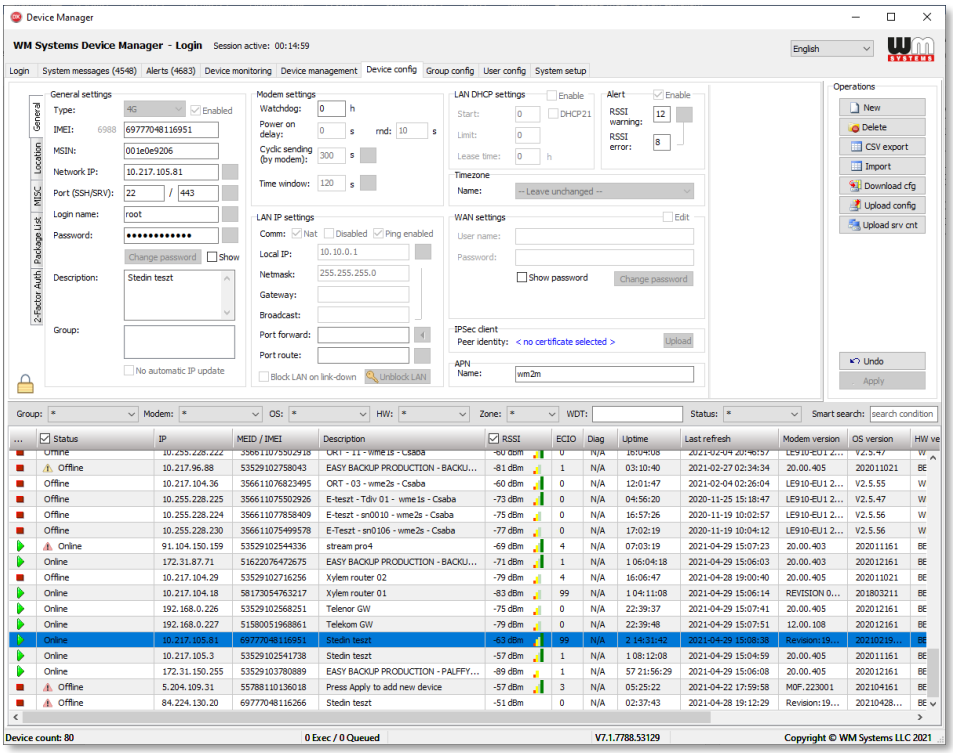
Device Manager® Server

for M2M Router and WM-Ex modem, WM-I3 devices

User Manual

v1.50



2021-08-13

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

Document specifications

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

Document category:	User Manual
Document subject:	Device Manager®
Author:	WM Systems LLC
Document version No.:	REV 1.50
Number of pages:	11
Device manager version:	v7.1
Software version:	DM_Pack_20210804_2
Document status:	FINAL
Last modified:	13 August, 2021
Approval date:	13 August, 2021

Table of contents

Chapter 1. Introduction

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

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

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

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

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

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

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

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

Chapter 2. Setup and Configuration

2.1. Prerequisites

Max. 10.000 metering devices can be managed by a single Device Manager instance.

The usage of Device Manager server application requires the following conditions:

Hardware environment:

- Physical installation and virtual environment usage are also supported
- 4 Core Processor (minimum) - 8 Core (preferred)
- 8 GB RAM (minimum) – 16 GB RAM (preferred), depends on the amount of the devices
- 1Gbit LAN network connection
- Max. 500 GB storage capacity (depends on the amount of the devices)

Software environment:

- Windows Server 2016 or newer - Linux or Mac OS not supported
- MS SQL Express Edition (minimum) – MS SQL Standard (preferred) - Other types of database are not supported (Oracle, MongoDB, MySql)
- MS SQL Server Management Studio – for creating accounts and database and managing the database (eg.: backup or restore)

2.2. System components

The Device Manager consists of three main software elements:

- *DeviceManagerDataBroker.exe* – communication platform between the database and the data collector service
- *DeviceManagerService.exe* – collecting the data from the connected routers and metering modems
- *DeviceManagerSupervisorSvc.exe* – for maintenance

Data Broker

The device manager's data broker's main task is maintaining the database connection with the SQL server and providing a REST API interface to the Device Manager Service.
Furthermore it has a data synchronization feature, to keep all the running UIs synchronized with the database.

