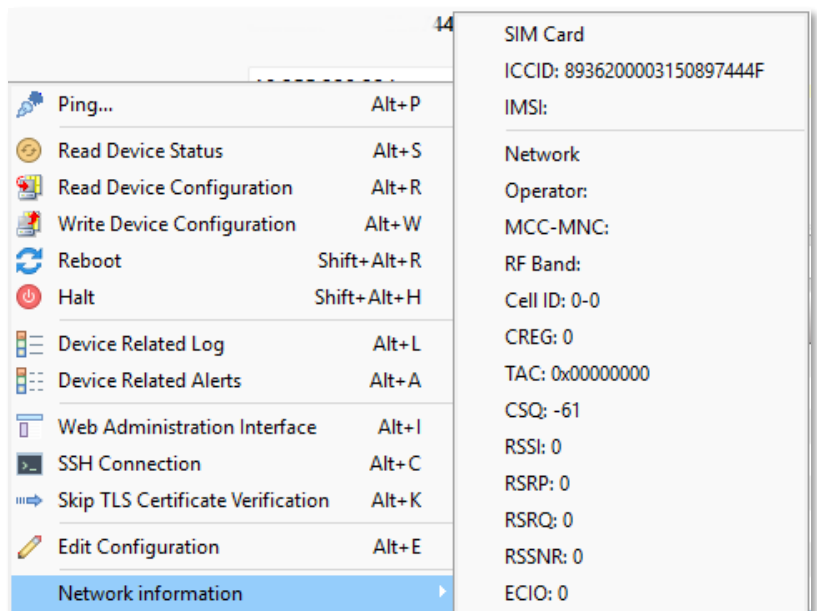
If the firmware does not contain a web server (ex.: if the modem is fully secured), then this function will not work.

**SSH Connection:** the application will open the **putty.exe** program from the DM directory and attempt to connect to the device directly with SSH protocol. Use the right **login name** and **password** for the selected device. If you try with the wrong password, then the modem will block the SSH communication for 1 minute.

**Skip TLS Certificate Verification:** the application will not checking the verification of the TLS certificate if you choose this option.

**Edit configuration:** enter to configuration editing mode.

**Network information:** here you can see additional important network information of the selected device.

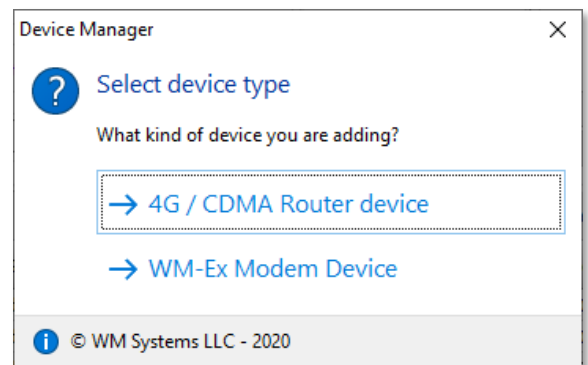


### 4.3 Add new device

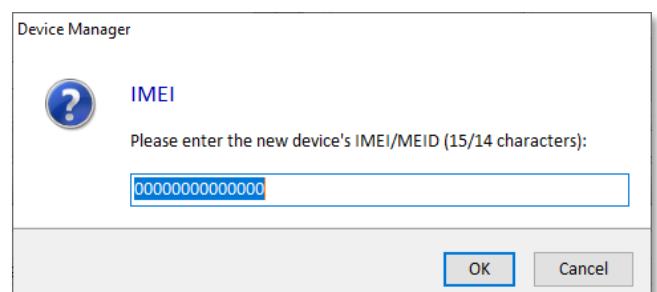
This feature is available for these access levels: *Administrators, Managers.*

Here, at **Device config** tab, you can add a new device with the  **New** button.

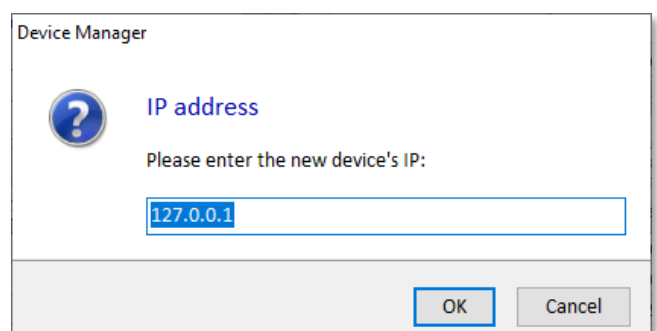
Select the device type: **WM-Ex Modem device.**



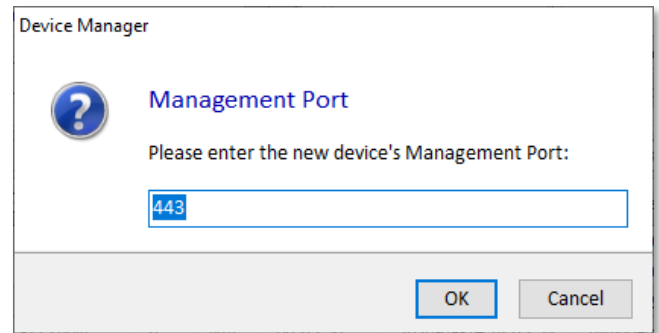
Then you have to enter the **IMEI/MEID** identifier of the cellular module of the modem.



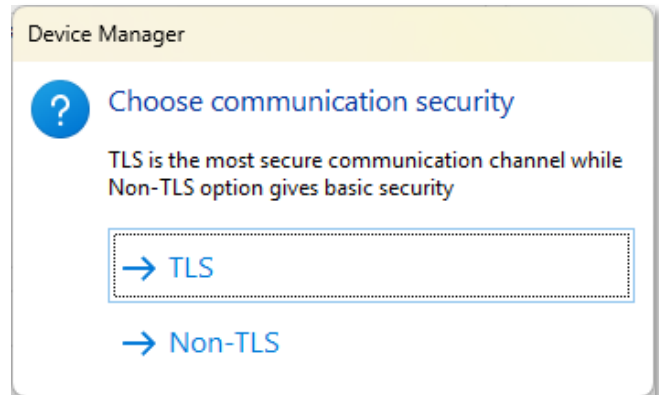
Fill the **IP address** of the device. If the IP address was not configured here, it is not a problem, because the device will communicate with the DM, and will send the current IP address and it will be stored in the database.




Fill 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.



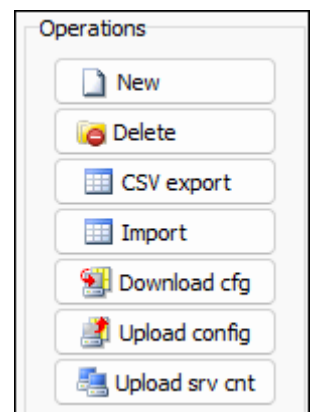
Then **Choose the communication security** level: **TLS** (encrypted by TLS protocol) or **Non-TLS** (standard transparent communication without encryption).



### IMPORTANT!

Any modification is possible only after pressing the **Apply** button. If you have to make some changes, enter to editor mode (press the  button) and make the modifications.

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



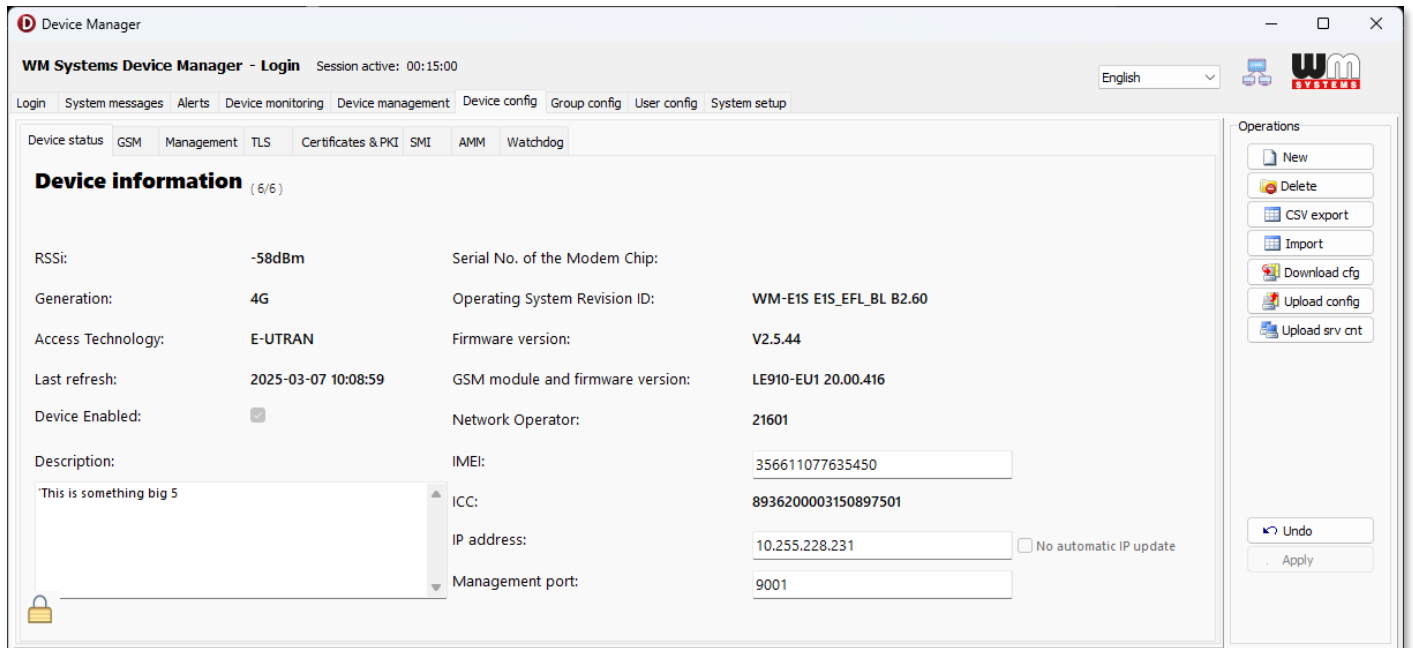
- **New:** add new devices
- **Delete:** this will delete the current / selected device(s) from the device list
- **CSV export:** export the device list with configuration data into CSV file
- **Import:** import devices with configuration into the database from CSV or XML or EDN file
- **Download cfg:** download the current configuration from the device into the database – if the device is online.
- **Upload config:** directly upload a configuration to the device if the device is online
- **Upload srv cnt:** upload the server settings (IP, port) from the current client

