

Device Manager[®]

for M2M Router devices

User Manual

v2.5

The screenshot displays the 'Device Manager' web interface. The top navigation bar includes 'Login', 'System messages (338)', 'Alerts (6440)', '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: 7661 51622076472675, ICC: 89367031561930039632, Network IP: 10.217.102.66, Port: 22 / 443, Login name: root, Password: [masked], Description: EASY BACKUP PRODUCTION - BACKUP_HC-PATROL, Group: BACKUP), 'Modem settings' (Watchdog: 0 h, Power on delay: 0 s, Cyclic sending: 120 s, Time window: 300 s, Technology: Auto, MCC: [empty], RSRP threshold: 0), 'LAN DHCP settings' (Start: 0, Limit: 0, Lease time: 0 h, Alert: Enable, RSSI warning: -90, RSSI error: -110), 'LAN IP settings' (Comm: Nat, Local IP: 192.168.1.150, Netmask: 255.255.255.0, Gateway: [empty], Broadcast: [empty], Port forward: [empty], Port route: [empty]), 'WAN settings' (User name: [empty], Password: [empty], New MSIN: [empty]), and 'APN' (Name: wm2m). A 'Scheduled Config Push' section is also visible.

Status	IP	MEID / IMEI	Description	RSSI / CSQ	RSRP	ECIO	Diag	Uptime	Last refresh	Modem version	OS
Online	84.224.157.88	59852053517018	Sajtbox Teszt12 ELS_16-13-000-302	-75 dBm	0	99	N/A	4 06:21:05	2025-03-07 09:17:22	17.00.523	
Online	172.31.153.92	59852054108155	EASY BACKUP PRODUCTION - BACKUP_RAB...	-73 dBm	0	0	N/A	00:07:47	2025-03-07 09:18:28	17.01.522	
Online	172.31.150.255	53529103780889	EASY BACKUP PRODUCTION - BACKUP_PAL...	-73 dBm	0	99	N/A	15:56:13	2025-03-07 09:18:28	20.00.405	
Online	130.43.231.73	59852054121349	Sajtbox Teszt3 ELS_16-06-000-200	-63 dBm	0	2	N/A	5 14:49:37	2025-03-07 09:18:32	17.01.522	
Online	10.202.185.203	53529102724433	EASY BACKUP PRODUCTION - BACKUP_OBJ...	-61 dBm	0	4	N/A	10 23:40:48	2025-03-07 09:18:12	20.00.405	
Online	10.217.102.66	51622076472675	EASY BACKUP PRODUCTION - BACKUP_HC...	-69 dBm	0	3	N/A	1 01:08:12	2025-03-07 09:18:19	20.00.403	
Online	192.168.30.228	53529102558625	VODAFONE_GW	-51 dBm	0	1	N/A	191 17:52:41	2025-03-07 09:16:53	20.00.405	
Online	172.31.14.233	59852053963238	EASY BACKUP PRODUCTION - BACKUP_ZAV...	-63 dBm	0	4	N/A	01:56:20	2025-03-07 09:18:25	17.01.522	
Offline	172.31.87.72	53529102573830	EASY BACKUP PRODUCTION - BACKUP_LEG...	-51 dBm	0	0	N/A	8 01:50:32	2024-07-26 12:35:18	20.00.403	
Offline	84.224.192.1	53529102543999	Sajtbox Teszt11 - ELS_16-13-000-300	-61 dBm	0	1	N/A	72 03:50:04	2024-11-07 16:24:13	20.00.405	

Device count: 70 | 0 Exec / 0 Queued | Alerts: 6440 | v7.3.41210.2 | Copyright © WM Systems LLC 2024

07-03-2025

Document specifications

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

Document category:	User Manual for M2M Router and DCU devices
Document subject:	Device Manager [®]
Author:	WM Systems LLC
Document version No.:	REV 2.5
Number of pages:	57
Device manager version:	v7.3 41210.2
Document status:	final
Last modified:	07.03.2025
Approval date:	07.03.2025

Table of contents

Chapter 1. Introduction	4
Chapter 2. Setup and Configuration	6
2.1 Prerequisites.....	6
2.2 System elements	6
2.3 Installation.....	7
2.4 TLS protocol communication	10
Chapter 3. System configuration.....	11
3.1 System setup	11
3.2 User settings	16
3.3 AD User settings	18
Chapter 4. Device settings.....	20
4.1 Device group configuration.....	20
4.2 Device config overview	21
4.3 Add new device	24
4.4 General settings	26
4.5 Location settings	30
4.6 Miscellaneous settings.....	30
4.7 Package List.....	311
4.8 Two-Factor Authentication settings	311
4.9 TLS settings	322
4.10 SCEP config.....	333
4.11 Firewall config.....	377
4.12 SYSLOG config.....	455
Chapter 5. Device Management.....	499
5.1 Firmware importing into the system	50
5.2 Firmware upgrade.....	51
Chapter 6. Device monitoring	533
Chapter 7. Alerts.....	54
Chapter 8. System messages	554
Chapter 9. Support.....	565
9.1 Technical Support	566
10. Legal notice	577

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 the WM-i data loggers).

In this part we will care about only the router and DCU devices.

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, vital 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 M2M devices in remote locations.

By receiving info on the device's availability, the monitoring of vital 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 M2M device and the Device Manager® software.

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

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

Chapter 2. Setup and Configuration

2.1 Prerequisites

Approximately 10,000 endpoint devices can be managed by a Device Manager. Here we describe the software usage with our router and DCU devices such as:

- M2M LTE Cat.4 Router
- M2M Industrial Router
- M2M Industrial Router 2 Secure
- M2M Industrial Router 2 DCU
- M2M Industrial Router 2 DCU MBUS
- M2M Industrial Router 2 DCU wMBUS
- M2M Router PRO4 / IoT Router Gateway PRO4
- M2M Router PRO4 DCU MBUS
- Industrial DIN Rail Router

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, 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

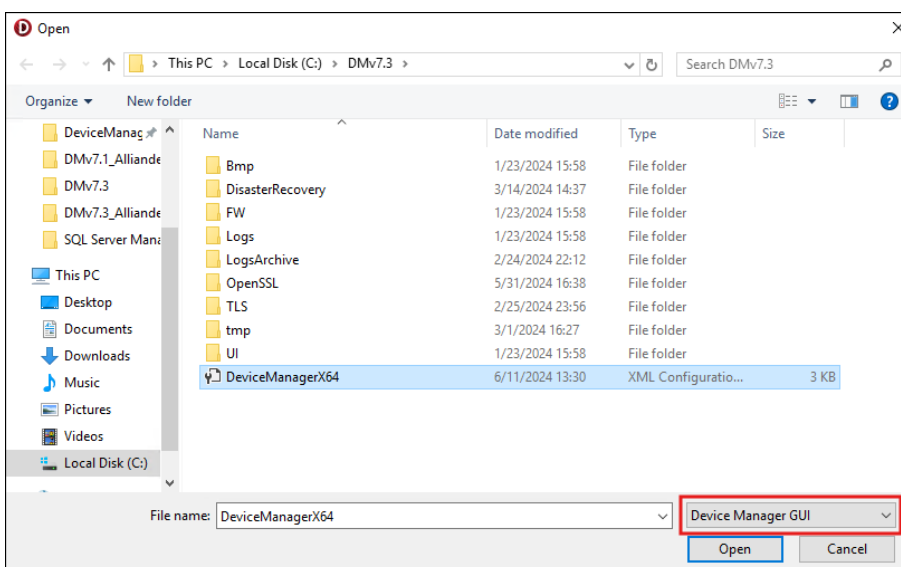
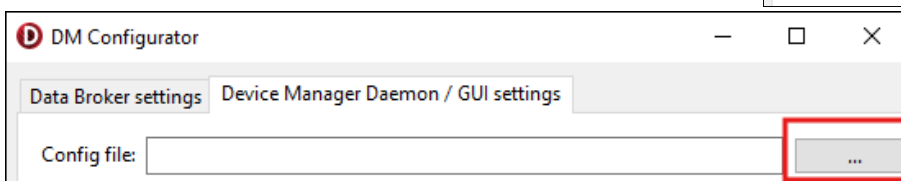
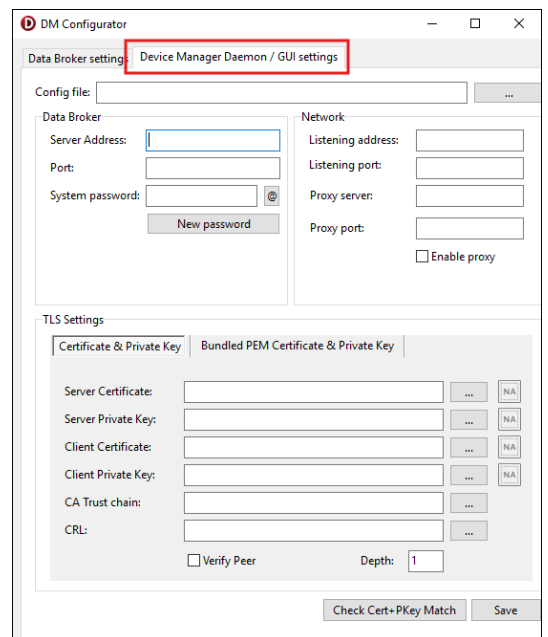
This is the device management user interface-, and business logic.

It communicates with the Data Broker via a REST API, and with the M2M devices through WM Systems' proprietary device management protocol.

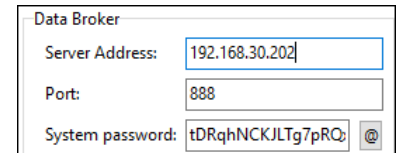
The communication flows in a TCP socket, which can optionally be secured with industry-standard TLS v1.2 transport layer security solution, based on mbedTLS (on the device side) and OpenSSL (on the server side).

2.3 Installation

1. Create the root folder on the destination system' 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.

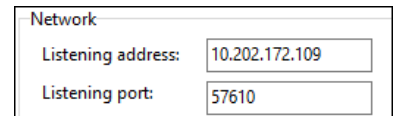


6. Set the parameters of the **Data Broker** and also set the password for the **Device Manager Daemon**.



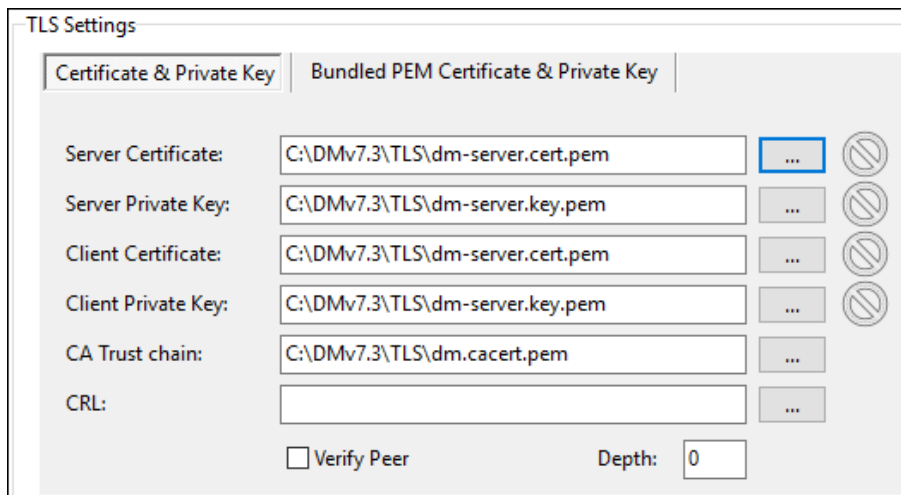
The screenshot shows the 'Data Broker' configuration window. It contains three input fields: 'Server Address' with the value '192.168.30.202', 'Port' with the value '888', and 'System password' with the value 'tDRqhNCKJLTg7pRQ;'. There is a small icon to the right of the password field.

7. 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 contains two input fields: 'Listening address' with the value '10.202.172.109' and 'Listening port' with the value '57610'.

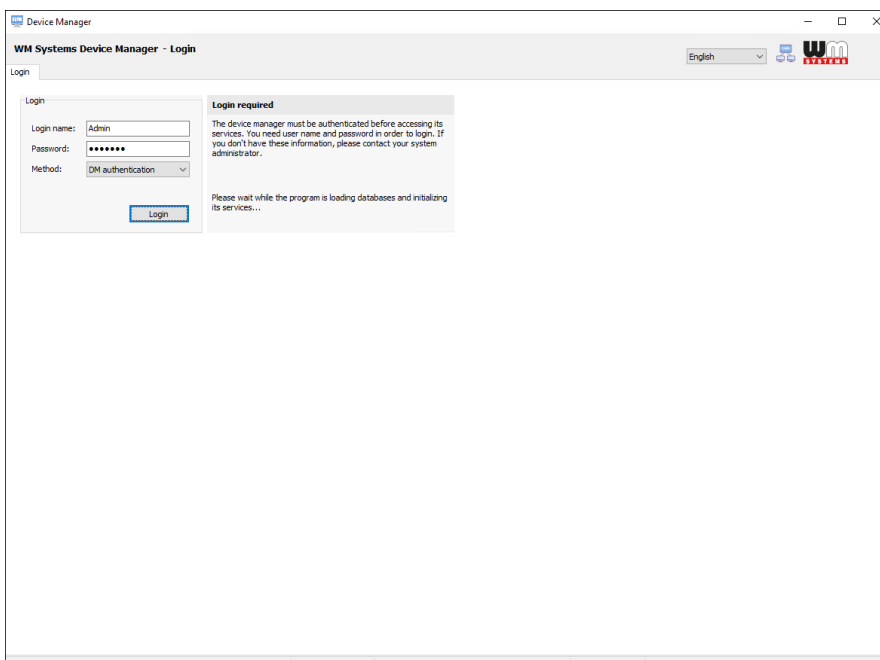
8. Locate and set all certificate files (with *.pem file extension) from the directory.



The screenshot shows the 'TLS Settings' window. It has two tabs: 'Certificate & Private Key' (selected) and 'Bundled PEM Certificate & Private Key'. Below the tabs are several input fields for certificates and keys, each with a browse button (three dots) and a lock icon. The fields are: 'Server Certificate', 'Server Private Key', 'Client Certificate', 'Client Private Key', 'CA Trust chain', and 'CRL'. All fields have the path 'C:\DMv7.3\TLS\dm-server.cert.pem' or 'C:\DMv7.3\TLS\dm-server.key.pem' or 'C:\DMv7.3\TLS\dm.cacert.pem'. At the bottom, there is a checkbox for 'Verify Peer' and a 'Depth' field set to '0'.

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

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



The screenshot shows the 'Device Manager' login window. The title bar says 'Device Manager' and the window content says 'WM Systems Device Manager - Login'. There is a language dropdown set to 'English' and a WM logo. The 'Login' section has three input fields: 'Login name' with 'Admin', 'Password' with masked characters, and 'Method' with 'DM authentication'. A 'Login' button is below. To the right, a 'Login required' message states: 'The device manager must be authenticated before accessing its services. You need user name and password in order to login. If you don't have these information, please contact your system administrator.' Below this, it says 'Please wait while the program is loading databases and initializing its services...'. At the bottom, the version 'v7.3.40530.8' and copyright 'Copyright © WM Systems LLC 2023' are visible.

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

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

(The login data are case-sensitive!)