Device Manager Service

This is the device management service, 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 device side) and OpenSSL (on server side).

Device Manager Supervisor Service

This service provide the maintanence functions between the GUI and the Device Manager Service. With this feature the system administrator is able to stop, start and restart the server service from the GUI.

2.3. Startup

2.3.1 Install and configure the SQL Server

If you need to install an SQL server, please visit the following website and select the preferred SQL product:
https://www.microsoft.com/en-us/sql-server/sql-server-downloads

If you already have an SQL server installation, create a new database eg. DM7.1 and make a database user account with owner rights on that DM7.1 database. When you start the data broker at first time, it will create all necessary tables and fields into the database. You don't need to create them manually.

First of all create the root folder on the destination system. eg.: C:\DMv7.1. Unzip the Device Manager compressed software package into the folder.

2.3.2 Data Broker

1. Modify the configuration file: *DeviceManagerDataBroker.config*

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

You must to fill the following parameters:

- *SQLServerAddress* → IP address of the SQL server
- *SQLServerUser* → username of the Device Manager database

- *SQLServerPass* → password of the Device Manager database
- *SQLServerDB* → name of the database
- *DataBrokerPort* → listening port of the data broker. The clients will use this port for communication with the data broker.

2. After the modifications, please run the data broker software with administrator privileges (**DeviceManagerDataBroker.exe**)
3. Now this will connect to the database server with the given credentials and create / modify automatically the database structure.

IMPORTANT!

If you want to change the Device Manager Data Broker settings, first of all stop the application.
If you finished the modification run the application as administrator.
In other case the application will overwrite the modified settings to the last working settings!

2.3.3 Device Manager Supervisor Service

1. Modify the configuration file: *Elman.ini*
2. Set the correct port number for the maintenance operations.
   DMSupervisorPort
3. If you want to make a service to run the DM automatically at every server start, then open the command line and execute the following command as administrator: **DeviceManagerSupervisorSvc.exe /install**
   Then the command will install the **DeviceManagerSupervisorSvc** as a service.
4. Start the service from the services list (windows+R → *services.msc*)

2.3.4 Device Manager Service

1. Modify the configuration file: *DeviceManagerService.config*
   (This is a JSON-based configuration file that must be modified for Device Manager to receive data from the connecting modems, routers.)
2. You must set the following recommended parameters:

- *DataBrokerAddress* → IP address of the data broker
- *DataBrokerPort* → communication port of the data broker
- *SupervisorPort* → communication port of the supervisor
- *ServerAddress* → external IP address for the modem communication

- *ServerPort* → external port for the modem communication
- *CyclicReadInterval* → 0 – disable, or value greater than 0 (in sec)
- *ReadTimeout* → parameter or state reading timeout (in sec)
- *ConnectionTimeout* → connection attempt timeout to the device (in sec)
- *ForcePolling* → value must be set to 0
- *MaxExecutingThreads* → max parallel threads in the same time (recommended: dedicated CPU core x 16, eg.: if you dedicated 4 core CPU for the Device Manager, then the value should be set to 64)

3. If you want to make a service to run the Device Manager automatically at every server start, then open the command line and execute the following command as administrator: **DeviceManagerService.exe /install**
   Then the command will install the Device Manager as a service.
4. Start the service from the services list (windows+R → *services.msc*)

IMPORTANT!

If you want to change the Device Manager Service settings, first stop the service. If you finished the modification start the service.

In another case, the service will overwrite the modified settings to the last working settings!

2.3.5 Network preparations

Please open the appropriate ports on the Device Manager Server for the correct communication.