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

## 4.4 General settings

On the **Device Status** tab, you can get information about the device and its operation, then it will be listed here. Furthermore, you can configure some settings here.

These settings are not applied immediately! To use the modified configuration, the configured parameters must be uploaded to the device!



**RSSI** – Received cellular network signal strength indication in dBm value. A greater value means worst, while lower value means signal quality.

**Generation** – Cellular modules' technology - highest possible network technology to be accessed logically

**Access Technology** – currently used cellular technology by the modem's internet module

**Last refresh** – Date and time of the last known and listed status information of the device

**Description** – here you can fill information about the device. It is a free text content.

**Serial No. of the Modem Chip** – if available

**Operation System Revision ID** – Modem's firmware version identifier

**GSM module and firmware version** – Internet module's manufacturer identifier

**IMEI** – cellular module's unique identifier – can be changed

**ICC** – SIM card's unique identifier

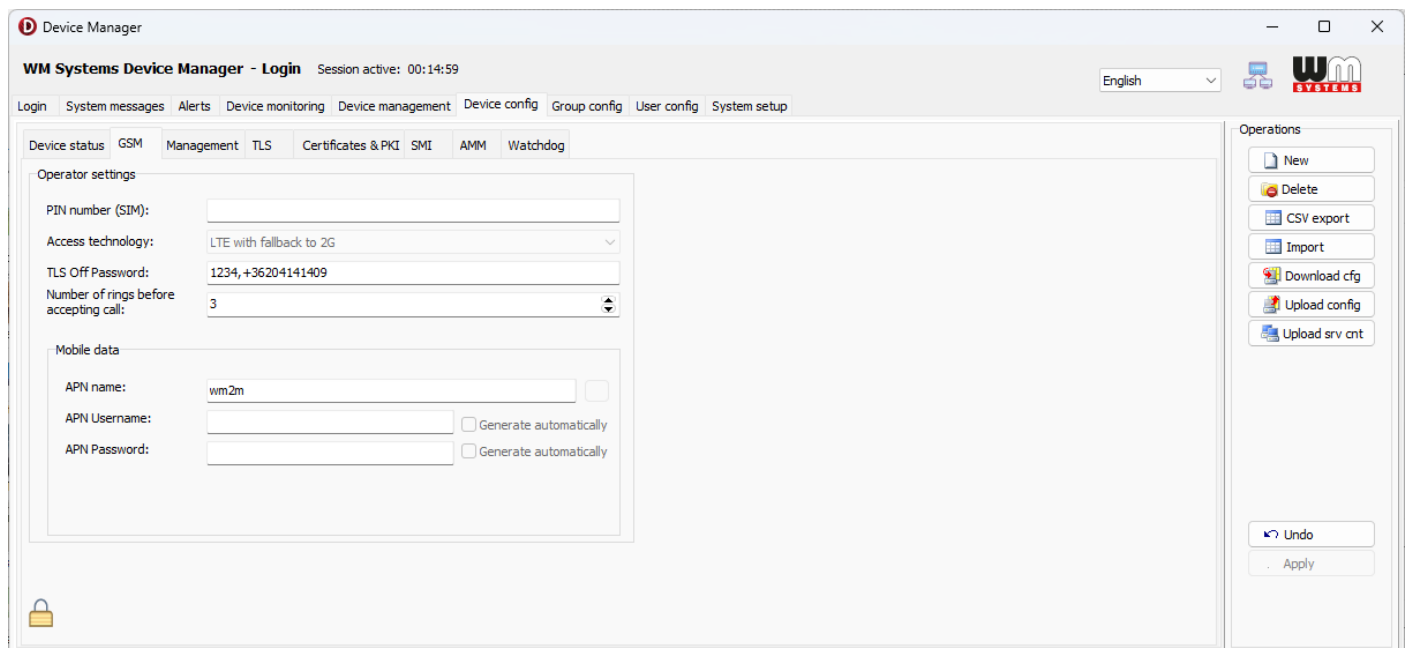
**IP address** – device IP address – can be changed

**Management Port** – device's port number to the the Device Manager communication  
– can be changed

The **GSM** (tab) part has the following fields:

**PIN number (SIM)** – if the SIM card uses a PIN code, you should enter here or leave it empty

**Access Technology** – currently used cellular technology by the modem's internet module



The screenshot shows the 'Device Manager' application window. The title bar reads 'Device Manager' and the main window title is 'WM Systems Device Manager - Login'. The session is active for 00:14:59. The interface has a top navigation bar with tabs: Login, System messages, Alerts, Device monitoring, Device management, Device config (selected), Group config, User config, and System setup. Below this, there are sub-tabs for GSM, Management, TLS, Certificates & PKI, SMI, AMM, and Watchdog. The 'GSM' tab is active, showing 'Operator settings' and 'Mobile data' sections. The 'Operator settings' section includes: 'PIN number (SIM):' (empty text field), 'Access technology:' (dropdown menu showing 'LTE with fallback to 2G'), 'TLS Off Password:' (text field with '1234,+36204141409'), and 'Number of rings before accepting call:' (spinner box set to '3'). The 'Mobile data' section includes: 'APN name:' (text field with 'wm2m'), 'APN Username:' (text field with 'Generate automatically' checkbox), and 'APN Password:' (text field with 'Generate automatically' 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. A lock icon is visible in the bottom left corner of the main content area.

**TLS Off Password** – the password for disabling the TLS encryption (if it will be requested later)

**Number of rings before accepting call** – the modem waits for the defined number of rings before accepting the data call (CSD)

## **Mobile data**

**APN Name** – here you have to add the APN zone name according to the modem SIM card (ask your Mobile Operator).

**APN username** – if the SIM requires a username, fill the field according the mobile operator hints of the SIM card.

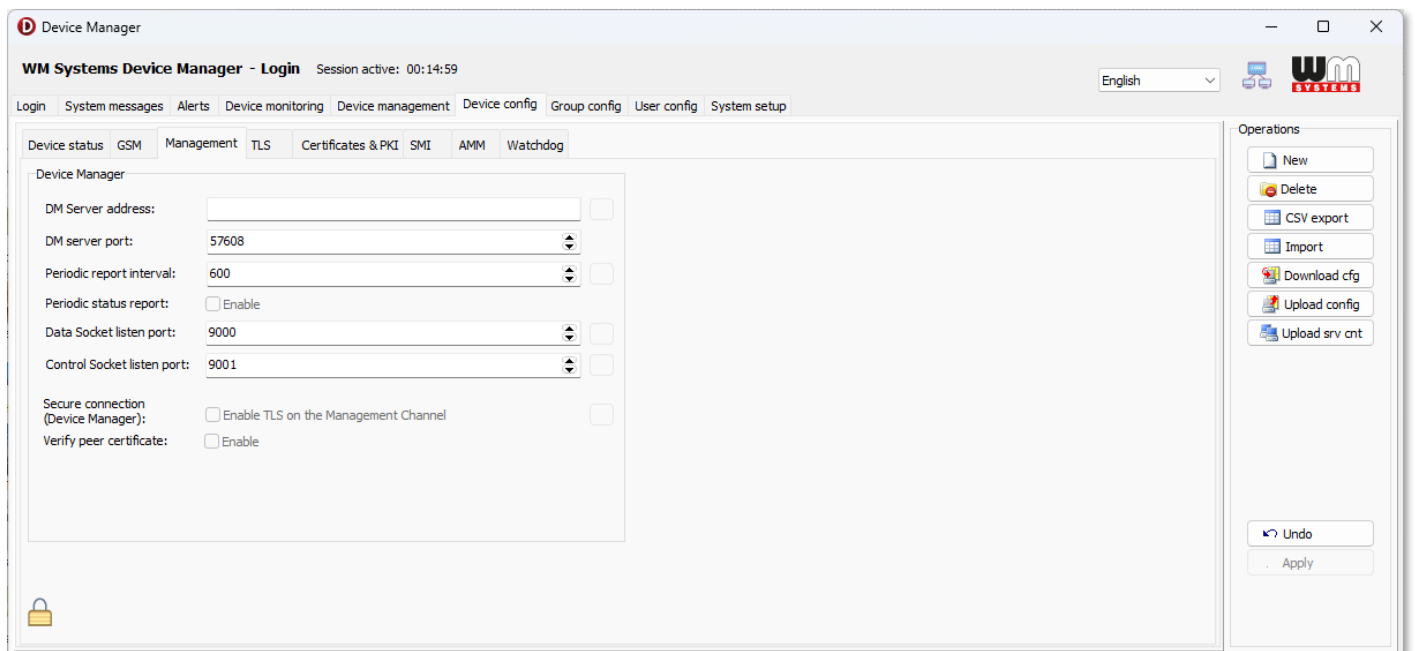
**APN Password** – Fill the field if the SIM card uses a password for the APN access.