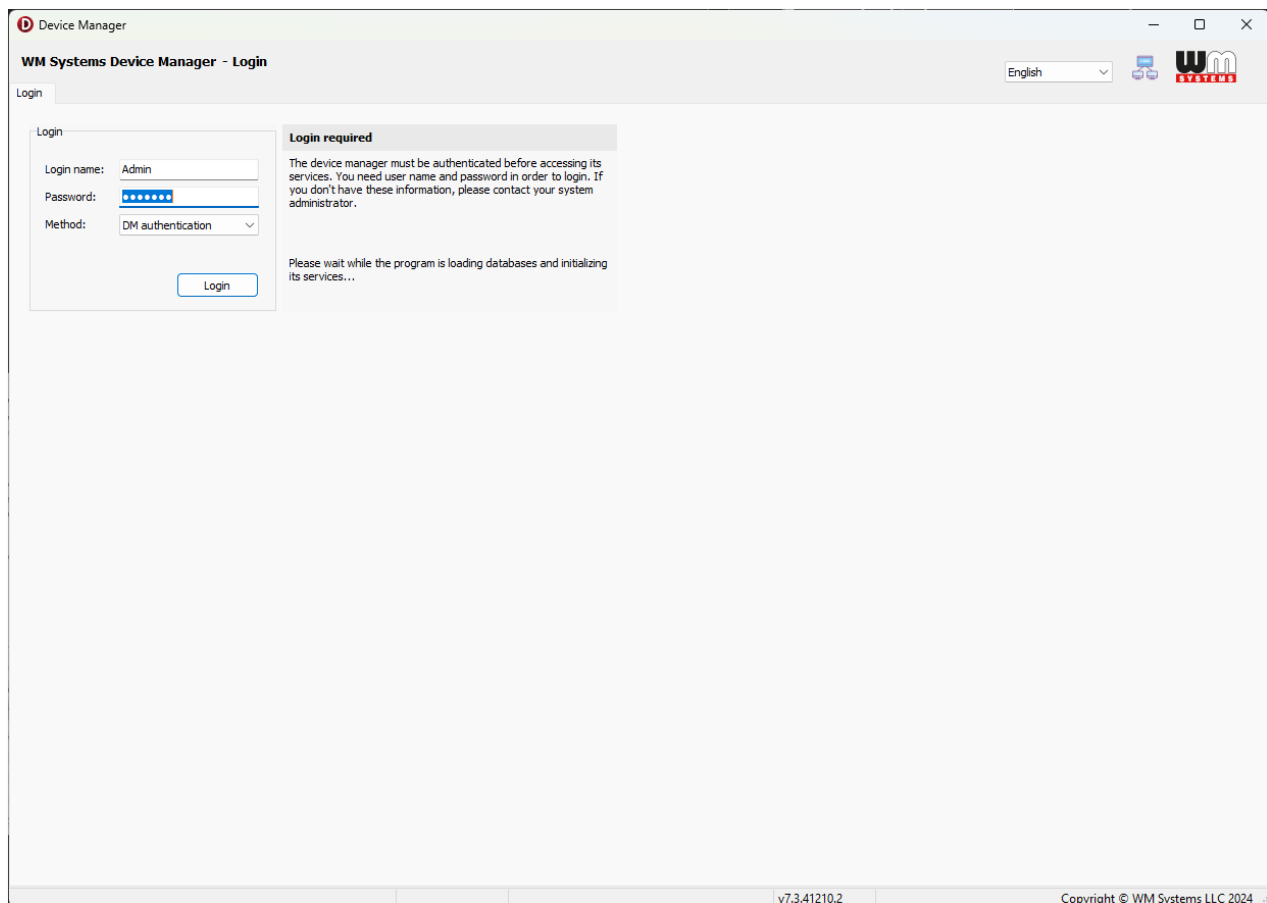
11. Press the **Login** button to enter into the system.

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 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 TLS solution can use a mutual authentication method as an option to identify the two parties involved in a communication.

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

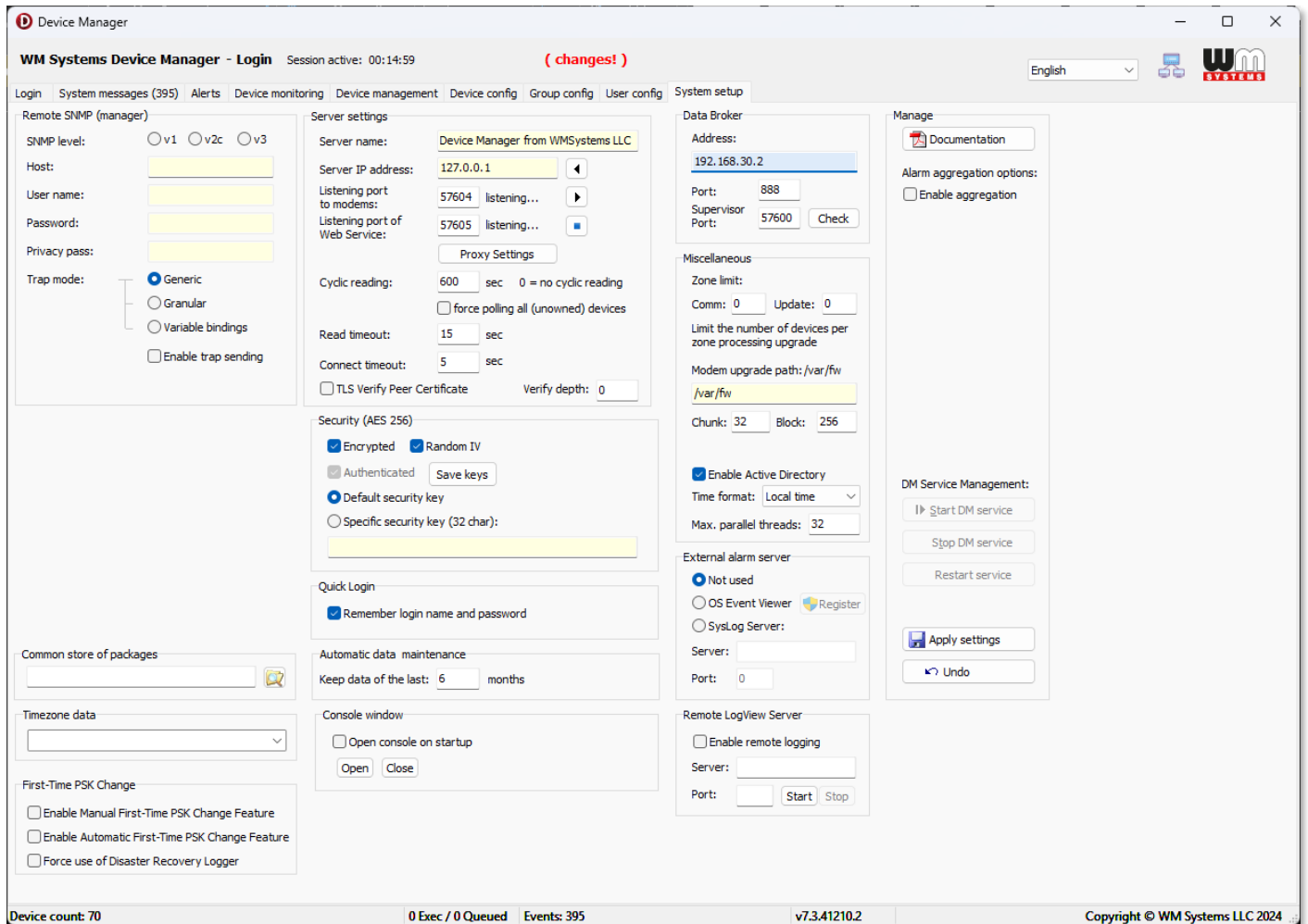
Only a factory default setting is implemented on the router, so the router does not check whether the certificate presented of a connected party is signed by a trusted party. Any TLS connection to the router can be established with any certificate, even if its self-signed.

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. routers). It sends the following SNMP traps to the SNMP server and the devices are sending their events:

- 1.3.6.1.6.3.1.1.5.1 – Cold Start
- 1.3.6.1.6.3.1.1.5.2 – Warm Start
- 1.3.6.1.6.3.1.1.5.3 – Ethernet link down
- 1.3.6.1.6.3.1.1.5.4 – Ethernet link up
- 1.3.6.1.6.3.1.1.5.5 – Authentication failure (unauthorized login attempt or wrong password)

The SNMP trap 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.

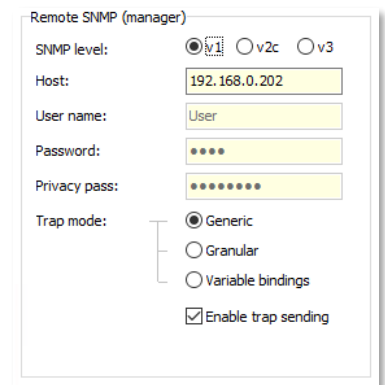
Trap mode: depending on the manager's capabilities, the program can send traps with the so-called variable bindings providing detailed information about the event and the relevant node.

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".

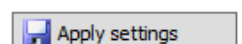
In case of failure, changed settings can be revoked by the **Undo** button.

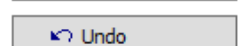
When you want to save the settings, press the **Apply settings** button.



The screenshot shows a configuration window titled "Remote SNMP (manager)". It contains the following fields and options:

- SNMP level:** Radio buttons for v1 (selected), v2c, and v3.
- Host:** Text input field containing "192.168.0.202".
- User name:** Text input field containing "User".
- Password:** Password input field with four dots.
- Privacy pass:** Password input field with eight dots.
- Trap mode:** Radio buttons for Generic (selected), Granular, and Variable bindings.
- Enable trap sending:** A checked checkbox.

 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.

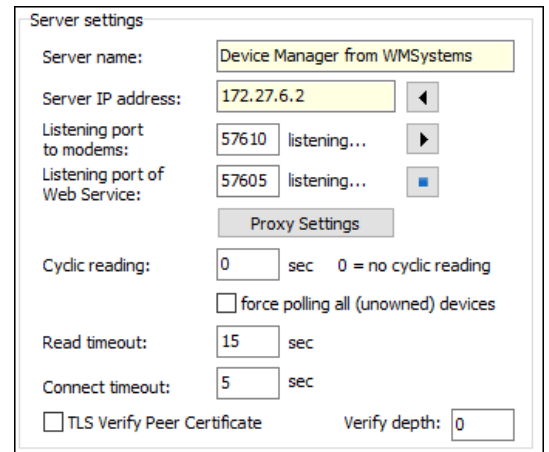
Cyclic reading (sec): you can define a periodic reading of the devices. The Device Manager can cyclically poll devices when configured to do so. We don't offer to configure smaller periodic than 600 seconds.

- The zero value equals no polling.

- The default value is "0" because the server does not initiate the 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 controls:

- 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 checkbox (unchecked)
- Read timeout: 15 sec
- Connect timeout: 5 sec
- TLS Verify Peer Certificate checkbox (unchecked)
- 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.

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. 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.

Miscellaneous

Zone limit: Restricts the number of simultaneous uploads to devices in the same zone (In the case of non-CDMA devices the zone is 0). Thus reduces the load of the network.

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:

Recall that users can initiate upload upgrade packages in the Device Manager screen to a large number of devices, and even to all devices in the network. If you use CDMA devices, without these settings, the CDMA network could be 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 firmware 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.

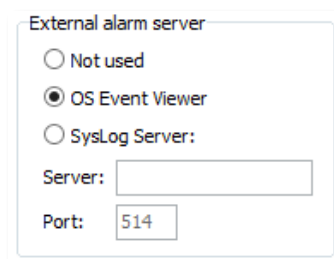
Time format: can be chosen from *Local time* or *UTC*.

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



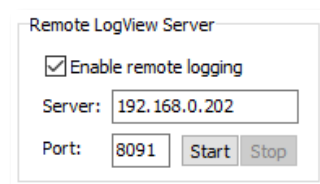
The screenshot shows a configuration window titled "External alarm server". It contains three radio button options: "Not used", "OS Event Viewer" (which is selected), and "SysLog Server:". Below the "SysLog Server:" option, there are two input fields: "Server:" and "Port:". The "Port:" field contains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

Remote LogView Server

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




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

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

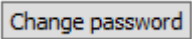
If you want to edit existing parameters, press the  button. This solution prevents accidental modification.

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.

Main data

Full name: (1) Admin

Login name: Admin

Password:

Change password

Access level: Administrator

Language: English

SNMP user Write permission

Session timeout: 0:00:00

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

Access level:

- **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 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.

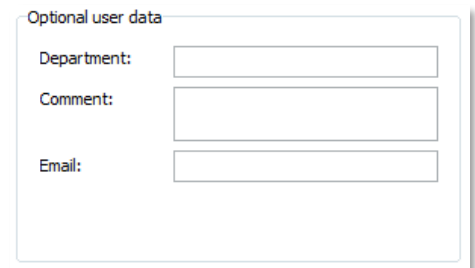
Session timeout: automatic logout can be also defined.

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:

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:

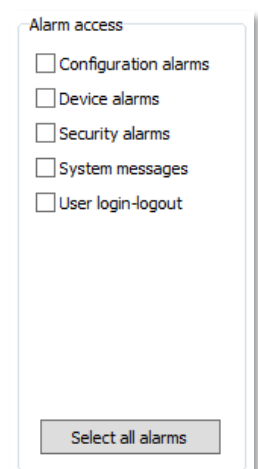
Group 2:

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.

User groups

Main data

Group Name: (5) DM_ADMINS

Domain name: WM

Access level: Administrator

Language: English

SNMP user Write permission AD auth.

Session timeout: 0:00:00

Optional user data

Department:

Comment:

Device group access

Main group: *

Group 2: *

Group 3: *

Alarm access

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

Select all alarms

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

Save Password Policy

Manage

New

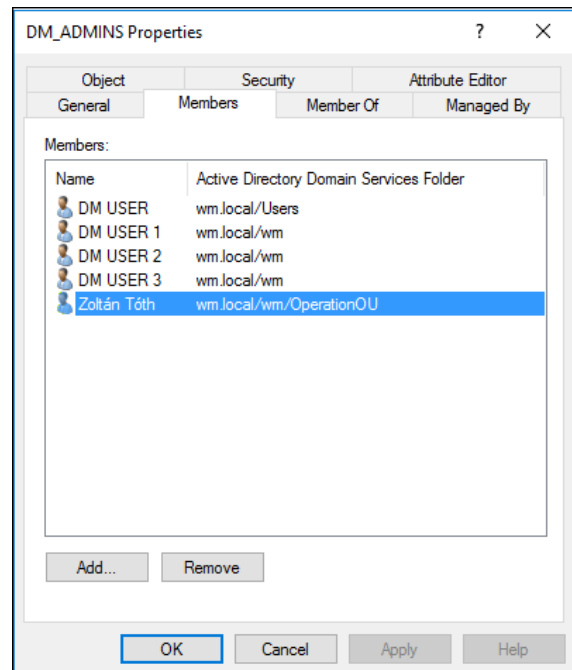
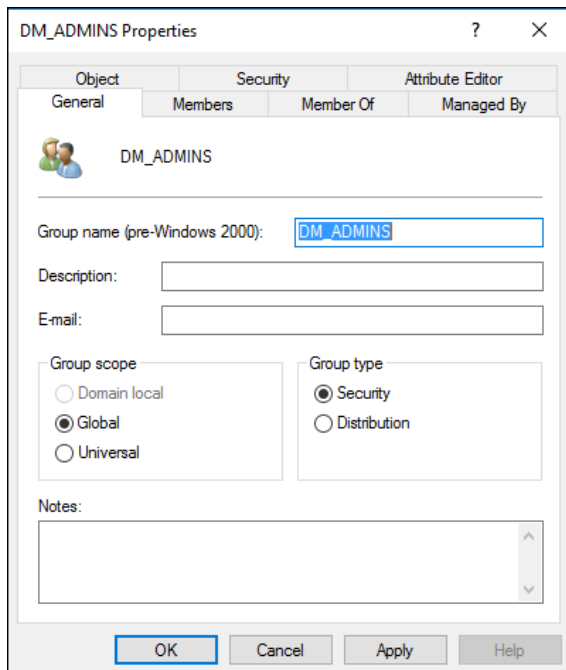
Delete

Undo

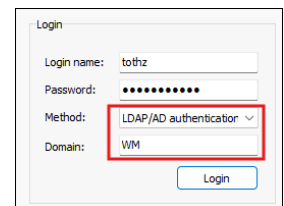
Apply

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.