- Server port for the incoming modem communication
- Data Broker port for the client communication
- Supervisor port for the maintenance operations from the clients

2.3.6 Starting the system

1. Start the **Supervisor** for the DeviceManager Service
2. Run the **DeviceManagerDataBroker.exe**
3. **DeviceManagerService**

2.4 TLS protocol communication

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

It used mbedTLS library on the client side (at modem/router), and OpenSSL library on the Device Manager side.

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

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

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

By factory default, it is implemented on the router, so the router does not check whether the certificate presented by the connected party is signed by a trusted party, so any TLS connection to the modem/router can be established with any certificate, even self-signed.
(You need to know the other encryption that is inside the TLS, otherwise, the communication will not work. It also has user authentication, so the connected party does not know enough about the communication, but you also have to have the root password, and successfully self-authenticate).

Chapter 3. Support

3.1 Technical Support

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

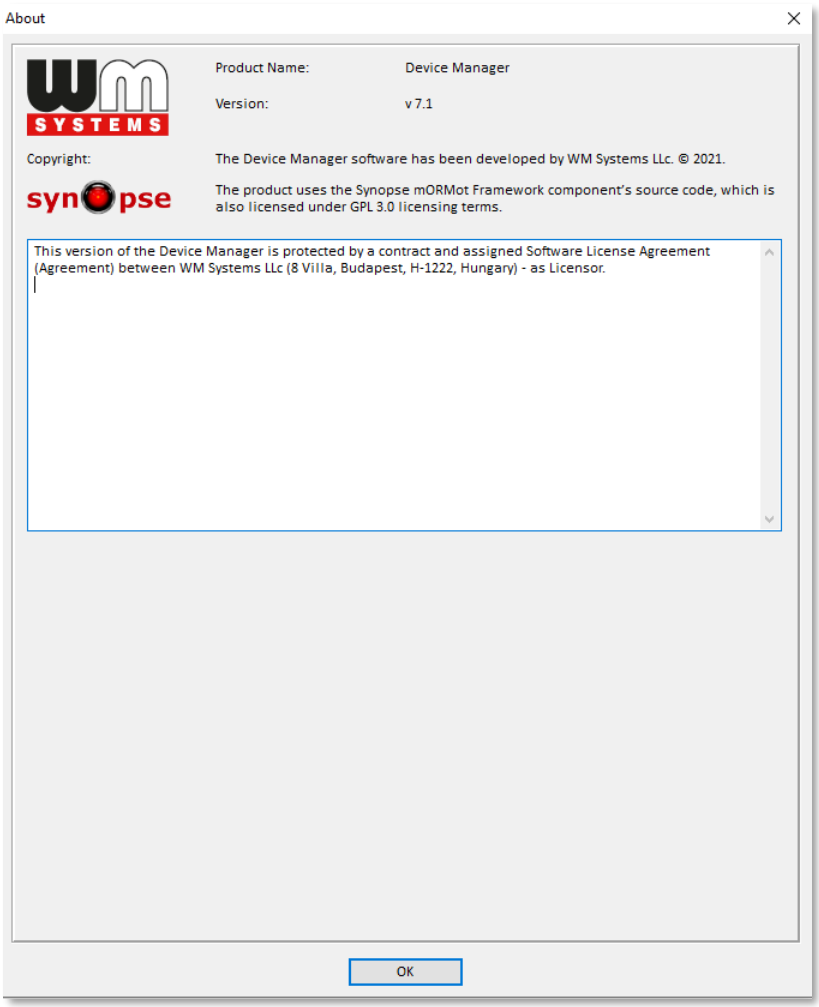
Online product support can be required here at our website:
https://www.m2mserver.com/en/support/

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

3.2 GPL license

The Device Manager® software is not a free product. WM Systems LLc own 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.



4. Legal notice

©2021. WM Systems LLC.

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

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

Warning! Any errors occurring during the program update process may result in failure of the device.