*Important! If the SIM is not using APN Username or APN Password values, then leave these fields blank.*

The **Management** (tab) part has the following fields:

**DM server address** – it is required to build the connection.

**DM server port** – must be added for the modem↔DM connection.



**Periodic report interval** – automatic reports interval in seconds

**Periodic status report** automatic reports

**Data Socket listen port** – listener port for incoming data

**Control Socket listen port** – listener port for control data

**Secure connection (Device Manager)** – you can enable the secure TLS connection with DM here

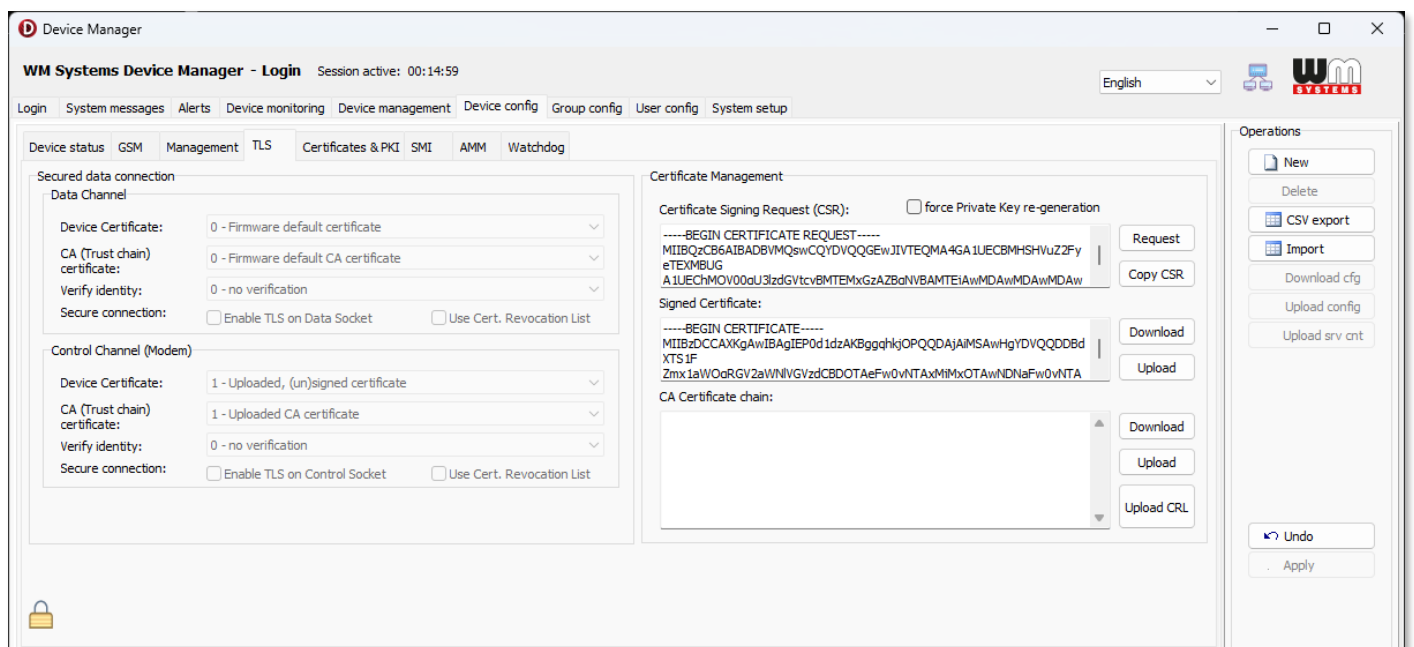
**Verify peer certificate** – you can enable the feature here

At **TLS** tab, you can configure a TLS v1.2 protocol-compatible communication for modems.

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.

After enabling the feature, device(s) will communicate with Device Manager software via TLS.

These parameters are not implemented in current firmware of modem and in DM.



The certification files can be generated by a PKI software. The CSR (Certificate Signing Request) file should be generated and the further CERT or PEM extension, CA Certification and normal Certification files and CRL files will be created automatically.

At right side of the screen, the **Certificate Signing Request (CSR)** the DM will readout the modem's CSR and certificate files. Or you can also read it by **Request** button file, or you can choose the << **Copy CSR** >> button.

Certification files and CA certifications (TLS) can be also handled here. TLS encrypted CA certification files are with .PEM or .CERT extension.

*Note, that this will be only effective, if you use TLS- compatible firmware version on the modem! Please, ask your sales product manager about the useful and appropriate firmware version before configuring this feature or updating the current firmware of the device.*

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

The **CA Certificate chain** can be requested to << **Download** >> or you can << **Upload** >> one or choose the << **Upload CRL** >>\*.

*\*In transparent mode, use of revoked certificates can be enabled with the CRL usage option (Certificate Revocation List).*

You can also << **Import** >> new certifications (CSV, EDN, XML file or a Shipment file) or you can make an export by using the << **CSV export** >> button.

Left side of the screen:

**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.

At **Certificates & PKI** tab, you can check the certification information in a detailed way.

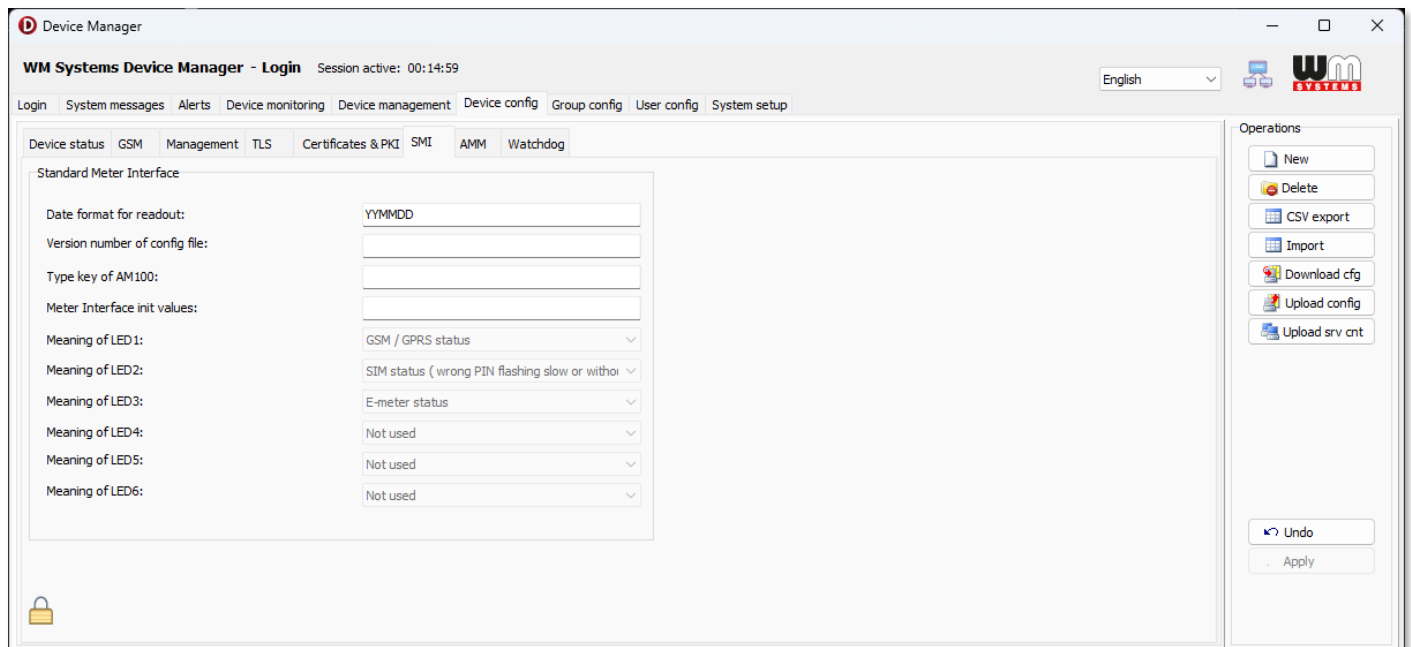
The screenshot shows the 'Device Manager' application window. The title bar reads 'WM Systems Device Manager - Login' with a session active for 00:14:59. The interface has a top navigation bar with tabs: 'Login', 'System messages', 'Alerts', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. Below this is a secondary navigation bar with tabs: 'Device status', 'GSM', 'Management', 'TLS', 'Certificates & PKI', 'SMI', 'AMM', and 'Watchdog'. The 'Certificates & PKI' tab is active, displaying 'Certificates information'. The certificate details are as follows:

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1061647735 (0x3f477577)
Signature Algorithm: ecdsa-with-SHA256
Issuer: CN=WM-Efluid DeviceTest CA
Validity
Not Before: Jan 23 19:00:43 2025 GMT
Not After : Jun 14 06:39:41 2025 GMT
Subject: CN=10000000000000000001
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
04:22:9b:70:8d:c1:ce:96:2b:d7:42:7a:13:71:d4:
af:61:90:e8:b1:ac:c1:41:2f:2d:3e:32:c0:48:dd:
7d:a3:fa:b9:0e:6d:a0:c4:9b:8e:14:50:c1:6c:fb:
4d:d2:77:75:ed:c2:26:1a:fc:cb:45:8f:52:a2:93:
e8:b7:e8:09:12
ASN1 OID: prime256v1
NIST CURVE: P-256
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Authority Key Identifier:
67:97:E2:D8:F7:29:E6:ED:AC:DE:89:5B:6A:01:D5:83:81:AE:16:07
X509v3 Extended Key Usage:
1.2.203.7064.1.1.369791.1, 1.2.203.7064.1.1.369791.2, TLS Web Client Authentication, E-mail Protection
```

The right-hand sidebar contains an 'Operations' panel with buttons: 'New', 'Delete', 'CSV export', 'Import', 'Download cfg', 'Upload cfg', 'Upload srv cnt', 'Undo', and 'Apply'.

At **SMI** tab, you can make the Standard Metering Information settings by the following:

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



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

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

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

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

At **AMM** tab, you can configure the AMM/IEC and DLMS settings of the modem.

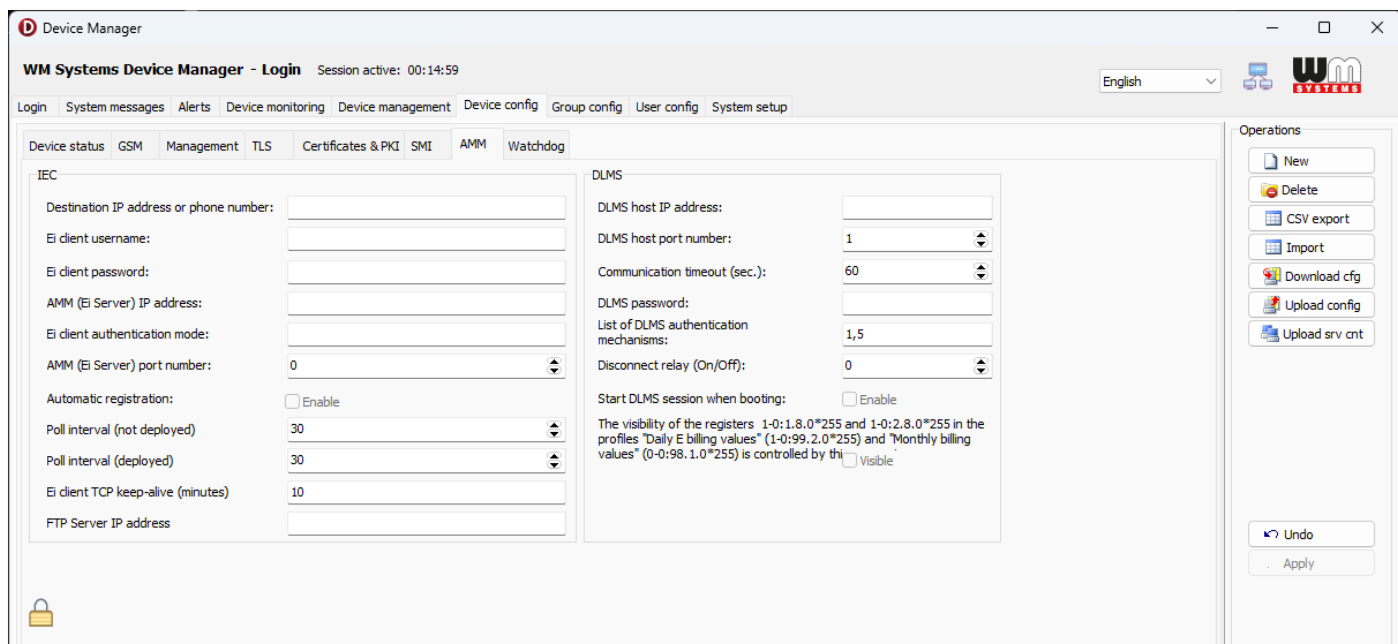
The following settings should be used consequently to the WM-ExS modem settings which are used in WM-E Term configuration software, at „**AMM/IEC settings**” parameter group.

#### **At left side of the screen (IEC) settings:**

**Destination IP Address or phone number** – here you can define the IP address where the data will be transmitted through the wireless network.

**EI Client username** is required for the connection IP address.

**EI Client password** is also also required, then fill these fields.



**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** means that a remote device can be configured and allowed to be connected to the modem and readout the data – by selecting authentication mode. Values: 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** – to the address - checkbox. In case of data push send automatically or not.

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

**Poll-interval slow (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**

### **At right side of the screen (DLMS):**

The following settings should be used consequently to the WM-ExS modem settings which are used in WM-E Term configuration software, at „**AMM/DLMS settings**” parameter group.

**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.

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

**DLMS password** – define password / DLMS encryption key (AES) for the connection.

**List of DLMS authentication mechanisms** – not used.

**Disconnect relay (On/Off)** - not implemented yet.

**Start DLMS session when booting** - You can enable the start DLMS session during the boot process.

**The visibility of the registers** ... of the profile - You can enable the visibility of the DLMS Load Profile registers here.

(1-0:1.8.0\*255 and 1-0:2.8.0\*255) in the profiles Daily E-billing values

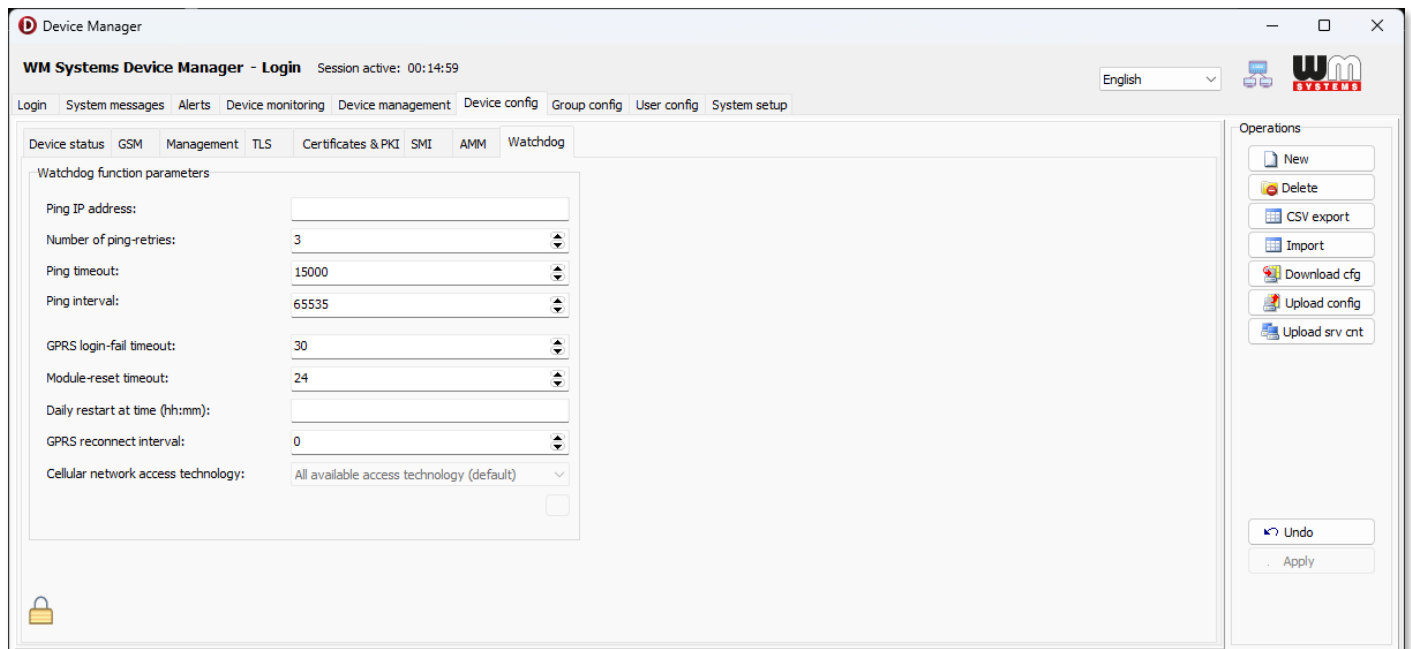
(1-0:99.2.0\*255) and Monthly billing values

(0-0:98.1.0\*255) is controlled by this parameter

*Important! It is important to use the appropriate firmware version on the metering modem, which can handle these parameters.*

At **Watchdog** tab, you can configure the modem watchdog settings of the modem.

The following settings should be used consequently to the WM-ExS modem settings which are used in WM-E Term configuration software, at „**Watchdog**” parameter group.



**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 / connection attempts.

**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. it is timeout when GPRS (PDP) login fail accours - tolerance interval of PDP connection establishment error.

**Module-reset timeout:** You can also configure length of GPRS connection trial in hours. from the start of the modem, the watchdog restarts the module at these hourly intervals. (This is true if the following field is not filled. If the Daily Restart on a fix, parametrized time field is filled, then only the settings there will take effect, meaning the modem will be restarted at a fixed time).

**Daily restart at time (hh:mm):** you can define an exact daily time for restarting the remote device. to schedule a time for daily restart of the modem – set an exact time it in *HHMM* time format. Or leave the field empty if you do not wish to restart every day.

E.g. 14 hours and 20 minutes – value 1420. (This will be applied if the previous field - Wait time until modem reset - is not filled. If it is filled, then the settings there will take effect, meaning the timing starts from the last restart of the modem, and upon the completion of the number of hours set there, the device will be restarted).

**GPRS reconnect interval:** length of GPRS reconnection (in seconds). Waiting time (in seconds) between establishing the PDP connection. This value is also used for ping! (If ping is configured (Ping Waiting Time (for response) parameter), then after the specified delay, it will automatically reconnect at the specified interval/repetition time.)

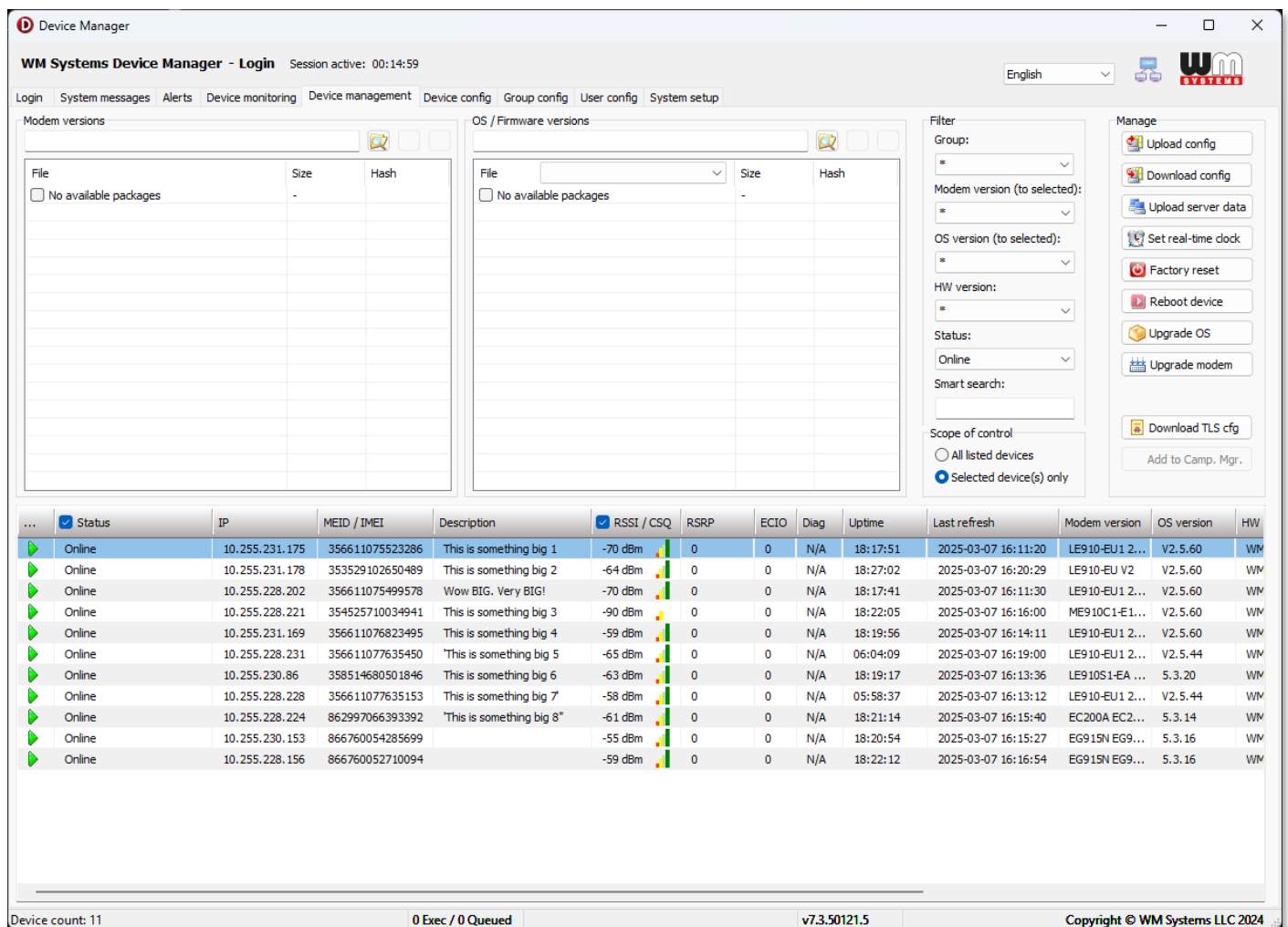