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



- 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.

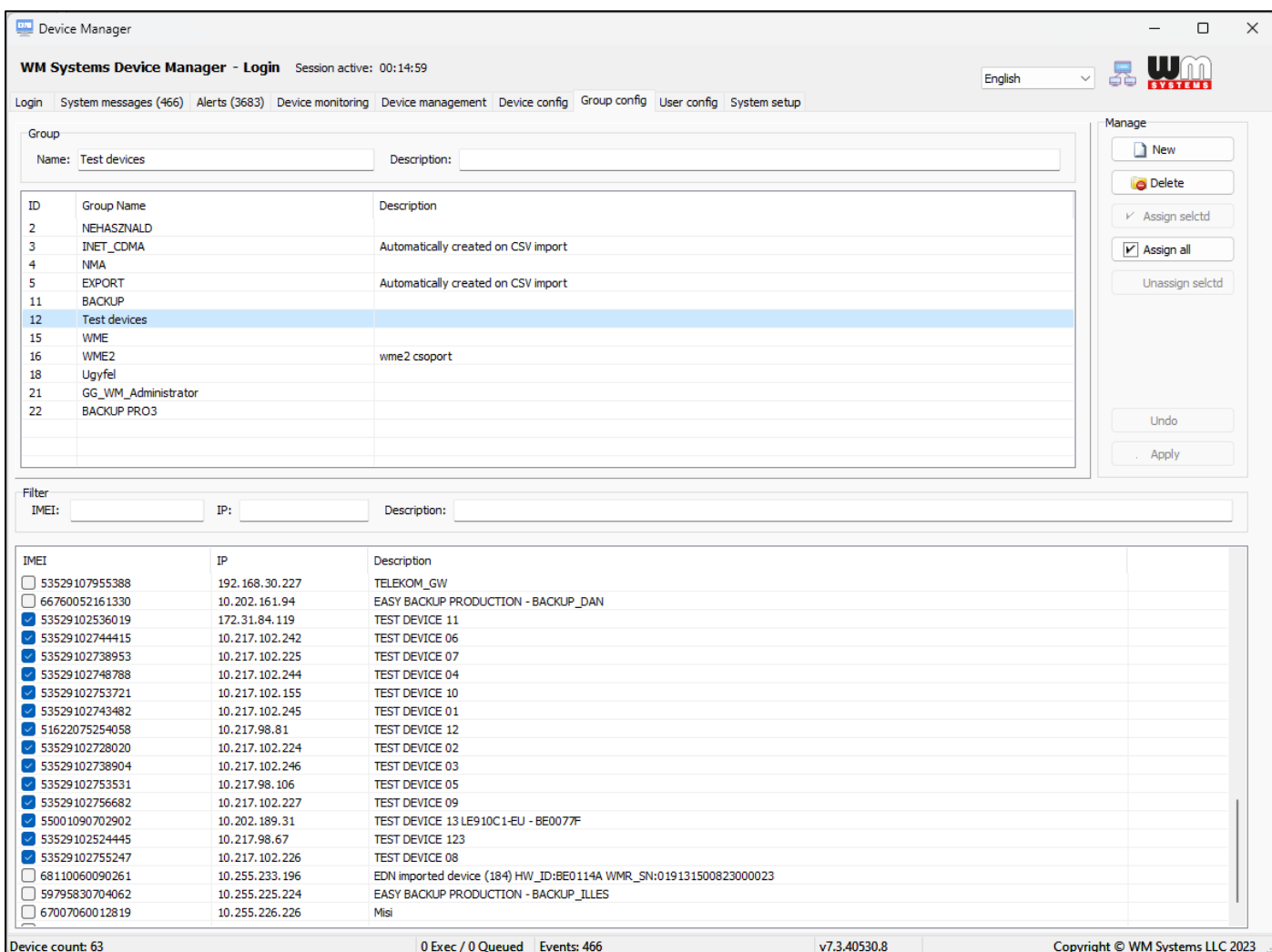
Choose a **Group name** and see the marked devices below.

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 → device 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 filled characters will be searched in entire the database

The screenshot displays the WH Systems Device Manager interface. The top section shows the 'Device config' tab for a selected device, with various settings panels including General settings, Modem settings, LAN DHCP settings, Alert settings, LAN IP settings, WAN settings, and APN settings. Below the settings is a filter bar with dropdown menus for Group, Modem, OS, HW, Zone, WDT, and Status, along with a Smart search field. The main area contains a table of devices with columns for Status, IP, MEID / IMEI, Description, RSSI / CSQ, RSRP, ECIO, Diag, Uptime, Last refresh, Modem version, OS version, HW version, Zone, FWSTM32, and wdt-cdma. The table lists various devices with their current status (Online, Never plugged in, Offline) and associated details. The bottom of the screen shows system information like 'Device count: 63', '0 Exec / 0 Queued', 'Events: 469', and 'v7.3.40530.8'.

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****.

**Reference Signals Received Power (RSRP) is a key measure of signal level and quality of the used LTE network of the router. When a mobile device moves from cell to another cell and performs cell selection/reselection and handover, it has to measure the signal strength/quality of the neighbor cells. RSRP Power is an RSSI type of measurement - the power of the LTE Reference Signals spread over the full bandwidth and narrowband.*

***EC/IO is a measure of the quality/cleanliness of the signal from the cellular tower to the internet module and indicates the signal-to noise ratio.*

The **Modem version** (router firmware 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 router.

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

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 router, 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.

Add to Firmware Upgrade Campaign Manager: Firmware Upgrade campaigns can be initiated by choosing this option. Available for routers only.

Please note, that in some Device Manager versions / configuration the following two options are also available:

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

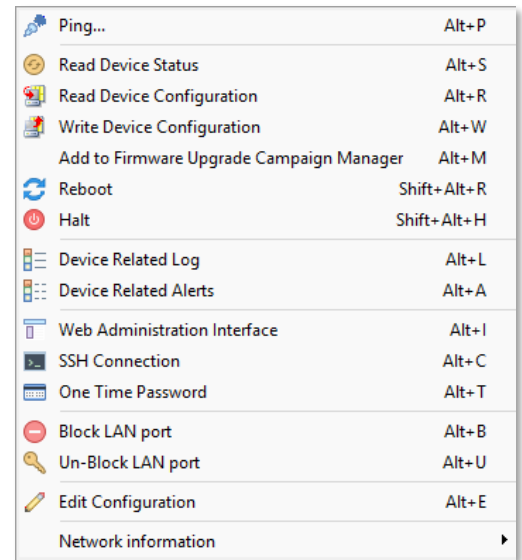
Halt: with this, you can reboot the router with a full power cycle.

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

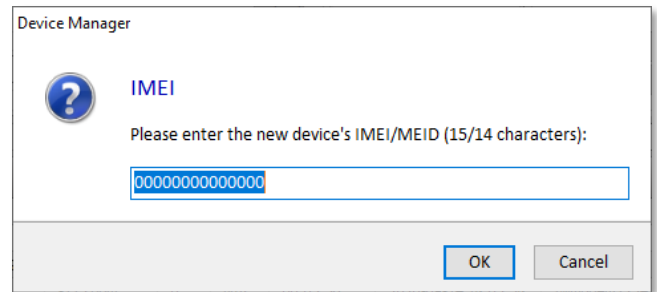
Device Related Alerts: here the screen will be redirected to the **Alerts** with filtering the selected device alerts.

Web Administration Interface: it will open the device web admin interface of the selected device in your internet browser. This function depends on the router firmware. If the firmware does not contain a web server (ex.: if the router 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



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



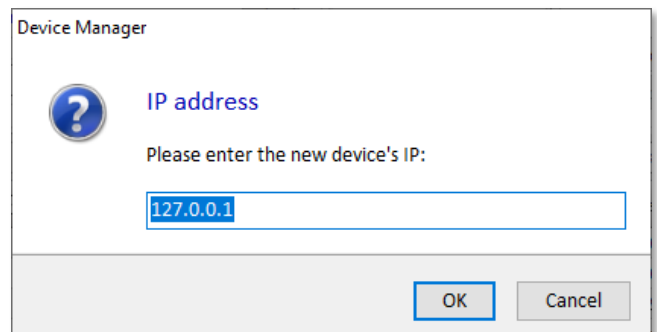
Device Manager

IMEI

Please enter the new device's IMEI/MEID (15/14 characters):

OK Cancel

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.



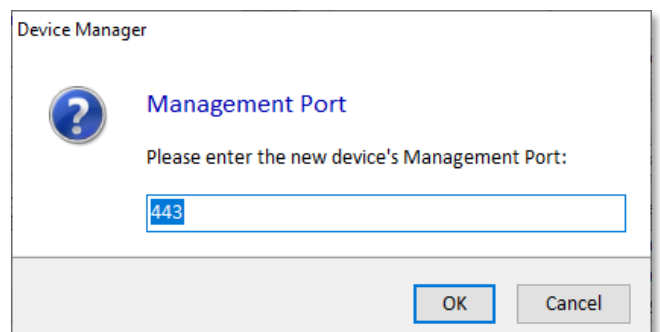
Device Manager

IP address

Please enter the new device's IP:

OK Cancel

Fill 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.



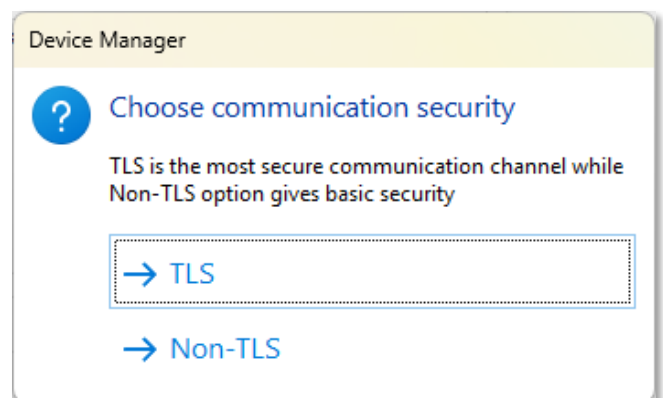
Device Manager

Management Port

Please enter the new device's Management Port:

OK Cancel

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



Device Manager

Choose communication security

TLS is the most secure communication channel while Non-TLS option gives basic security

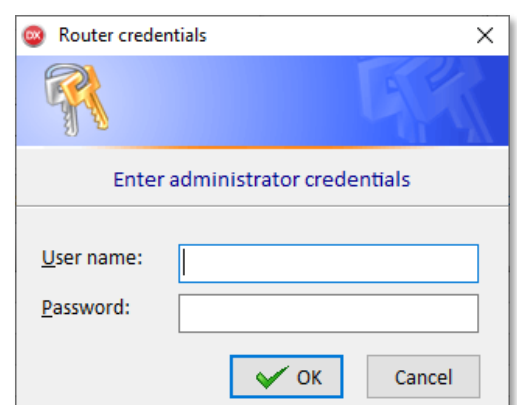
→ TLS

→ Non-TLS

Then enter the root credentials (**user name** is **root**, **password** must be unique for each device) of the router to add a new device to the DM.

IMPORTANT!

Any modification is possible only after pressing the **Apply** button.




Router credentials

Enter administrator credentials

User name:

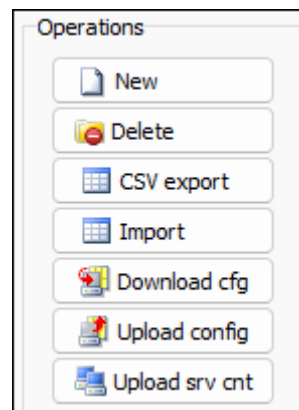
Password:

OK Cancel

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.

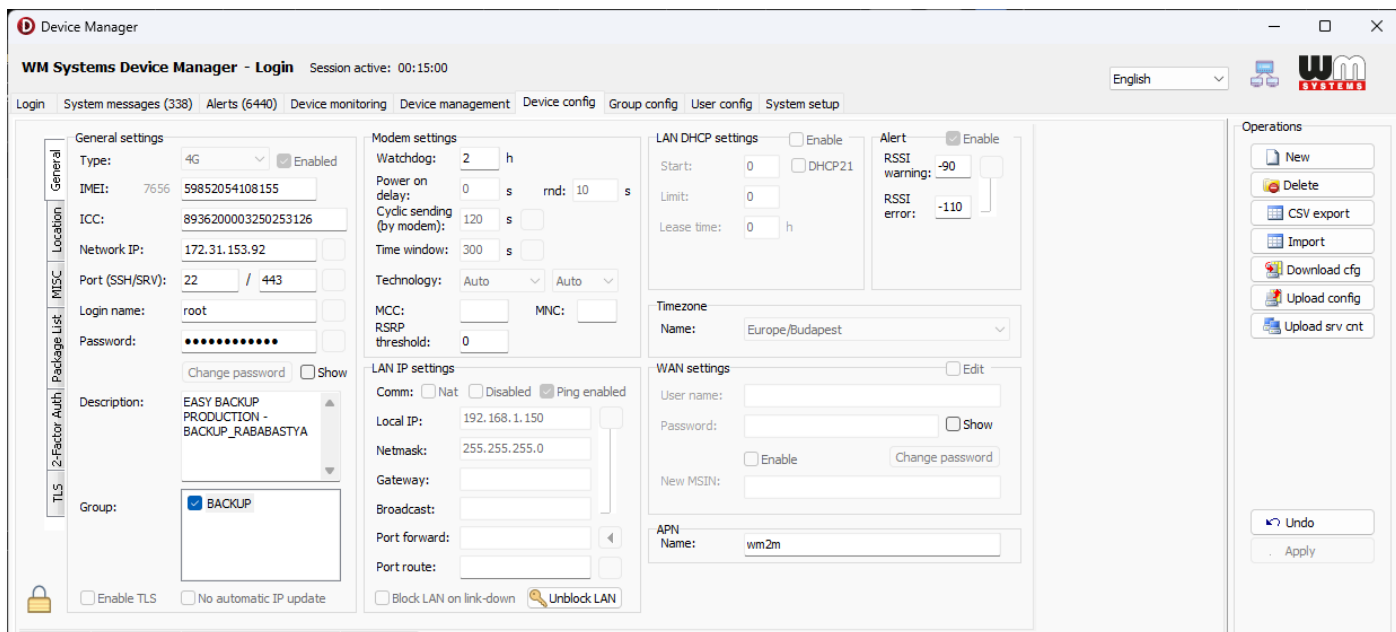
- **New:** add new devices
- **Delete:** this will delete the current / selected device(s) from the device list
- **CSV export:** export the device list with configuration data into CSV file
- **Import:** import devices with configuration into the database from CSV or XML or EDN file
- **Download cfg:** 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 **General** tab, in **General settings** part, you can get information about the device and its operation, then it will be listed here. Furthermore, you can configure some settings here.

A screenshot of the WM Systems Device Manager web interface. The main window shows the "General settings" tab for a device. The interface includes a top navigation bar with tabs like "Login", "System messages (338)", "Alerts (6440)", "Device monitoring", "Device management", "Device config", "Group config", "User config", and "System setup". The "General settings" section is divided into several panels: "General" (Type: 4G, IMEI: 59852054108155, ICC: 8936200003250253126, Network IP: 172.31.153.92, Port: 22 / 443, Login name: root, Password: [masked]), "Modem settings" (Watchdog: 2 h, Power on delay: 0 s, rmd: 10 s, Cyclic sending: 120 s, Time window: 300 s, Technology: Auto), "LAN DHCP settings" (Start: 0, Limit: 0, Lease time: 0 h), "Alert" (RSSI warning: -90, RSSI error: -110), "Timezone" (Name: Europe/Budapest), "WAN settings" (User name, Password, New MSIN), and "APN" (Name: wm2m). There are also checkboxes for "Enable TLS", "No automatic IP update", "Block LAN on link-down", and "Unblock LAN". A sidebar on the right contains the "Operations" menu.

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

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

IMEI or **MSIN** (CDMA450 router) – cellular module's unique identifier

ICC – SIM card's unique identifier

Network IP – device IP address

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

Login name – device's root account name

Password – device's unique password for login

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

Group – you can see the assigned groups

The **Modem settings** (tab) part for Internet module settings are the following:

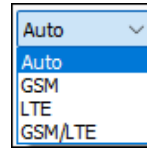
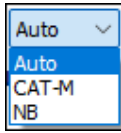
Watchdog – cellular module watchdog monitoring interval (value in hours)

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

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

Time window – timeout value between 2 periodic data

Technology – here you can select the network type and the mobile access technology.



IMPORTANT! If the cellular module or the mobile operator does not support the selected parameters, the device may be unavailable on the cellular network!

The router contains an embedded backup technology for these cases. If the device will be not able to connect to the mobile operator, the technology settings will be rolled back to the previous working settings.

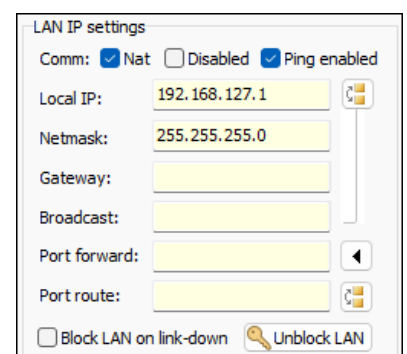
MCC and MNC – manual operator selection

RSRP threshold – RSRP level below which LED2 on the router should blink. This is helpful during installation if you see that the reception signal on the router is not good. LED2 is active on the router if the RSRP level is greater then the given value here and the WAN interface is configured and existing on the router. Sure, the router should communicate with DM. In every other case, the LED2 is blank. This is important for installers to see if its status has changed (e.g. if the device is on a cell border, it may bounce between OFF and ON, which is not good)

LAN IP settings part:

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

- **Nat:** if selected, then the router will use the NAT rules in the firewall
- **Disabled:** if selected, the LAN communication will be disabled
- **Ping enabled:** if selected, the device will answer the PING request on the LAN interface



The screenshot shows the 'LAN IP settings' configuration window. At the top, there are three radio buttons: 'Nat' (checked), 'Disabled', and 'Ping enabled' (checked). Below this, there are several input fields: 'Local IP' with the value '192.168.127.1', 'Netmask' with '255.255.255.0', 'Gateway', 'Broadcast', 'Port forward', and 'Port route'. At the bottom, there are two checkboxes: 'Block LAN on link-down' (unchecked) and 'Unblock LAN' (checked).

Netmask – IP netmask


Gateway – Gateway IP address

Broadcast – Broadcast IP address

Port forward – you can add further simple port forward rules for different device's IP behind the router

Port route – you can add direct port route rules. The selected port traffic will be forwarded to the first DHCP client's IP address.

Block LAN on link down – with this option, you can enable or disable the BlockLAN feature on the router.

 If the LAN interface is blocked, you can release the block with this button. The effect is immediate, there is no need to upload a newer configuration.

LAN DHCP settings part:

Enable – enable the DHCP service on the router

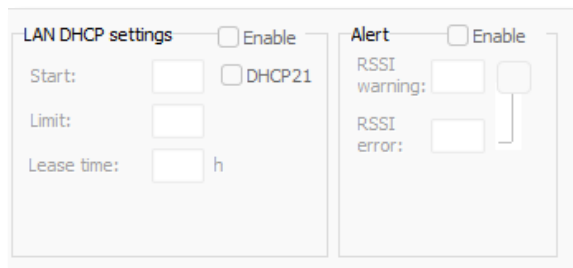
DHCP21 – you can enable the DHCP21 option.

With this option, the device (behind the router) will get the router's WAN IP address in the DHCP request.

Start – Beginning IP address

Limit – Number of max. given IP addresses

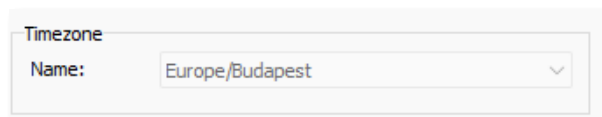
Lease time – Renewal time interval in hour



The screenshot shows the LAN DHCP settings interface. On the left, there is a section titled 'LAN DHCP settings' with an 'Enable' checkbox. Below it are three input fields: 'Start:', 'Limit:', and 'Lease time:' (with a unit 'h'). There is also a 'DHCP21' checkbox. On the right, there is an 'Alert' section with an 'Enable' checkbox. Below it are two input fields: 'RSSI warning:' and 'RSSI error:'.

Time zone part

Name – you can set the current time zone of the router



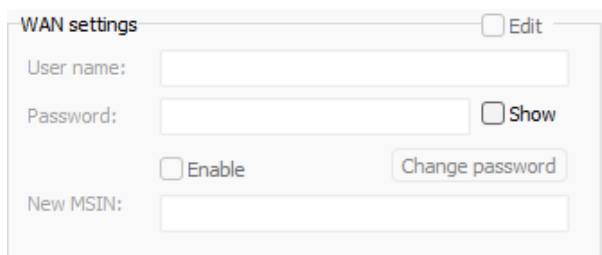
The screenshot shows the Timezone settings interface. It has a 'Timezone' label and a dropdown menu. The dropdown menu is currently set to 'Europe/Budapest'.

WAN settings part

If the APN requires **user name** and **password** for connection, you can set it here.

User name – APN or SIM user name

Password – APN or SIM password



The screenshot shows the WAN settings interface. It has a title 'WAN settings' and an 'Edit' button. There are four input fields: 'User name:', 'Password:', 'New MSIN:', and a 'Show' checkbox next to the Password field. There is also an 'Enable' checkbox and a 'Change password' button.

APN part

Name – APN name for cellular network registration



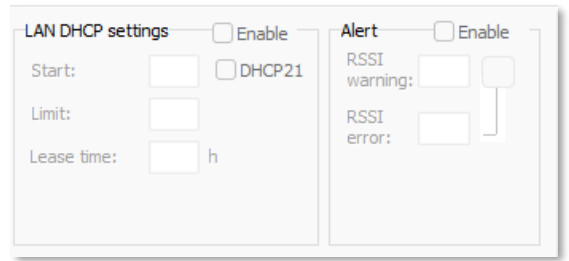
The screenshot shows the APN settings interface. It has a title 'APN' and an input field for 'Name:' which is currently set to 'wm2m'.

Alert part

Enable – you can enable the RSSI monitoring feature in the DM

RSSI warning – low cellular signal strength value

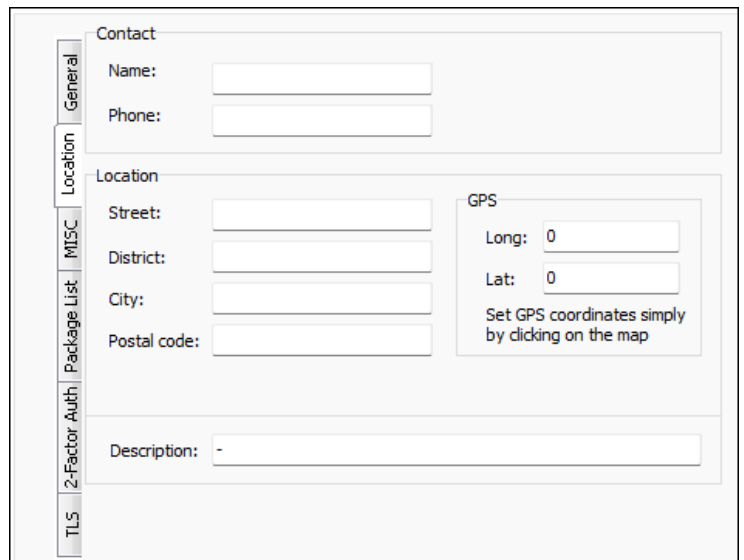
RSSI error – critical low cellular signal strength value



The screenshot shows two configuration panels. The left panel is titled 'LAN DHCP settings' and includes an 'Enable' checkbox, a 'Start' field with a 'DHCP21' checkbox, a 'Limit' field, and a 'Lease time' field with a unit 'h'. The right panel is titled 'Alert' and includes an 'Enable' checkbox, an 'RSSI warning' field with a slider, and an 'RSSI error' field with a slider.

4.5 Location settings

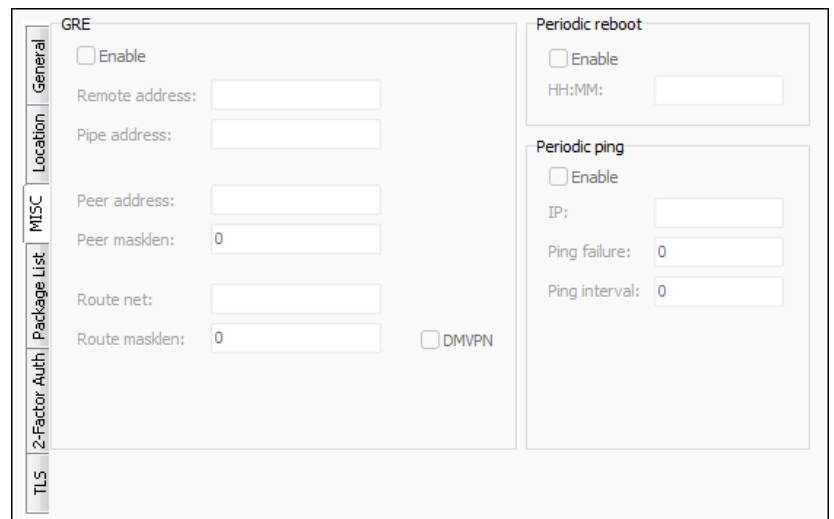
At the left **Location** tab, you can configure the device's location information (contact, address, description, etc).



The screenshot shows the 'Location' tab in a settings application. It features a vertical sidebar with tabs: General, Location, MISC, Package List, 2-Factor Auth, and TLS. The main content area is divided into sections: 'Contact' with 'Name' and 'Phone' fields; 'Location' with 'Street', 'District', 'City', and 'Postal code' fields; 'GPS' with 'Long' and 'Lat' fields and a note 'Set GPS coordinates simply by clicking on the map'; and 'Description' with a text area.

4.6 Miscellaneous settings

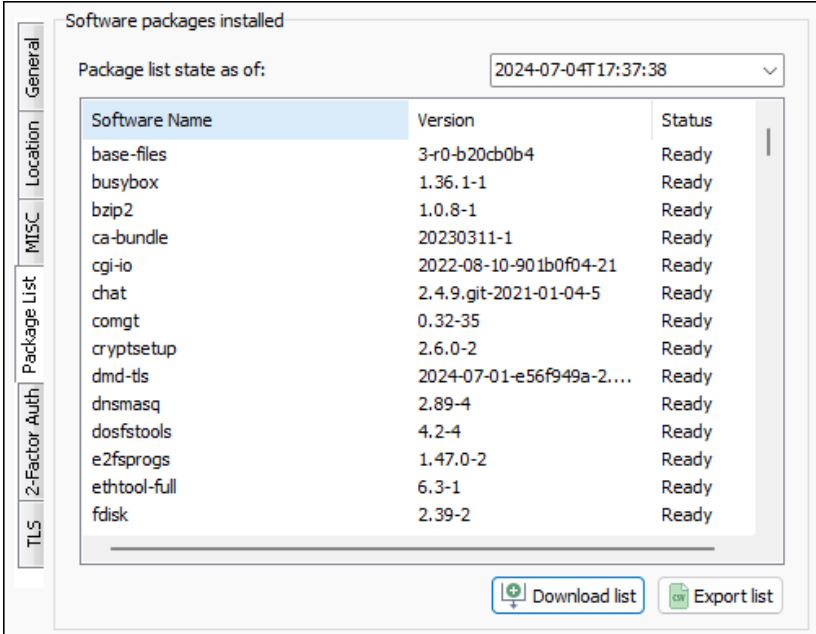
The **MISC** tab will allow you to use GRE or apply **Periodic reboot**, **Periodic ping** features on the device. Currently, these parameters are not implemented in the router's firmware and in the application.



The screenshot shows the 'MISC' tab in a settings application. It features a vertical sidebar with tabs: General, Location, MISC, Package List, 2-Factor Auth, and TLS. The main content area is divided into sections: 'GRE' with an 'Enable' checkbox, 'Remote address', 'Pipe address', 'Peer address', 'Peer masklen', 'Route net', 'Route masklen', and a 'DMVPN' checkbox; 'Periodic reboot' with an 'Enable' checkbox and 'HH:MM' field; and 'Periodic ping' with an 'Enable' checkbox, 'IP', 'Ping failure', and 'Ping interval' fields.