Here you can specify how long the device should wait after the provider cuts off the modem from the network before trying to reconnect to the mobile network again. Ask your mobile service provider for recommended settings.

*Attention! If there is less data traffic and there is no ping configured, the device may not stay on the network for a long time. If you set this parameter to a low value that can cause frequent network reconnections. Therefore, according to the circumstances, should you set this value lower as your mobile service provider recommends. (because there are some mobile network providers that limit the number of the modem network connection and registering attempts during the time (e.g. limit to four times per hour – or similar used to be configured by MOs).*

**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.



Here on this screen, you can see **ONLINE** devices only.

There you can see information of the devices (like on the **Device configuration** tab).

Status	IP	MEID / IMEI	Description	RSSI / CSQ	RSRP	ECIO	Diag	Uptime	Last refresh	Modem version	OS version
--------	----	-------------	-------------	------------	------	------	------	--------	--------------	---------------	------------

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

- **Upload config:** write the configuration to the device(s) (settings will be overwritten on the device).
- **Download config:** read the configuration from the remote device(s) into the DM's database.
- **Upload server data:** upload server data from DM to the device(s). This data contains the server IP address, port, and name.
- **Set real-time clock:** configure date/time of the device(s)

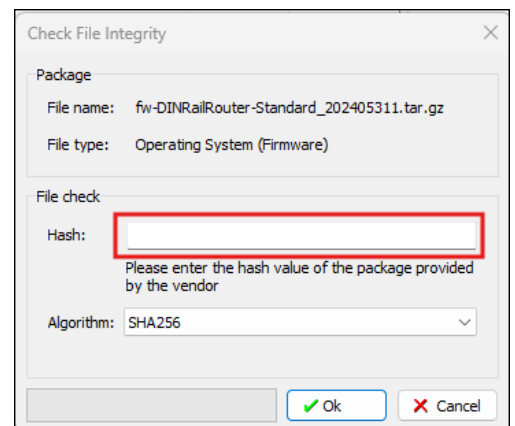
- **Factory reset:** doing a configuration reset of the remote device to the factory default.
- **Reboot device:** immediate restart of the remote device(s).
- **Upgrade OS:** device firmware upgrade or downgrade from the selected list to the remote device(s).
- **Upgrade modem:** this feature is not implemented yet.
- **Download TLS cfg:** you can download the TLS configuration here from devices.

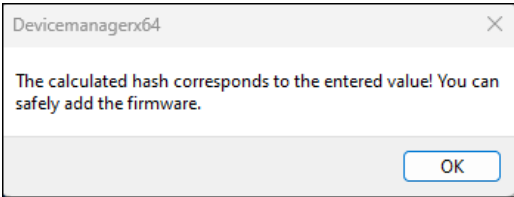
## 5.1 Firmware importing into the system


1. If you already have the released firmware file, first upload the file to the database. You need the hash for that firmware file, because during importing firmware the system will check it.

2. Browse the firmware file 

3. In the popup window insert the hash and press the **OK** button. The hash is coming from the firmware vendor with the firmware file.



4. If you see this message:  then you can add the

firmware to the database with the add button: 

Then wait for a few second until the completion of firmware adding and upload. It depends on the size of the file.

## 5.2 Firmware upgrade

With this feature, you can refresh the firmware on the device(s).

**Warning!** Any intervention during the firmware upgrade process may cause the failure of the device.

1. Select device(s) from the list from online devices.

Status	IP	MEID / IMEI	Description	RSSI / CSQ	RSRP	ECIO	Diag	Uptime	Last refresh	Modem version	OS version
Online	84.224.156.243	59852053517018	Sajtbox Teszt2 ELS_16-1...	-71 dBm	0	0	N/A	00:26:19	2024-07-04 20:27:01	17.00.523	20230726..
Online	94.44.27.111	59852054121349	Sajtbox Teszt3 ELS_16-0...	-61 dBm	0	4	N/A	3 01:29:42	2024-07-04 20:26:56	17.01.522	20230726..
Online	91.104.18.129	53529102543999	Sajtbox Teszt1 - ELS_16-...	-61 dBm	0	5	N/A	6 08:34:10	2024-07-04 20:25:41	20.00.405	20230726..
Online	10.217.102.242	53529102744415	TEST DEVICE 06	-71 dBm	0	1	N/A	20 05:58:42	2024-07-04 20:25:56	20.00.405	20230726..
Online	10.217.102.225	53529102738953	TEST DEVICE 07	-69 dBm	0	2	N/A	107 03:27:38	2024-07-04 20:26:07	20.00.405	20230726..
Online	10.217.102.244	53529102748788	TEST DEVICE 04	-71 dBm	0	2	N/A	107 03:26:57	2024-07-04 20:25:49	20.00.405	20230726..
Online	10.217.102.155	53529102753721	TEST DEVICE 10	-75 dBm	0	2	N/A	107 03:27:26	2024-07-04 20:25:56	20.00.405	20230726..
Online	10.217.102.245	53529102743482	TEST DEVICE 01	-69 dBm	0	2	N/A	06:20:18	2024-07-04 20:26:12	20.00.405	20230726..
Online	10.217.98.81	51622075254058	TEST DEVICE 12	-67 dBm	0	1	N/A	107 03:27:03	2024-07-04 20:25:47	20.00.406	20230726..
Online	10.217.102.224	53529102728020	TEST DEVICE 02	-71 dBm	0	2	N/A	107 03:26:45	2024-07-04 20:25:10	20.00.405	20230726..
Online	10.217.102.246	53529102738904	TEST DEVICE 03	-71 dBm	0	2	N/A	101 09:33:50	2024-07-04 20:26:06	20.00.405	20230726..
Online	10.217.98.106	53529102753531	TEST DEVICE 05	-73 dBm	0	1	N/A	101 09:35:02	2024-07-04 20:27:01	20.00.405	20230726..
Online	10.217.102.227	53529102756682	TEST DEVICE 09	-71 dBm	0	2	N/A	101 09:34:34	2024-07-04 20:26:18	20.00.405	20230726..
Online	10.202.189.51	53001090702902	TEST DEVICE 13 LE910C1...	-63 dBm	0	2	N/A	107 03:27:40	2024-07-04 20:25:54	25.20.223	20230726..
Online	10.217.98.67	53529102524445	TEST DEVICE 123	-69 dBm	0	1	N/A	101 09:34:12	2024-07-04 20:25:50	20.00.405	20230726..
Online	10.217.102.226	53529102755247	TEST DEVICE 08	-69 dBm	0	4	N/A	101 09:35:04	2024-07-04 20:27:01	20.00.405	20230726..