4.7 Package List

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



Software packages installed

Package list state as of: 2024-07-04T17:37:38

Software Name	Version	Status
base-files	3-r0-b20cb0b4	Ready
busybox	1.36.1-1	Ready
bzip2	1.0.8-1	Ready
ca-bundle	20230311-1	Ready
cgi-io	2022-08-10-901b0f04-21	Ready
chat	2.4.9.git-2021-01-04-5	Ready
comgt	0.32-35	Ready
cryptsetup	2.6.0-2	Ready
dmd-tls	2024-07-01-e56f949a-2...	Ready
dnsmasq	2.89-4	Ready
dosfstools	4.2-4	Ready
e2fsprogs	1.47.0-2	Ready
ethtool-full	6.3-1	Ready
fdisk	2.39-2	Ready

Download list Export list

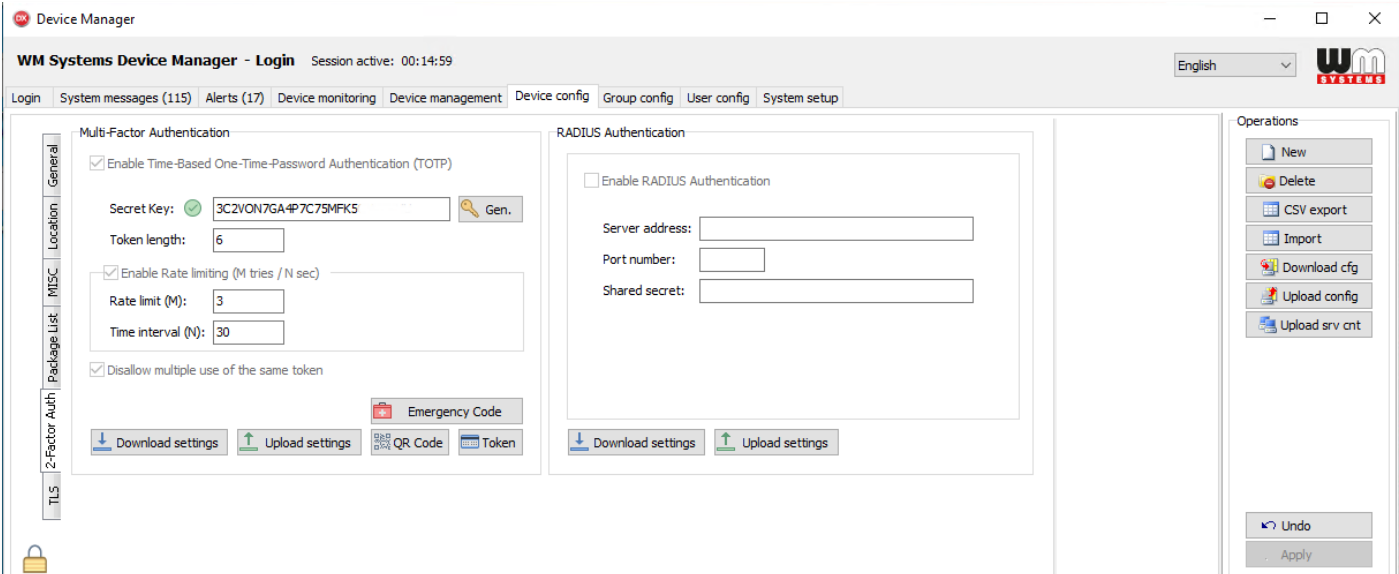
4.8 Two-Factor Authentication settings

These parameters are not implemented in the router current firmware and in the application.

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**, and **Time interval** fields.

Here you can select the **Download settings** or **Upload settings** button for an easier configuration.



Device Manager

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

English

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

Multi-Factor Authentication

Enable Time-Based One-Time-Password Authentication (TOTP)

Secret Key: Gen.

Token length:

Enable Rate limiting (M tries / N sec)

Rate limit (M):

Time interval (N):

Disallow multiple use of the same token

Emergency Code

Download settings Upload settings QR Code Token

RADIUS Authentication

Enable RADIUS Authentication

Server address:

Port number:

Shared secret:

Download settings Upload settings

Operations

New Delete CSV export Import Download cfg Upload cfg Upload srv cnt

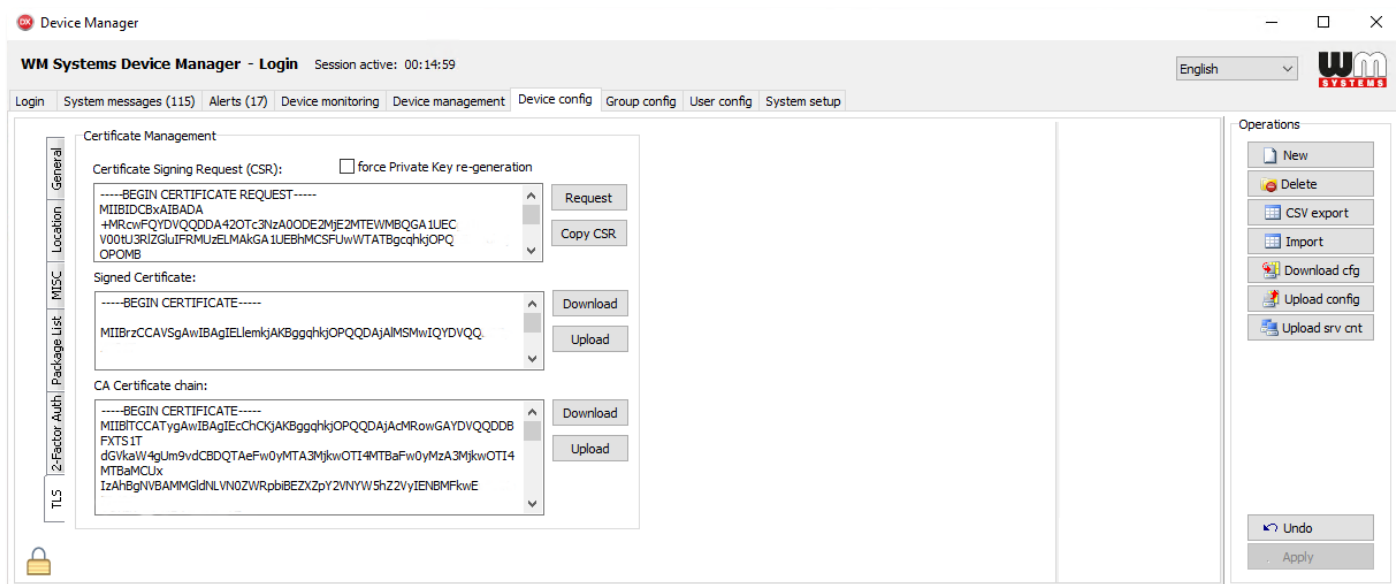
Undo Apply

The **RADIUS Authentication** feature can be configured here. For that, fill **Server address** (of Radius server), **Port number** (of the server), and **Shared secret key** fields to provide a safe connection.

4.9 TLS settings

At **TLS** tab, you can configure a TLS v1.2 protocol-compatible communication for router(s). Then device(s) will communicate with Device Manager software via TLS.

These parameters are not implemented in current firmware of router 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 the **Certificate Signing Request (CSR)** you can **Request** the CSR file, or you can choose the **Copy CSR** button.

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

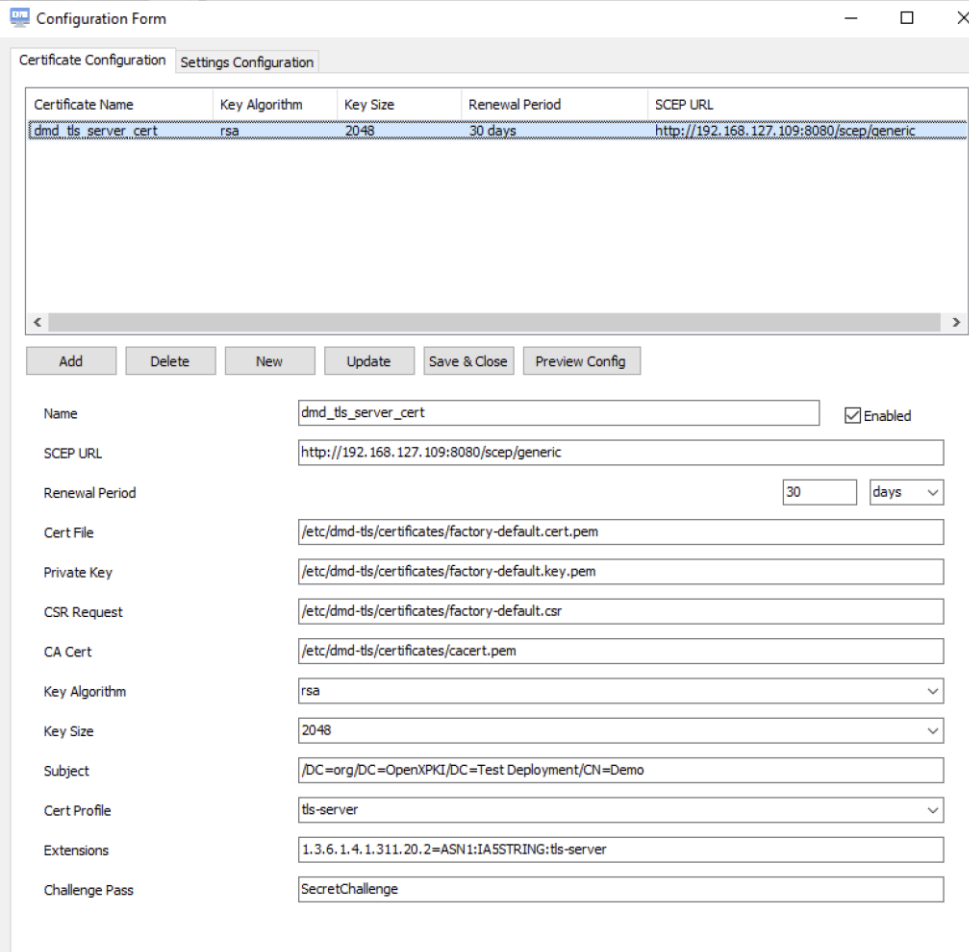
The **CA Certificate chain** can be requested to **Download** or you can **Upload** one.

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

4.10 SCEP config

Automated Certificate Renewal via SCEP Protocol - Configuration

Overview



The screenshot shows a web-based configuration form titled "Certificate Configuration" with two tabs: "Certificate Configuration" and "Settings Configuration". The "Certificate Configuration" tab is active, displaying a table with the following data:

Certificate Name	Key Algorithm	Key Size	Renewal Period	SCEP URL
dmd_tls_server_cert	rsa	2048	30 days	http://192.168.127.109:8080/scep/generic

Below the table are several buttons: Add, Delete, New, Update, Save & Close, and Preview Config. The "Add" button is highlighted. Below the buttons is a detailed configuration form for the selected certificate, "dmd_tls_server_cert". The form includes the following fields:

- Name: dmd_tls_server_cert (with an "Enabled" checkbox)
- SCEP URL: http://192.168.127.109:8080/scep/generic
- Renewal Period: 30 days (with a dropdown menu)
- Cert File: /etc/dmd-tls/certificates/factory-default.cert.pem
- Private Key: /etc/dmd-tls/certificates/factory-default.key.pem
- CSR Request: /etc/dmd-tls/certificates/factory-default.csr
- CA Cert: /etc/dmd-tls/certificates/cacert.pem
- Key Algorithm: rsa (with a dropdown menu)
- Key Size: 2048 (with a dropdown menu)
- Subject: /DC=org/DC=OpenXPKI/DC=Test Deployment/CN=Demo
- Cert Profile: tls-server (with a dropdown menu)
- Extensions: 1.3.6.1.4.1.311.20.2=ASN1:IA5STRING:tls-server
- Challenge Pass: SecretChallenge

The configuration form is used to set up and manage automated certificate renewal using the Simple Certificate Enrollment Protocol (SCEP).

Certificate Configuration Tab

This tab allows users to manage certificates for automated renewal.

1. Certificate List

- Displays the list of configured certificates.
- Shows details such as Certificate Name, Key Algorithm, Key Size, Renewal Period, and SCEP URL.

2. Buttons

- **Add:** Adds a new certificate configuration.
- **Delete:** Removes the selected certificate configuration.

- **New:** Clears the form for a new certificate configuration.
- **Update:** Updates the selected certificate configuration with the current form details.
- **Save & Close:** Saves all configurations and closes the form.
- **Preview Config:** Previews the current configuration settings.

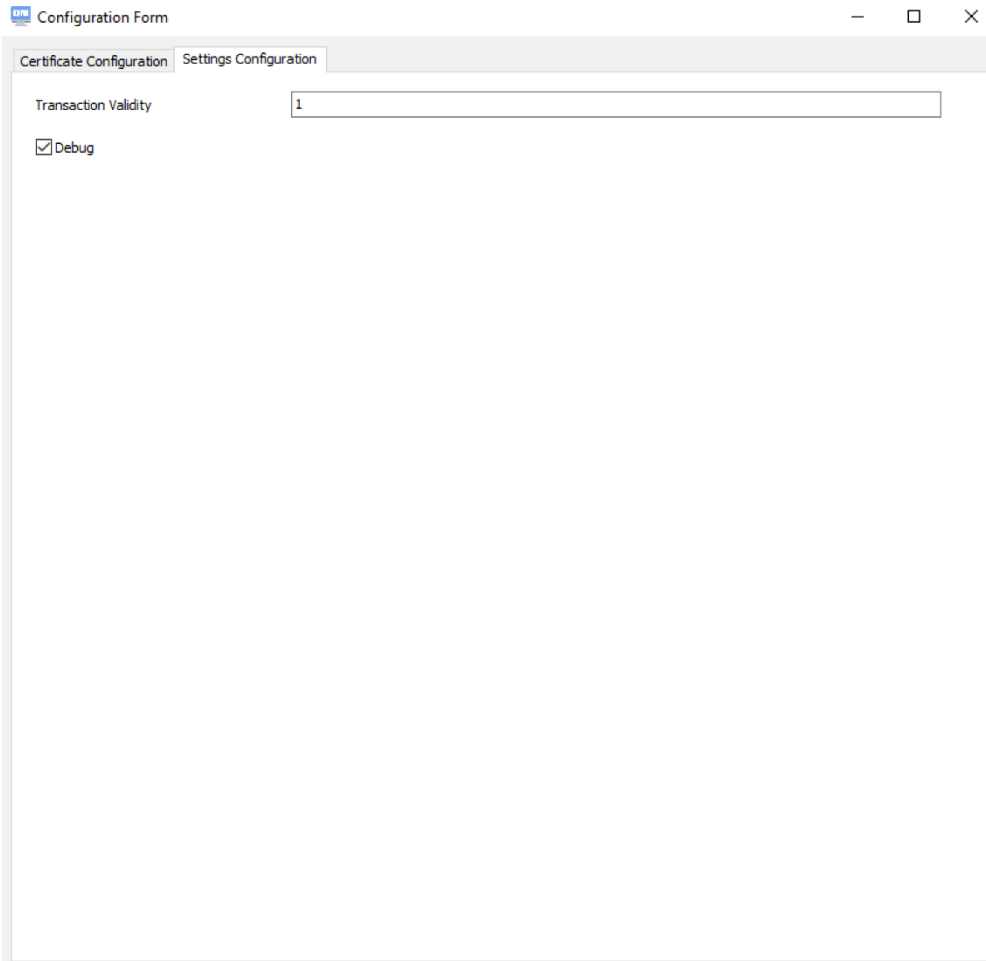
3. Certificate Details Section

- **Enabled:** Checkbox to enable or disable the certificate configuration.
- **Name:** Name of the certificate configuration.
- **SCEP URL:** URL for the SCEP server.
- **Renewal Period:** Period (in days) for certificate renewal. 0 indicates no renewal.
- **Cert File:** Path to the certificate file.
- **Private Key:** Path to the private key file.
- **CSR Request:** Path to the CSR (Certificate Signing Request) file.
- **CA Cert:** Path to the CA (Certificate Authority) certificate file.
- **Key Algorithm:** Algorithm used for the key (e.g., RSA).
- **Key Size:** Size of the key (e.g., 2048 bits).
- **Subject:** Distinguished name fields for the certificate subject.
- **Cert Profile:** Profile to be used for the certificate.
- **Extensions:** Extensions for the certificate.
- **Challenge Pass:** Challenge password for the SCEP enrollment.

Example Configuration

- **Name:** dmd_tls_server_cert
- **SCEP URL:** http://192.168.127.109:8080/scep/generic
- **Renewal Period:** 30 days
- **Cert File:** /etc/dmd-tls/certificates/factory-default.cert.pem
- **Private Key:** /etc/dmd-tls/certificates/factory-default.key.pem
- **CSR Request:** /etc/dmd-tls/certificates/factory-default.csr
- **CA Cert:** /etc/dmd-tls/certificates/cacert.pem

- **Key Algorithm:** rsa
- **Key Size:** 2048
- **Subject:** /DC=org/DC=OpenXPKI/DC=Test Deployment/CN=Demo
- **Cert Profile:** tls-server
- **Extensions:** 1.3.6.1.4.1.311.20.2=ASN1:IA5STRING:tls-server
- **Challenge Pass:** *(Optional)*



The screenshot shows a window titled "Configuration Form" with two tabs: "Certificate Configuration" and "Settings Configuration". The "Settings Configuration" tab is active. It contains a "Transaction Validity" field with the value "1" and a checked "Debug" checkbox.

Settings Configuration Tab

This tab allows users to configure general settings related to the certificate renewal transactions.

1. Transaction Validity

- Defines the validity period for transactions in days.
- Example: 1 days

2. Debug

- Checkbox to enable or disable debugging mode. Debugging mode helps with more verbose logging

Automated Renewal Process

The Certificate Renewal procedure is executed by the **M2M Secure Router** and the **Public Key Infrastructure** (PKI) system.

A certificate renewal process is run by an automated crontab task in the background, which executes every 5 minutes. According to the given configuration, this task performs the following actions:

1. Certificate Validity Check

- The task checks the validity of all configured certificates.
- It determines if any certificate is approaching its expiration date.

2. Renewal Action

- If a certificate's expiration date is sooner than the configured renewal period and the renewal is enabled for it, the task initiates the renewal process.
- This ensures that the certificate is renewed well before it expires, maintaining continuous secure operations.

3. Multiple Certificates Management

- This feature supports renewing multiple certificates, not just a single one.
- The crontab task iterates through the list of configured certificates and renews any that meet the criteria for renewal.

By leveraging this automated process, users can ensure that all their certificates remain valid and up-to-date, reducing the risk of service interruptions due to expired certificates.

Steps for Configuration

1. Adding a New Certificate Configuration

- Click on the **New** button to clear the form.
- Fill in the details in the **Certificate Details Section**.
- Click **Add** to add the configuration to the list.

2. Updating an Existing Certificate Configuration

- Select the certificate from the list.
 - Modify the details in the **Certificate Details Section**.
 - Click **Update** to save the changes.
3. **Deleting a Certificate Configuration**
 - Select the certificate from the list.
 - Click **Delete** to remove the configuration.
 4. **Saving and Closing the Configuration**
 - Click **Save & Close** to save all configurations and close the form.
 5. **Previewing the Configuration**
 - Click **Preview Config** to preview the current settings.
 6. **Configuring General Settings**
 - Navigate to the **Settings Configuration** tab.
 - Set the **Transaction Validity**.
 - Enable or disable **Debug** mode as needed.

4.11 Firewall config

M2M Secure Router's Firewall Configuration

The following description provides detailed instructions for configuring the firewall rules on an M2M Secure Router using the Device Manager's graphical user interface. The firewall utilizes Linux's iptables and follows the OpenWRT firewall logic, managing traffic between LAN and WAN zones.

Firewall Configuration Overview

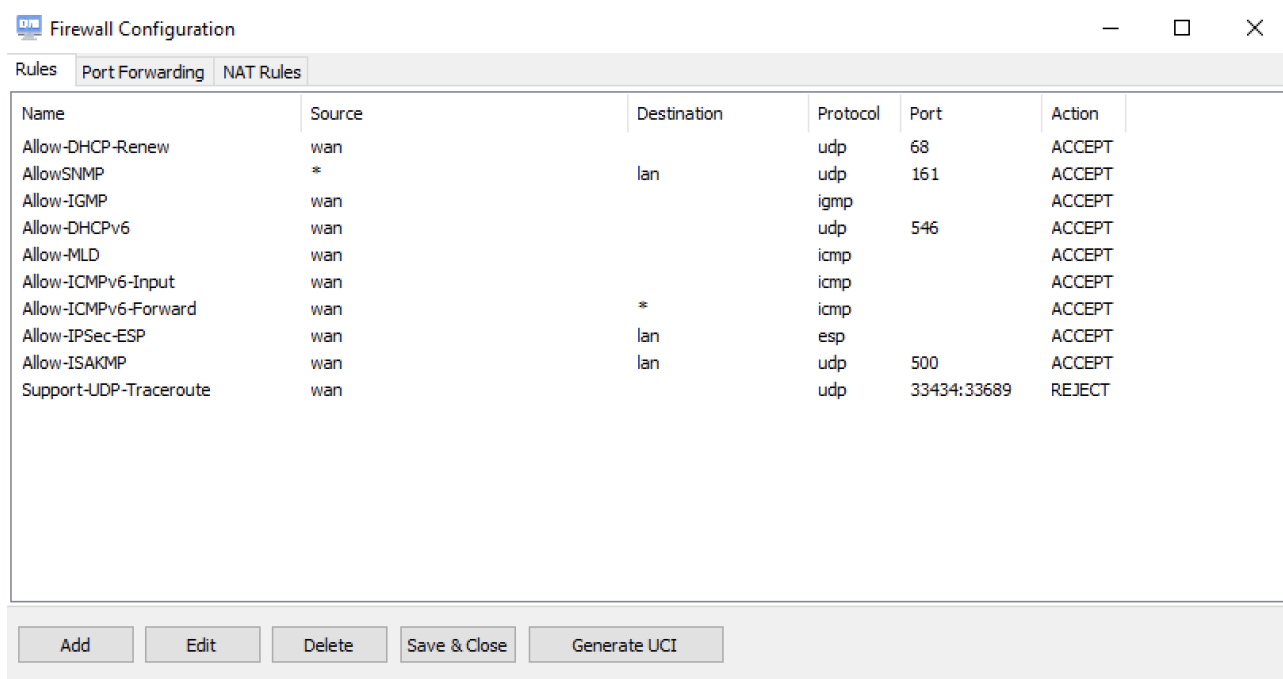
The Firewall Configuration interface allows users to define rules for managing network traffic, port forwarding, and NAT (Network Address Translation).

The main sections include:

1. **Rules**
2. **Port Forwarding**
3. **NAT Rules**

Each section includes options to add, edit, and delete rules. The configurations can be saved and applied using the "Save & Close" button.

Rules Tab



Name	Source	Destination	Protocol	Port	Action
Allow-DHCP-Renew	wan		udp	68	ACCEPT
AllowSNMP	*	lan	udp	161	ACCEPT
Allow-IGMP	wan		igmp		ACCEPT
Allow-DHCPv6	wan		udp	546	ACCEPT
Allow-MLD	wan		icmp		ACCEPT
Allow-ICMPv6-Input	wan		icmp		ACCEPT
Allow-ICMPv6-Forward	wan	*	icmp		ACCEPT
Allow-IPSec-ESP	wan	lan	esp		ACCEPT
Allow-ISAKMP	wan	lan	udp	500	ACCEPT
Support-UDP-Traceroute	wan		udp	33434:33689	REJECT

This tab is used to configure general firewall rules that determine how traffic is managed between the LAN and WAN zones.

1. Firewall Rules List

- Displays a list of currently configured rules with details such as Name, Source, Destination, Protocol, Port, and Action.

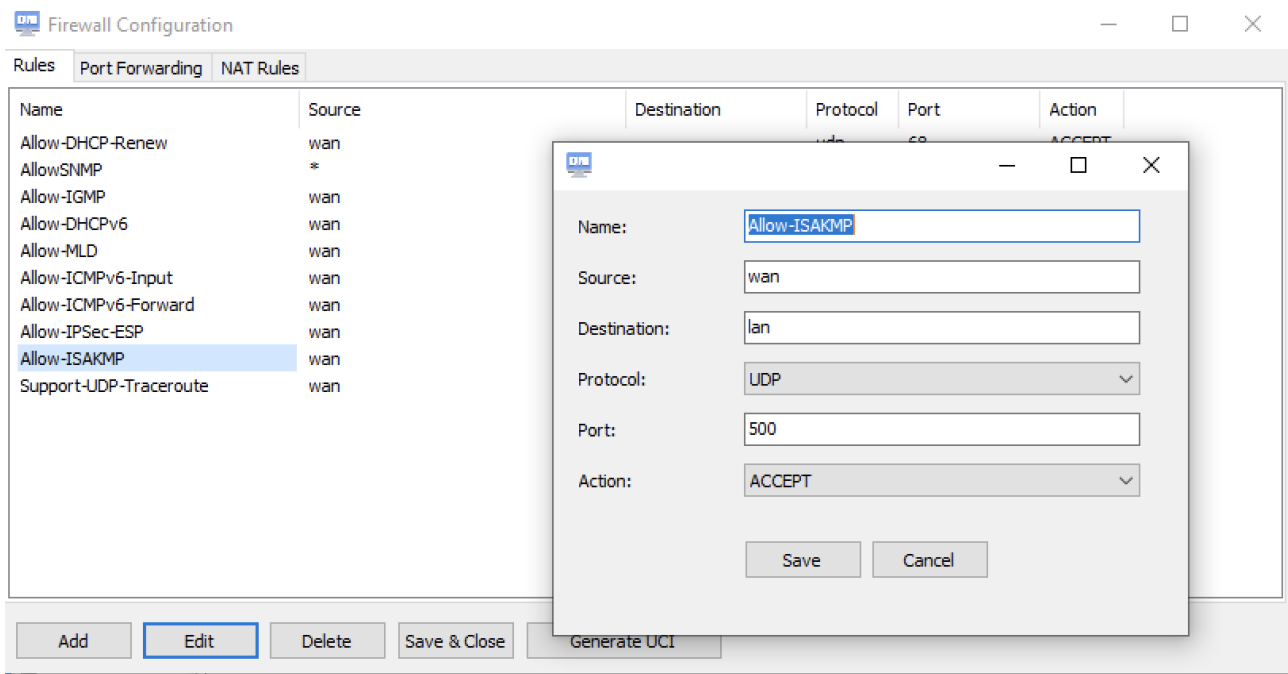
2. Buttons

- **Add:** Opens a dialog to create a new firewall rule.
- **Edit:** Opens the selected rule for editing.
- **Delete:** Removes the selected rule.
- **Save & Close:** Saves the current configuration and closes the interface.
- **Generate UCI:** Generates UCI (Unified Configuration Interface) commands based on the current configuration.

3. Adding/Editing a Rule

- **Name:** A descriptive name for the rule.
- **Source:** The source zone/interface (e.g., wan).

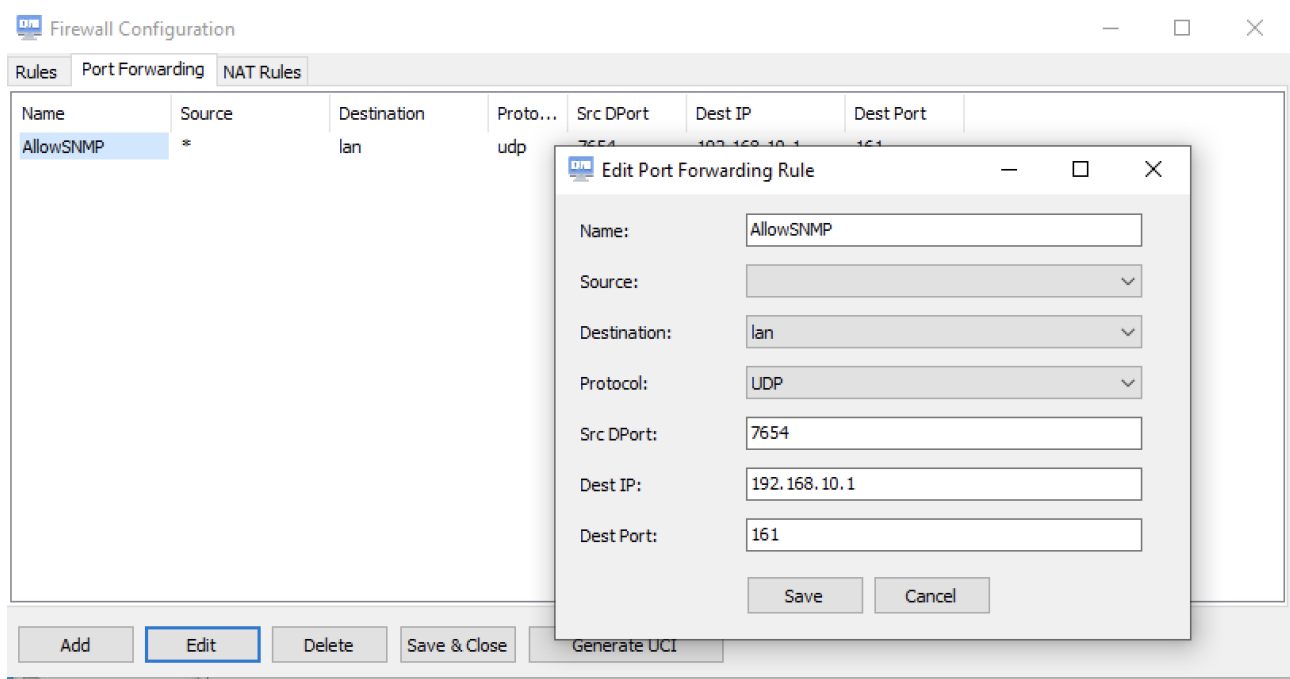
- **Destination:** The destination zone/interface (e.g., lan).
- **Protocol:** The protocol used (e.g., UDP, TCP).
- **Port:** The port number or range.
- **Action:** The action to be taken (e.g., ACCEPT, REJECT).



4. Example Configuration:

- **Name:** Allow-ISAKMP
- **Source:** wan
- **Destination:** lan
- **Protocol:** UDP
- **Port:** 500
- **Action:** ACCEPT

Port Forwarding Tab



This tab is used to configure port forwarding rules, which redirect traffic from the WAN to specific devices on the LAN.

1. Port Forwarding Rules List

- Displays a list of port forwarding rules with details such as Name, Source, Destination, Protocol, Source Port, Destination IP, and Destination Port.

2. Buttons

- **Add:** Opens a dialog to create a new port forwarding rule.
- **Edit:** Opens the selected rule for editing.
- **Delete:** Removes the selected rule.
- **Save & Close:** Saves the current configuration and closes the interface.

3. Adding/Editing a Port Forwarding Rule

- **Name:** A descriptive name for the rule.
- **Source:** The source zone/interface.
- **Destination:** The destination zone/interface.

- **Protocol:** The protocol used (e.g., UDP, TCP).
- **Src DPort:** The source port number.
- **Dest IP:** The destination IP address on the LAN.
- **Dest Port:** The destination port number.

Example Configuration:

- **Name:** AllowSNMP
- **Source:** *
- **Destination:** lan
- **Protocol:** UDP
- **Src DPort:** 7654
- **Dest IP:** 192.168.10.1
- **Dest Port:** 161

NAT Rules Tab

Firewall Configuration

Rules | Port Forwarding | NAT Rules

Name	Proto...	Outbound Zone	Source Address	Sour...	Destination Add...	Desti...	Action	Rewrite IP Addr...
SNAT1-no dst ip	Any	lan	192.168.127.109				MASQUERADE	
AllowSNMP	UDP	*		123		161	ACCEPT	

This tab is used to configure NAT (Network Address Translation) rules, including Source NAT (SNAT) and Destination NAT (DNAT).

1. NAT Rules List

- Displays a list of NAT rules with details such as Name, Protocol, Outbound Zone, Source Address, Source Port, Destination Address, Destination Port, Action, and Rewrite IP Address.

2. Buttons

- **Add:** Opens a dialog to create a new NAT rule.
- **Edit:** Opens the selected rule for editing.
- **Delete:** Removes the selected rule.
- **Save & Close:** Saves the current configuration and closes the interface.