Device count: 16      0 Exec / 0 Queued      Events: 8096      v7.3.40530.8      Copyright © WM Systems LLC 2023

2. Select the firmware file from the file list and press to the **Upgrade OS** button.

File	Size	Hash
<input type="checkbox"/> fwos-BE0077B_CDMA450_...	7552067	C65E5B00
<input checked="" type="checkbox"/> fwos-BE0077B_CDMA450_...	7729324	4C9E7118
<input type="checkbox"/> fw-DINRailRouter-Standar...	12144190	AADADDE6

Manage

- Upload config
- Download config
- Upload server data
- Set real-time clock
- Factory reset
- Reboot device
- Upgrade OS**
- Upgrade modem
- Remote WIPE

Device Manager

**!** Are you sure to upload the configuration data of the selected (3) devices?

This could take long time, when many devices selected. This will cause the devices be restarted.




OK    Cancel

3. In the popup window you can still **Cancel** the upgrade process or press the **OK** button to perform the firmware update.




4. In the device list you will see the progress of the firmware upgrade.
  - a. The DM will upload the selected firmware file to the device(s). The time duration depends on file size, network speed, and network quality.

🔄	12%
🔄	14%
🔄	19%

At the system messages you can see:

	2024-07-04 18:34:26 UTC+02:00	3	Initializing firmware upgrade
	2024-07-04 18:34:26 UTC+02:00	3	Initializing firmware upgrade
	2024-07-04 18:34:26 UTC+02:00	3	Initializing firmware upgrade

- b. Then the device(s) will start the firmware upgrade. During this the device will be unavailable. This can take several minutes (up to 10 minutes). During this, it is FORBIDDEN to restart the device manually. That can cause damage of the device.







	Firmware upgrade
	Firmware upgrade
	Firmware upgrade

At the system messages you can see:

	2024-07-04 18:34:59 UTC+02:00	1	Device is upgrading firmware
	2024-07-04 18:34:56 UTC+02:00	1	Device is upgrading firmware
	2024-07-04 18:34:54 UTC+02:00	1	Device is upgrading firmware

- c. Whn the firmware upgrade is complete, devices are online again.

At the system messages you can see:

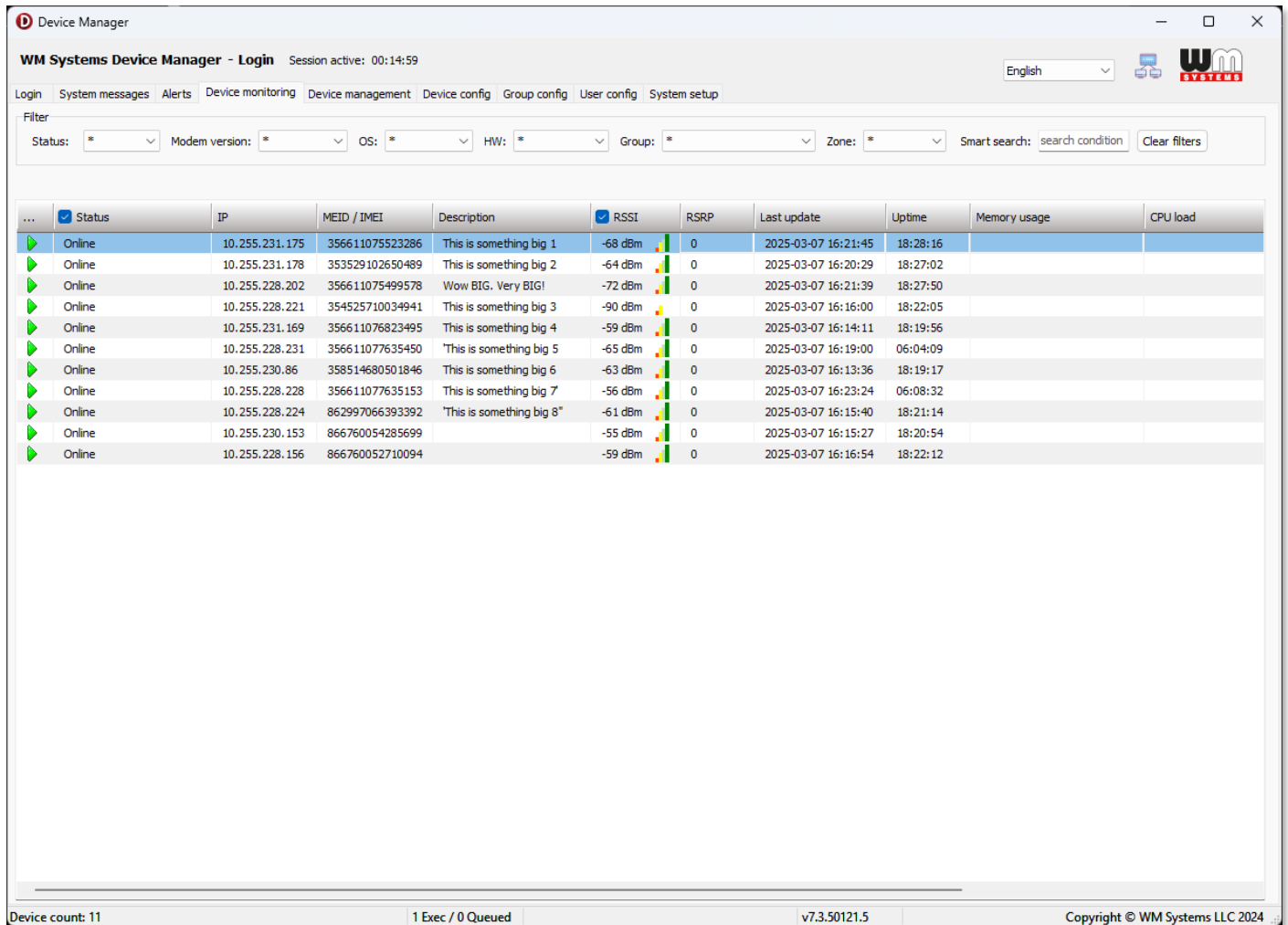
	2024-07-04 18:45:09 UTC+02:00	1	Setting RTC	
	2024-07-04 18:45:06 UTC+02:00	1	Firmware upgrade successfully finished	after reboot
	2024-07-04 18:44:59 UTC+02:00	1	Setting RTC	
	2024-07-04 18:44:58 UTC+02:00	1	Setting RTC	
	2024-07-04 18:44:56 UTC+02:00	1	Firmware upgrade successfully finished	after reboot
	2024-07-04 18:44:55 UTC+02:00	1	Firmware upgrade successfully finished	after reboot

After few minutes the OS version will be refreshed and you can see listed the new firmware version of the device.

OS version
202307261_RC
202307261_RC
202307261_RC

## Chapter 6. Device monitoring

On the **Device Monitoring** tab, you will find the current known status of your configured devices.



The screenshot shows the 'Device Manager' window with the 'Device monitoring' tab selected. The interface includes a navigation menu, a filter section, and a table of device data. The table has 11 columns: Status, IP, MEID / IMEI, Description, RSSI, RSRP, Last update, Uptime, Memory usage, and CPU load. All 11 devices listed are in an 'Online' status. The status column also contains small green and red icons. The bottom status bar shows 'Device count: 11', '1 Exec / 0 Queued', 'v7.3.50121.5', and 'Copyright © WM Systems LLC 2024'.

Status	IP	MEID / IMEI	Description	RSSI	RSRP	Last update	Uptime	Memory usage	CPU load
Online	10.255.231.175	356611075523286	This is something big 1	-68 dBm	0	2025-03-07 16:21:45	18:28:16		
Online	10.255.231.178	353529102650489	This is something big 2	-64 dBm	0	2025-03-07 16:20:29	18:27:02		
Online	10.255.228.202	356611075499578	Wow BIG. Very BIG!	-72 dBm	0	2025-03-07 16:21:39	18:27:50		
Online	10.255.228.221	354525710034941	This is something big 3	-90 dBm	0	2025-03-07 16:16:00	18:22:05		
Online	10.255.231.169	356611076823495	This is something big 4	-59 dBm	0	2025-03-07 16:14:11	18:19:56		
Online	10.255.228.231	356611077635450	This is something big 5	-65 dBm	0	2025-03-07 16:19:00	06:04:09		
Online	10.255.230.86	358514680501846	This is something big 6	-63 dBm	0	2025-03-07 16:13:36	18:19:17		
Online	10.255.228.228	356611077635153	This is something big 7	-56 dBm	0	2025-03-07 16:23:24	06:08:32		
Online	10.255.228.224	862997066393392	This is something big 8	-61 dBm	0	2025-03-07 16:15:40	18:21:14		
Online	10.255.230.153	866760054285699		-55 dBm	0	2025-03-07 16:15:27	18:20:54		
Online	10.255.228.156	866760052710094		-59 dBm	0	2025-03-07 16:16:54	18:22:12		

Here you can also filter some device properties. As you can see there are *offline*, *disabled*, and *online* listed devices besides the status 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 devices are listed, such as the signal strength of the cellular network (**RSSI**), the **RSRP**, **Last update** date/time, **Uptime** (spent time since last reboot or device start). Other information can be seen only for modems, not for the modems.

The QoS information will always help you to check and maintain your devices.

**IMPORTANT!** Note, that these data are not real-time, the status values show the last known operation behavior and vital 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 them by **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 00:15:00. The interface includes a navigation bar with 'Login', 'System messages (63)', 'Alerts (199)', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. A search bar is present with the text 'Smart search: search condition' and a 'Reverse Order' checkbox that is checked. An 'Acknowledge All' button is located in the top right of the alert list area.

ID	Timestamp	Event ID	Message	Details	Device ID	Operator