3. Adding/Editing a NAT Rule

- **General Settings**
 - **Name:** A descriptive name for the rule.
 - **Protocol:** The protocol used (e.g., Any, UDP, TCP).
 - **Outbound Zone:** The outbound zone/interface.
 - **Source Address:** The source IP address.
 - **Source Port:** The source port number.
 - **Destination Address:** The destination IP address.
 - **Destination Port:** The destination port number.
 - **Action:** The action to be taken (e.g., MASQUERADE).
 - **Rewrite IP Address:** The IP address to rewrite (if applicable).
 - **Rewrite Port:** The port to rewrite (if applicable).

Firewall - NAT Rules - SNAT Rule Edit

General Settings | Advanced Settings | Time Restrictions

Name: SNAT1-no dst ip

Protocol: Any

Outbound zone: lan

Source address: 192.168.127.109 (00:E0:4C:68:2D:AE)

Source port:

Destination address:

Destination port:

Action: MASQUERADE - Automatically rewrite to outbo

Rewrite IP address:

Rewrite port:

Save Dismiss

Example Configuration:

- **Name:** SNAT - no dst ip
- **Protocol:** Any
- **Outbound Zone:** lan
- **Source Address:** 192.168.127.109
- **Action:** MASQUERADE
- **Advanced Settings**
 - **Outbound Device:** The outbound device (e.g., 4g-wan).
 - **Match Mark:** The match mark for traffic.
 - **Limit Matching:** The limit for matching traffic (e.g., 10/second).
 - **Limit Burst:** The limit burst value.

- **Extra Arguments:** Any extra arguments for the rule.

Firewall - NAT Rules - SNAT Rule Edit

General Settings | **Advanced Settings** | Time Restrictions

Outbound device: 4g-wan

Match mark:

Limit matching: 10/second

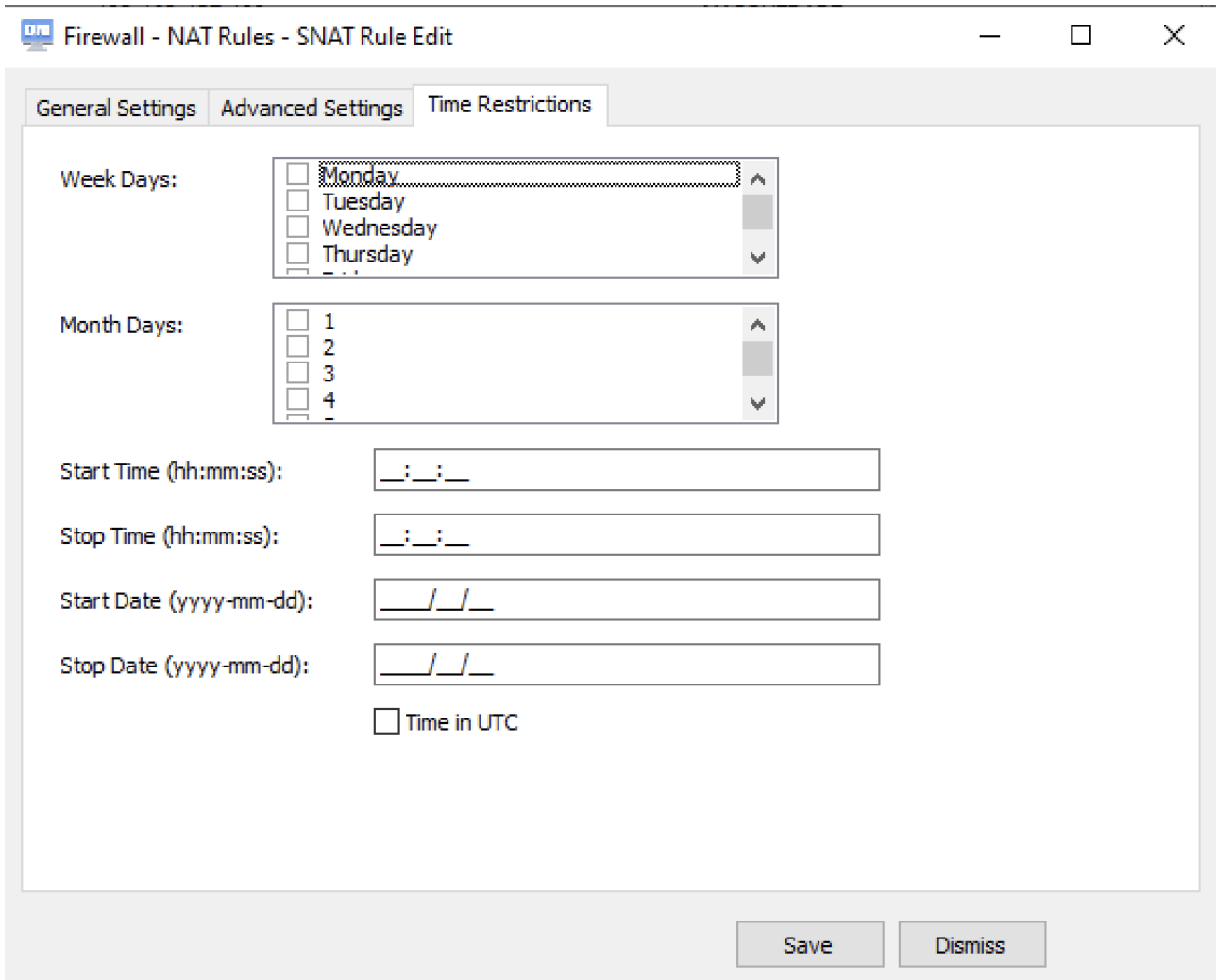
Limit burst:

Extra arguments:

Save Dismiss

- **Time Restrictions**

- **Week Days:** Days of the week the rule is active.
- **Month Days:** Days of the month the rule is active.
- **Start Time:** The start time (hh:mm:ss) for the rule.
- **Stop Time:** The stop time (hh:mm:ss) for the rule.
- **Start Date:** The start date (yyyy-mm-dd) for the rule.
- **Stop Date:** The stop date (yyyy-mm-dd) for the rule.
- **Time in UTC:** Checkbox to use UTC time.



By following these instructions, users can effectively configure the firewall rules of their M2M Secure Router with the help of the Device Manager, to manage and secure network traffic according to their specific needs.

4.12 SYSLOG config

Configuring the M2M Secure Router's Syslog Client

The syslog client can be configured to parse specific system log message patterns and send syslog formatted messages to a specified syslog server.

Syslog Configuration Tab

The Syslog Configuration tab allows users to define patterns for system log messages and configure how these messages are sent to a syslog server.

The screenshot shows a web application window titled "Syslog Configuration Form". At the top, there is a table with two columns: "Pattern" and "Severity". The first row contains the text "bad password" under "Pattern" and "LOG_ALERT" under "Severity". Below the table is a row of six buttons: "Add", "Delete", "New", "Update", "Save & Close", and "Preview Config". Underneath the buttons is a form with five fields: "Pattern" (text input with "bad password"), "Severity" (dropdown menu with "LOG_ALERT"), "Server" (text input with "192.168.127.2"), "Port" (text input with "514"), and "Protocol" (dropdown menu with "udp").

Pattern	Severity
bad password	LOG_ALERT

Add **Delete** **New** **Update** **Save & Close** **Preview Config**

Pattern: bad password
Severity: LOG_ALERT
Server: 192.168.127.2
Port: 514
Protocol: udp

Syslog Configuration List

- Displays a list of configured syslog message patterns.
- Shows details such as Pattern and Severity.

Buttons

- **Add:** Adds a new syslog message pattern with the current form details.
- **Delete:** Removes the selected syslog message pattern.
- **New:** Clears the form for entering a new syslog message pattern.
- **Update:** Updates the selected syslog message pattern with the current form details.
- **Save & Close:** Saves all configurations and closes the form.
- **Preview Config:** Previews the current configuration settings.

Pattern Details Section

- **Pattern:** The specific log message pattern to match. This can be a regular expression (regex).
- **Severity:** The severity level of the log message (e.g., LOG_ALERT).
- **Server:** The IP address or hostname of the syslog server.
- **Port:** The port number of the syslog server (e.g., 514).
- **Protocol:** The protocol used to send messages (e.g., TCP or UDP).

Example Configuration

- **Pattern:** bad password
- **Severity:** LOG_ALERT
- **Server:** 192.168.127.2
- **Port:** 514
- **Protocol:** udp

Steps for Configuration :

1. Adding a New Syslog Message Pattern

- Click on the **New** button to clear the form.
- Fill in the details in the **Pattern Details Section:**
 - **Pattern:** Enter the log message pattern (e.g., bad password).
 - **Severity:** Select the severity level from the dropdown (e.g., LOG_ALERT).
 - **Server:** Enter the IP address or hostname of the syslog server (e.g., 192.168.127.2).
 - **Port:** Enter the port number of the syslog server (e.g., 514).
 - **Protocol:** Select the protocol (e.g., udp).
- Click **Add** to add the configuration to the list.

2. **Updating an Existing Syslog Message Pattern**

- Select the pattern from the list.
- Modify the details in the **Pattern Details Section**.
- Click **Update** to save the changes.

3. **Deleting a Syslog Message Pattern**

- Select the pattern from the list.
- Click **Delete** to remove the configuration.

4. **Saving and Closing the Configuration**

- Click **Save & Close** to save all configurations and close the form.

5. **Previewing the Configuration**

- Click **Preview Config** to preview the current settings.

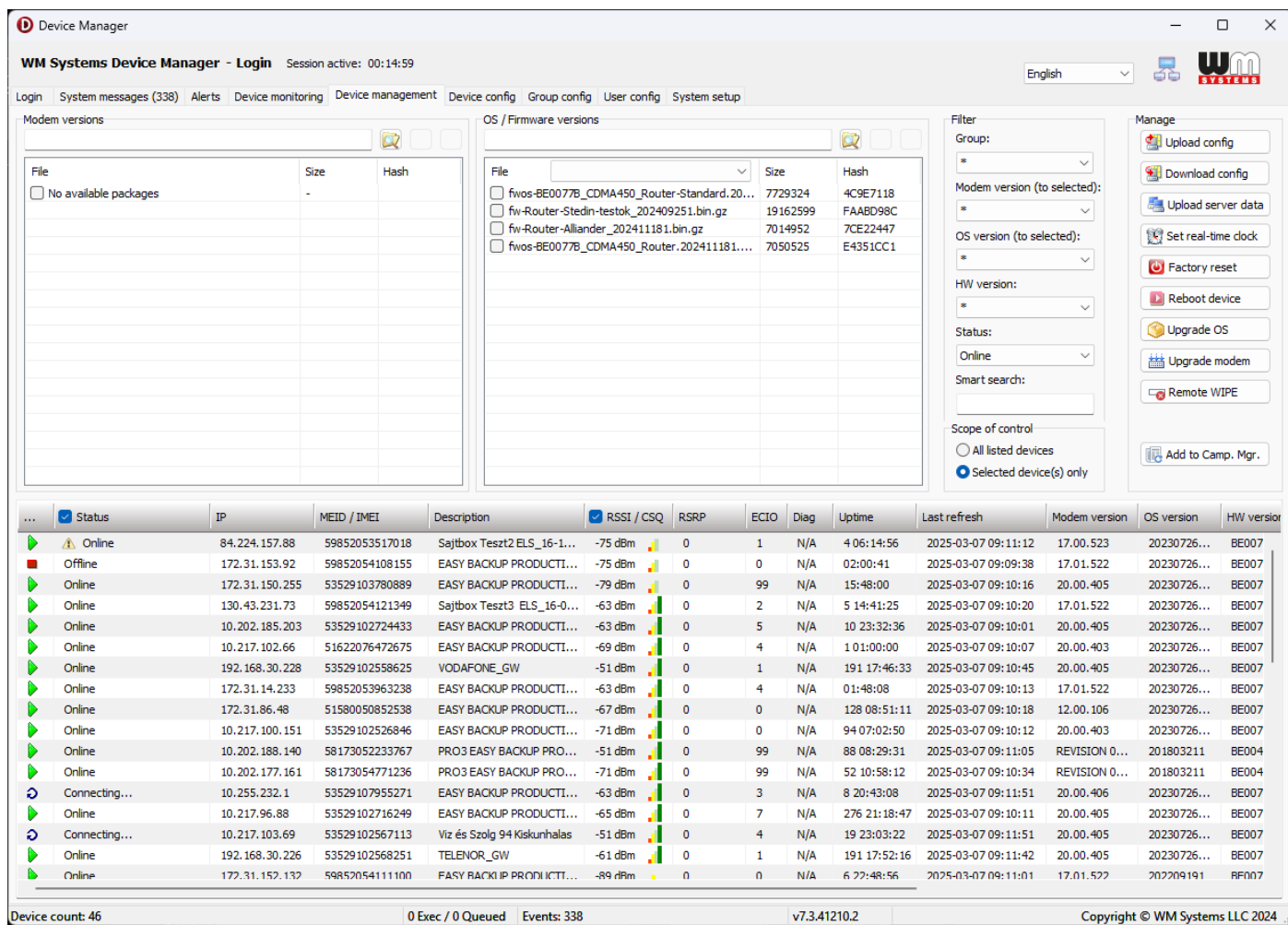
How It Works

- The syslog_client daemon runs on the M2M Secure Router, continuously monitoring system logs.
- It parses the logs based on the configured message patterns.
- If a log message matches a configured pattern (using regex matching), the daemon formats the message according to the syslog standard.
- The formatted syslog message is then sent to the specified syslog server at the configured address and port, using the chosen protocol (TCP or UDP).

By following these instructions, users can effectively configure the syslog client on their M2M Secure Router to monitor specific system log messages and forward them to a centralized syslog server for further analysis and monitoring.

Chapter 5. Device Management

On the **Device Management** tab, you can remotely manage the devices.



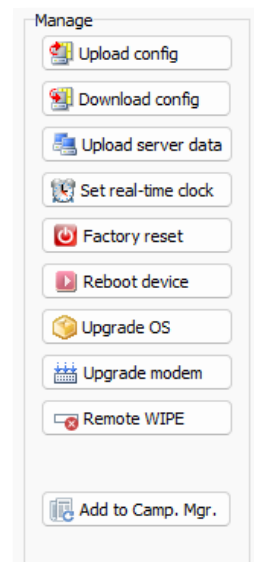
Here on this screen, you can see **ONLINE** devices only.

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)

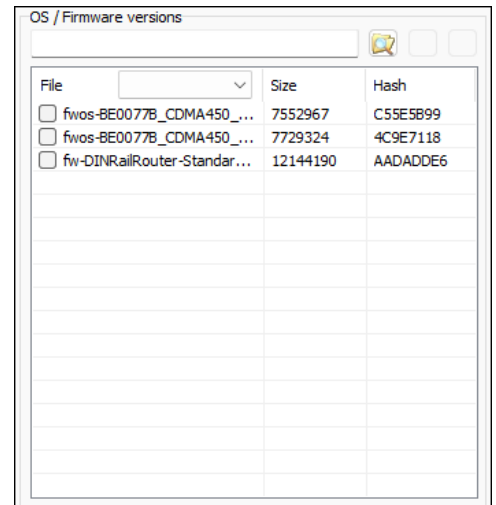


- **Factory reset:** doing a configuration reset of the remote device to the factory default.
- **Reboot device:** immediate restart of the remote device(s).
- **Upgrade OS:** device software/firmware upgrade or downgrade from the selected list to the remote device(s).
- **Upgrade modem:** this feature is not implemented yet.
- **Remote WIPE:** remove all settings and user files from the device and perform a device restart. After wiping, the device will be not able to connect to the cellular network.
- **Add to Camp. Mgr.:** you can add devices to the firmware Campaign Manager

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.

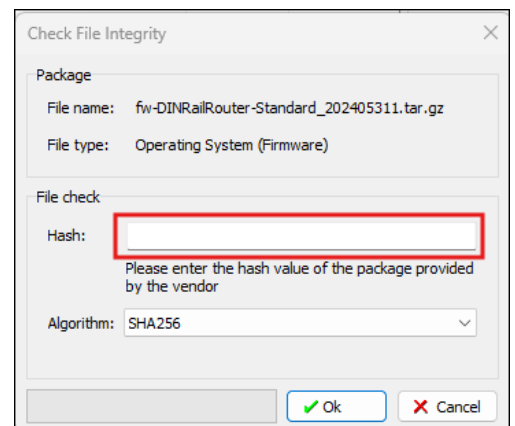


File	Size	Hash
<input type="checkbox"/> fwos-BE0077B_CDMA450_...	7552967	C55E5B99
<input type="checkbox"/> fwos-BE0077B_CDMA450_...	7729324	4C9E7118
<input type="checkbox"/> fw-DINRailRouter-Standar...	12144190	AADADDE6

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.



Check File Integrity

Package

File name: fw-DINRailRouter-Standard_202405311.tar.gz

File type: Operating System (Firmware)

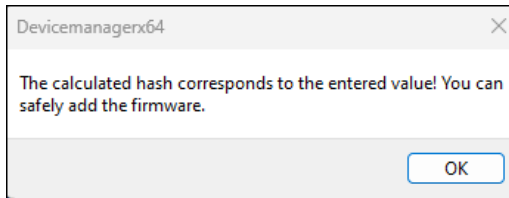
File check

Hash:

Please enter the hash value of the package provided by the vendor

Algorithm: SHA256

Ok Cancel



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).

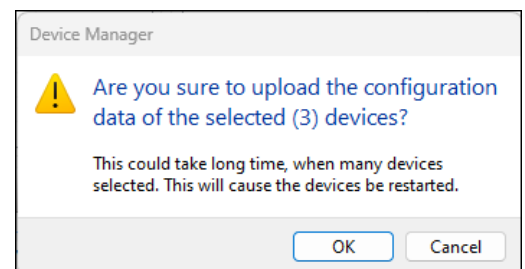
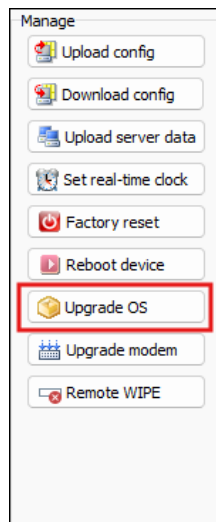
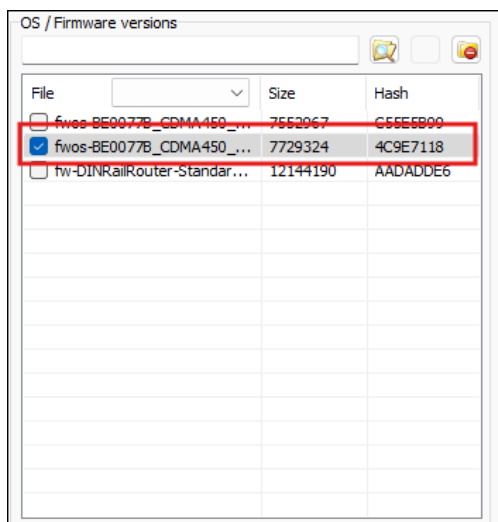
Warning! Any intervention during the firmware upgrade process may cause the failure of the device.

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




...	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	10.202.189.31	35001090702902	TEST DEVICE 13 LE910C L...	-65 dBm	0	2	N/A	107 03:27:40	2024-07-04 20:25:34	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.






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.

	<div style="width: 12%; height: 10px; background-color: orange;"></div>	12%
	<div style="width: 14%; height: 10px; background-color: orange;"></div>	14%
	<div style="width: 19%; height: 10px; background-color: orange;"></div>	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. When 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 filter section at the top with dropdown menus for Status, Modem version, OS, HW, and Group, along with a 'Smart search' field. Below the filter is a table of devices. The table has columns for Status, IP, MEID / IMEI, Description, RSSI, RSRP, Last update, Uptime, Memory usage, and CPU load. The status column uses pictograms: a green triangle for 'Online', a red square for 'Offline', a red square with a white triangle for 'Never plugged in', and a blue circle with a white triangle for 'Connecting...'. The memory usage column shows values like '14,6 MB/122,2 MB free:93,0 MB'. The CPU load column shows values like '1min:0 5min:0 15min:0'. At the bottom of the window, there is a status bar with 'Device count: 70', '0 Exec / 0 Queued', 'Events: 338', 'v7.3.41210.2', and 'Copyright © WM Systems LLC 2024'.

Status	IP	MEID / IMEI	Description	RSSI	RSRP	Last update	Uptime	Memory usage	CPU load
Online	84.224.157.88	59852053517018	Sajtbox Teszt2 ELS_16-1...	-75 dBm	0	2025-03-07 09:13:15	4 06:16:59	14,6 MB/122,2 MB free:93,0 MB	1min:0 5min:0 15min:0
Online	172.31.153.92	59852054108155	EASY BACKUP PRODUCTI...	-73 dBm	0	2025-03-07 09:14:22	00:03:40	13,4 MB/122,2 MB free:95,8 MB	1min:0 5min:0 15min:0
Online	172.31.150.255	53529103780889	EASY BACKUP PRODUCTI...	-73 dBm	0	2025-03-07 09:14:21	15:52:06	14,8 MB/122,2 MB free:94,4 MB	1min:0 5min:0 15min:0
Online	130.43.231.73	598520541121349	Sajtbox Teszt3 ELS_16-0...	-63 dBm	0	2025-03-07 09:14:26	5 14:45:31	14,5 MB/122,2 MB free:93,2 MB	1min:0 5min:0 15min:0
Online	10.202.185.203	53529102724433	EASY BACKUP PRODUCTI...	-63 dBm	0	2025-03-07 09:14:07	10 23:36:42	15,0 MB/122,2 MB free:94,1 MB	1min:0 5min:0 15min:0
Online	10.217.102.66	51622076472675	EASY BACKUP PRODUCTI...	-67 dBm	0	2025-03-07 09:14:13	1 01:04:06	15,0 MB/122,2 MB free:94,2 MB	1min:0 5min:0 15min:0
Online	192.168.30.228	53529102558625	VODAFONE_GW	-51 dBm	0	2025-03-07 09:12:48	191 17:48:35	19,6 MB/122,2 MB free:87,1 MB	1min:0 5min:0 15min:0
Online	172.31.14.233	59852053963238	EASY BACKUP PRODUCTI...	-57 dBm	0	2025-03-07 09:14:19	01:52:14	13,5 MB/122,2 MB free:95,7 MB	1min:0 5min:0 15min:0
Offline	172.31.87.72	53529102573830	EASY BACKUP PRODUCTI...	-51 dBm	0	2024-07-26 12:35:18	8 01:50:32	14,7 MB/122,2 MB free:94,5 MB	1min:0 5min:0 15min:0
Offline	84.224.192.1	53529102543999	Sajtbox Teszt1 - ELS_16...	-61 dBm	0	2024-11-07 16:24:13	72 03:50:04	19,4 MB/122,2 MB free:88,0 MB	1min:0 5min:0 15min:0
Never plugged in	192.168.30.223	55788110055341	TRV_GW	-113 dBm	0	1899-12-30 01:00:00	00:00:00		
Online	172.31.86.48	51580050852538	EASY BACKUP PRODUCTI...	-67 dBm	0	2025-03-07 09:14:25	128 08:55:18	16,7 MB/122,2 MB free:92,4 MB	1min:0 5min:0 15min:0
Never plugged in	10.202.163.62	51580054112384	EASY BACKUP PRODUCTI...	-113 dBm	0	1899-12-30 01:00:00	00:00:00		
Online	10.217.100.151	53529102526846	EASY BACKUP PRODUCTI...	-71 dBm	0	2025-03-07 09:14:19	94 07:06:56	15,6 MB/122,2 MB free:93,4 MB	1min:0 5min:0 15min:0
Online	10.202.188.140	58173052233767	PRO3 EASY BACKUP PRO...	-51 dBm	0	2025-03-07 09:13:09	88 08:31:34		
100%	10.202.177.161	58173054771236	PRO3 EASY BACKUP PRO...	-71 dBm	0	2025-03-07 09:14:36	52 11:00:16		
Online	10.255.232.1	53529107955271	EASY BACKUP PRODUCTI...	-63 dBm	0	2025-03-07 09:13:59	8 20:47:14	16,5 MB/122,2 MB free:92,5 MB	1min:0 5min:0 15min:0
Online	10.217.96.88	53529102716249	EASY BACKUP PRODUCTI...	-67 dBm	0	2025-03-07 09:14:16	276 21:22:53	16,7 MB/122,2 MB free:90,9 MB	1min:0 5min:0 15min:0
Online	10.217.103.69	53529102567113	Viz és Szolg 94 Kiskunhalas	-53 dBm	0	2025-03-07 09:11:56	19 23:08:27	14,8 MB/122,2 MB free:94,3 MB	1min:0 5min:0 15min:0
Never plugged in	10.217.96.98	59852054108007	EASY BACKUP PRODUCTI...	-113 dBm	0	1899-12-30 01:00:00	00:00:00		
Never plugged in	192.168.30.227	51580051968861	Telekom_GW	-113 dBm	0	1899-12-30 01:00:00	00:00:00		
Never plugged in	172.31.158.212	51580051074991	EASY BACKUP PRODUCTI...	-113 dBm	0	1899-12-30 01:00:00	00:00:00		
Online	192.168.30.226	53529102568251	TELENOR_GW	-61 dBm	0	2025-03-07 09:13:45	191 17:54:19	20,0 MB/122,2 MB free:86,7 MB	1min:0 5min:0 15min:0
Online	172.31.152.132	59852054111100	EASY BACKUP PRODUCTI...	-89 dBm	0	2025-03-07 09:13:06	6 22:51:01	13,3 MB/122,2 MB free:96,0 MB	1min:0 5min:0 15min:0
Offline	10.217.103.70	53529102572659	Viz és Szolg 94 Kiskunhalas	-61 dBm	0	2025-01-20 08:04:33	00:01:35	14,1 MB/122,2 MB free:95,2 MB	1min:0 5min:0 15min:0
Connecting...	172.31.155.82	59852053963287	EASY BACKUP PRODUCTI...	-63 dBm	0	2025-03-07 09:14:36	153 23:19:43	14,7 MB/122,2 MB free:94,4 MB	1min:0 5min:0 15min:0
Never plugged in	172.31.115.91	55788110136018	PRO4	-113 dBm	0	1899-12-30 01:00:00	00:00:00		
Online	84.224.152.140	59852054119582	Bela NVR	-71 dBm	0	2025-03-07 09:14:06	12:41:57	15,8 MB/122,2 MB free:91,8 MB	1min:0 5min:0 15min:0
Online	194.152.153.83	53529102558732	M2M-Router-CAM	-63 dBm	0	2025-03-07 09:14:31	114 21:18:05	20,4 MB/122,2 MB free:84,5 MB	1min:0 5min:0 15min:0
Never plugged in	192.168.10.1	68110060037718	NMA	-113 dBm	0	1899-12-30 01:00:00	00:00:00		
Online	10.202.186.200	53529102573558	EASY BACKUP PRODUCTI...	-81 dBm	0	2025-03-07 09:13:02	267 19:30:39	16,7 MB/122,2 MB free:92,4 MB	1min:0 5min:0 15min:0

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 **Last update** date/time, **Uptime** (spent time since last reboot or device start), **Memory usage**, **CPU load** of the device, **Storage status** (free space), **MAC address**, **SIM eid**.

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

IMPORTANT! Note, that these data are not 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. The interface includes a search bar with the text 'Smart search: search condition' and a checked 'Reverse Order' option. A blue 'Acknowledge All' button is visible in the top right of the table area. The table lists various system events with columns for ID, Timestamp, Event ID, Message, Details, Device ID, and Operator. The messages include kernel warnings, power source failures, and USB connection events. At the bottom, a status bar shows 'Device count: 293', '0 Exec / 0 Queued', 'Alerts: 199', 'v7.3.40530.8', and 'Copyright © WM Systems LLC 2023'.

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 10:35:50] 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

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.

The screenshot displays the 'System messages' tab in the WM Systems Device Manager. The interface includes a top navigation bar with tabs for 'Login', 'System messages (63)', 'Alerts (199)', 'Device monitoring', 'Device management', 'Device config', 'Group config', 'User config', and 'System setup'. Below this is a toolbar with various filters and a search bar. The main area contains a table of system messages with columns for ID, Timestamp, Event ID, Message, Details, Device ID, and Operator. The messages list various system events such as kernel warnings, daemon warnings, device configuration downloads, and IP address changes.

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.e...		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/>

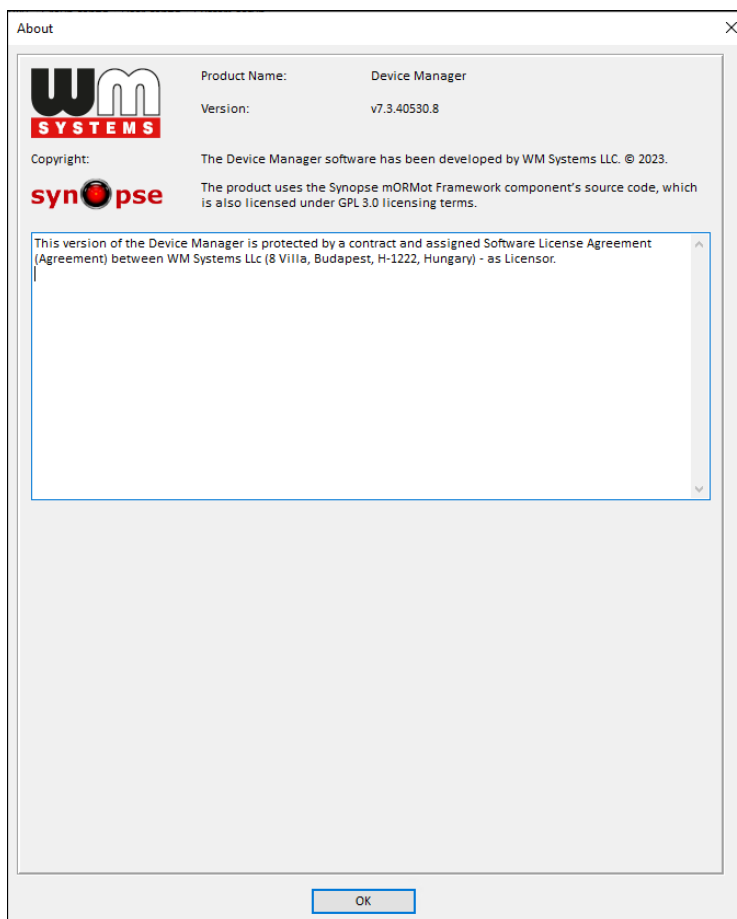
The documentation and software release for this product can be accessed via the following link:

<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.