2	2024-07-04 10:24:46 UTC+02:00	2	[2024-01-19 08:31:31] authpriv.warn vbus: Power off. System halted.		68110060089560	System
2	2024-07-04 10:24:46 UTC+02:00	2	[2024-01-24 08:18:32] kern.info kernel: [ 1756.644999] mach_f802c000.et...		68110060089560	System
2	2024-07-04 10:24:46 UTC+02:00	2	[2024-01-24 08:36:59] kern.info kernel: [ 2863.203080] mach_f802c000.et...		68110060089560	System
2	2024-07-04 10:24:46 UTC+02:00	2	[2024-01-24 08:36:59] authpriv.warn vbus: Power off. System halted.		68110060089560	System
2	2024-07-04 10:24:46 UTC+02:00	2	[2024-07-04 10:35:50] kern.info kernel: [ 5598.321131] mach_f802c000.et...		68110060089560	System
2	2024-07-04 10:24:46 UTC+02:00	2	[2024-07-04 10:35:51] authpriv.warn vbus: Power off. System halted.		68110060089560	System
2	2024-07-04 10:05:07 UTC+02:00	2	[2024-01-23 08:38:24] authpriv.warn vbus: Power off. System halted.		68110060096219	System
2	2024-07-03 11:06:46 UTC+02:00	2	[2024-01-24 11:23:19] authpriv.warn vbus: Power off. System halted.		68110060099155	System
2	2024-07-03 09:54:29 UTC+02:00	2	[2024-01-22 13:23:48] authpriv.warn vbus: Power off. System halted.		68110060095823	System
2	2024-07-03 08:54:03 UTC+02:00	2	[2024-07-03 10:49:51] authpriv.warn vbus: Power off. System halted.		68110060408836	System
1	2024-07-03 08:49:54 UTC+02:00	1	Power source failure	shutting down	68110060408836	System
2	2024-07-03 08:41:55 UTC+02:00	2	[2024-07-03 10:41:39] authpriv.warn vbus: uUSB connected.		68110060408836	System
1	2024-07-02 21:33:29 UTC+02:00	1	Power source failure	shutting down	68110060400551	System
1	2024-07-02 21:33:27 UTC+02:00	1	Power source failure	shutting down	68110060400551	System
2	2024-07-02 21:28:00 UTC+02:00	2	[2024-07-02 16:47:35] authpriv.warn vbus: Power off. System halted.		68110060400551	System
1	2024-07-02 14:47:37 UTC+02:00	1	Power source failure	shutting down	68110060400551	System
1	2024-07-02 13:14:53 UTC+02:00	1	Power source failure	shutting down	68110060401344	System
1	2024-07-02 13:14:51 UTC+02:00	1	Power source failure	shutting down	67007060012603	System
2	2024-07-02 13:13:38 UTC+02:00	2	[2024-07-02 15:13:27] authpriv.warn vbus: uUSB disconnected.		68110060401344	System
2	2024-07-02 11:57:26 UTC+02:00	2	[2024-07-02 13:57:12] kern.info kernel: [ 463.141267] mach_f802c000.et...		68110060401344	System
2	2024-07-02 11:57:26 UTC+02:00	2	[2024-07-02 13:57:23] authpriv.warn vbus: uUSB connected.		68110060401344	System
2	2024-07-02 11:55:42 UTC+02:00	2	[2024-06-27 12:05:51] authpriv.warn vbus: Power off. System halted.		68110060400551	System
2	2024-07-02 11:52:10 UTC+02:00	2	[2024-06-27 13:11:01] authpriv.warn vbus: Power off. System halted.		68110060401344	System
2	2024-07-02 11:12:18 UTC+02:00	2	[2024-01-24 08:37:09] authpriv.warn vbus: Power off. System halted.		68110060100243	System
2	2024-07-02 10:53:34 UTC+02:00	2	[2024-01-24 13:05:15] authpriv.warn vbus: Power off. System halted.		68110060180930	System
2	2024-07-02 08:58:26 UTC+02:00	2	[2024-01-24 13:05:15] authpriv.warn vbus: Power off. System halted.		68110060092671	System
2	2024-07-01 12:33:01 UTC+02:00	2	[2024-07-01 14:32:40] kern.info kernel: [ 2145.529168] mach_f802c000.et...		68110060177704	System
2	2024-07-01 12:32:59 UTC+02:00	2	[2024-07-01 14:32:40] kern.info kernel: [ 2137.691683] mach_f802c000.et...		68110060091202	System
2	2024-07-01 12:32:29 UTC+02:00	2	[2024-07-01 14:32:09] kern.info kernel: [ 2106.246451] mach_f802c000.et...		68110060409115	System
2	2024-07-01 12:32:01 UTC+02:00	2	[2024-07-01 14:31:49] kern.info kernel: [ 2086.338239] mach_f802c000.et...		68110060413539	System
2	2024-07-01 12:31:57 UTC+02:00	2	[2024-07-01 14:31:41] kern.info kernel: [ 2078.249880] mach_f802c000.et...		68110060182183	System
2	2024-07-01 11:59:05 UTC+02:00	2	[2024-07-01 13:45:35] authpriv.warn vbus: Power off. System halted.		68110060182183	System
2	2024-07-01 11:58:46 UTC+02:00	2	[2024-07-01 09:53:07] authpriv.warn vbus: Power off. System halted.		68110060409115	System
2	2024-07-01 11:58:46 UTC+02:00	2	[2024-07-01 13:41:10] authpriv.warn vbus: Power off. System halted.		68110060177704	System
2	2024-07-01 11:58:46 UTC+02:00	2	[2024-07-01 13:54:33] authpriv.warn vbus: Power off. System halted.		68110060177704	System
2	2024-07-01 11:58:45 UTC+02:00	2	[2024-07-01 13:53:44] authpriv.warn vbus: Power off. System halted.		68110060091202	System
2	2024-07-01 11:58:44 UTC+02:00	2	[2024-06-29 18:49:28] authpriv.warn vbus: Power off. System halted.		68110060413539	System
1	2024-07-01 11:54:35 UTC+02:00	1	Power source failure	shutting down	68110060177704	System
1	2024-07-01 11:54:35 UTC+02:00	1	Power source failure	shutting down	68110060177704	System
1	2024-07-01 11:53:46 UTC+02:00	1	Power source failure	shutting down	68110060091202	System
2	2024-07-01 11:53:23 UTC+02:00	2	[2024-07-01 13:36:40] authpriv.warn vbus: Power off. System halted.		68110060091202	System

Device count: 293      0 Exec / 0 Queued      Alerts: 199      v7.3.40530.8      Copyright © WM Systems LLC 2023

# 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 related checkbars on the color message type icons – to filter the messages by event type(s).

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

ID	Timestamp	Event ID	Message	Details	Device ID	Operator
1	2024-07-04 10:24:46 UTC+02:00	2	[2024-01-24 08:36:59] kern.info kernel: [ 2863.203080] macb f802000.et...		68110060089560	System
2	2024-07-04 10:24:46 UTC+02:00	2	[2024-01-24 08:36:59] authpriv.warn vbus: Power off. System halted.		68110060089560	System
3	2024-07-04 10:24:46 UTC+02:00	1	[2017-01-01 01:02:56] daemon.warn dmd[1295]: because isWAN_interfac...		68110060089560	System
4	2024-07-04 10:24:46 UTC+02:00	2	[2024-07-04 10:35:50] kern.info kernel: [ 5598.321131] macb f802000.et...		68110060089560	System
5	2024-07-04 10:24:46 UTC+02:00	2	[2024-07-04 10:35:51] authpriv.warn vbus: Power off. System halted.		68110060089560	System
6	2024-07-04 10:24:46 UTC+02:00	1	[2017-01-01 01:01:40] daemon.warn dmd[1295]: because isWAN_interfac...		68110060089560	System
7	2024-07-04 10:24:46 UTC+02:00	1	[2024-07-04 12:24:32] daemon.warn dmd[1295]: Install condition check I.E...		68110060089560	System
8	2024-07-04 10:24:46 UTC+02:00	1	[2024-07-04 12:24:32] daemon.warn dmd[1295]: because isCALL_Process...		68110060089560	System
9	2024-07-04 10:24:41 UTC+02:00	1	Device configuration downloaded		68110060089560	System
10	2024-07-04 10:24:36 UTC+02:00	1	Setting RTC		68110060089560	System
11	2024-07-04 10:24:33 UTC+02:00	1	IP address changed	10.219.113.39 -> 10.219.112.87	68110060089560	System
12	2024-07-04 10:24:32 UTC+02:00	1	Device connected for the first time		68110060089560	System
13	2024-07-04 10:07:25 UTC+02:00	1	Connection lost with the device.	Missing periodic call	68110060096219	System
14	2024-07-04 10:07:25 UTC+02:00	1	Connection lost with the device.	Missing periodic call	68110060096219	System
15	2024-07-04 10:05:11 UTC+02:00	1	Uploaded device configuration	Scheduled config push	68110060096219	System
16	2024-07-04 10:05:07 UTC+02:00	2	[2024-01-23 08:38:24] authpriv.warn vbus: Power off. System halted.		68110060096219	System
17	2024-07-04 10:05:07 UTC+02:00	1	[2024-07-04 12:04:53] daemon.warn dmd[1294]: Install condition check I.E...		68110060096219	System
18	2024-07-04 10:05:07 UTC+02:00	1	[2024-07-04 12:04:53] daemon.warn dmd[1294]: because isCALL_Process...		68110060096219	System
19	2024-07-04 10:05:07 UTC+02:00	1	[2024-07-04 12:04:53] daemon.warn dmd[1294]: because isWAN_interfac...		68110060096219	System
20	2024-07-04 10:05:03 UTC+02:00	1	Device configuration downloaded		68110060096219	System
21	2024-07-04 10:04:57 UTC+02:00	1	Setting RTC		68110060096219	System
22	2024-07-04 10:04:52 UTC+02:00	1	IP address changed	10.219.114.189 -> 10.219.112.25	68110060096219	System
23	2024-07-04 10:04:51 UTC+02:00	1	Device connected for the first time		68110060096219	System
24	2024-07-04 08:13:43 UTC+02:00	1	[2024-07-04 10:12:23] daemon.warn dmd[1312]: Install condition check I.E...		68110060090261	System
25	2024-07-04 08:13:43 UTC+02:00	1	[2024-07-04 10:12:23] daemon.warn dmd[1312]: because isCALL_Process...		68110060090261	System
26	2024-07-04 08:13:43 UTC+02:00	1	[2024-07-04 10:13:33] daemon.warn dmd[1312]: Install condition check I.E...		68110060090261	System
27	2024-07-04 08:13:43 UTC+02:00	1	[2024-07-04 10:13:33] daemon.warn dmd[1312]: because isCALL_Process...		68110060090261	System
28	2024-07-04 08:09:59 UTC+02:00	1	[2024-07-04 10:09:18] daemon.warn dmd[1312]: Install condition check I.E...		68110060090261	System
29	2024-07-04 08:09:59 UTC+02:00	1	[2024-07-04 10:09:18] daemon.warn dmd[1312]: because isCALL_Process...		68110060090261	System
30	2024-07-04 08:09:59 UTC+02:00	1	[2024-07-04 10:09:53] daemon.warn dmd[1312]: Install condition check I.E...		68110060090261	System
31	2024-07-04 08:09:59 UTC+02:00	1	[2024-07-04 10:09:53] daemon.warn dmd[1312]: because isCALL_Process...		68110060090261	System
32	2024-07-04 04:02:15 UTC+02:00	1	[2024-07-04 06:00:57] daemon.warn dmd[1312]: Install condition check I.E...		68110060090261	System
33	2024-07-04 04:02:15 UTC+02:00	1	[2024-07-04 06:00:57] daemon.warn dmd[1312]: because isCALL_Process...		68110060090261	System
34	2024-07-04 04:02:15 UTC+02:00	1	[2024-07-04 06:02:07] daemon.warn dmd[1312]: Install condition check I.E...		68110060090261	System
35	2024-07-04 04:02:15 UTC+02:00	1	[2024-07-04 06:02:07] daemon.warn dmd[1312]: because isCALL_Process...		68110060090261	System
36	2024-07-04 01:07:53 UTC+02:00	1	[2024-07-04 03:07:41] daemon.warn dmd[1312]: Install condition check I.E...		68110060090261	System
37	2024-07-04 01:07:53 UTC+02:00	1	[2024-07-04 03:07:41] daemon.warn dmd[1312]: because isEMF_Level_OK...		68110060090261	System
38	2024-07-04 01:07:53 UTC+02:00	1	[2024-07-04 03:07:46] daemon.warn dmd[1312]: Install condition check I.E...		68110060090261	System
39	2024-07-04 01:07:53 UTC+02:00	1	[2024-07-04 03:07:46] daemon.warn dmd[1312]: because isEMF_Level_OK...		68110060090261	System

# 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/>

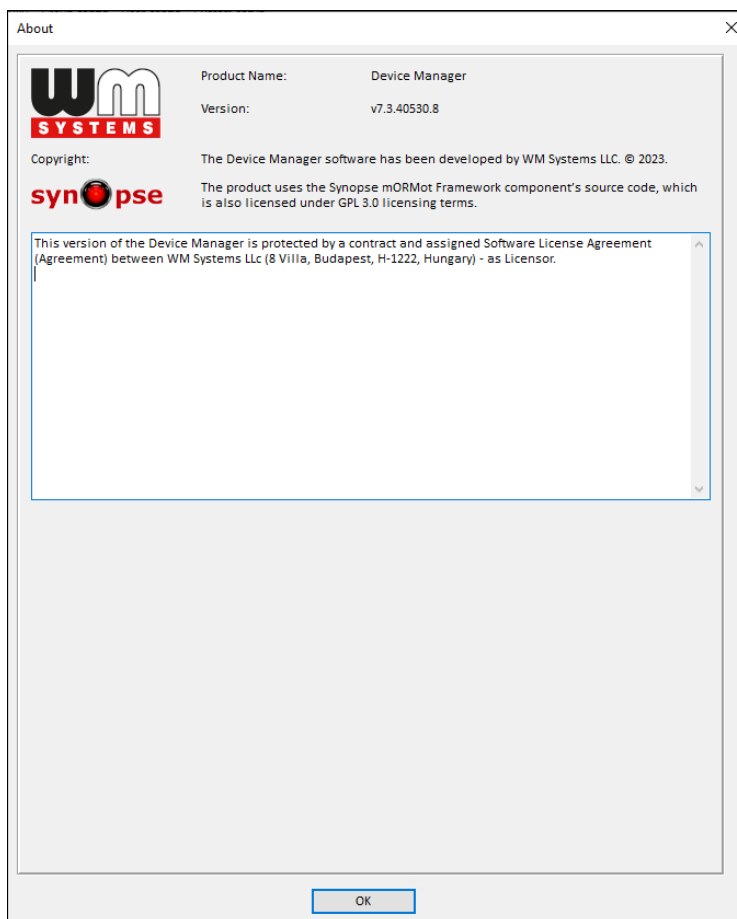
The documentation and software release for this product can be accessed via the following link:

<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.



## 10. Legal notice

©2025. WM Systems LLC.

The content of this documentation (all information, pictures, tests, descriptions, guides, and 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.