MCRN2P PoE-Reader

ISO14443 & ISO15693
OLED Display

User Manual

Jan. 2025 Rev 1.7

Minova Technology GmbH

Company Headquarters
Auf dem Wall 29
78628 Rottweil
Germany

www.minovatech.de

The information contained herein is provided solely for the purpose of allowing customers to operate and service Minova manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Minova Technology. Information and specifications contained in this document are subject to change without prior notice and do not represent a commitment on the part of Minova Technology.

Revision History

Changes of this document are listed below:

Date	Revision	Note
31.08.2021	1.0	First release
10.09.2021	1.1	Added configuration commands
20.09.2021	1.2	Updated LCDTEXT command description
10.01.2022	1.3	Added DESFire Authentication and Offline Modes
14.02.2022	1.4	Added LED commands
26.04.2023	1.5	Added LED flashing commands
01.11.2023	1.6	Added slave devices support
01.01.2025	1.7	Added AES-128 encryption

Table of Contents

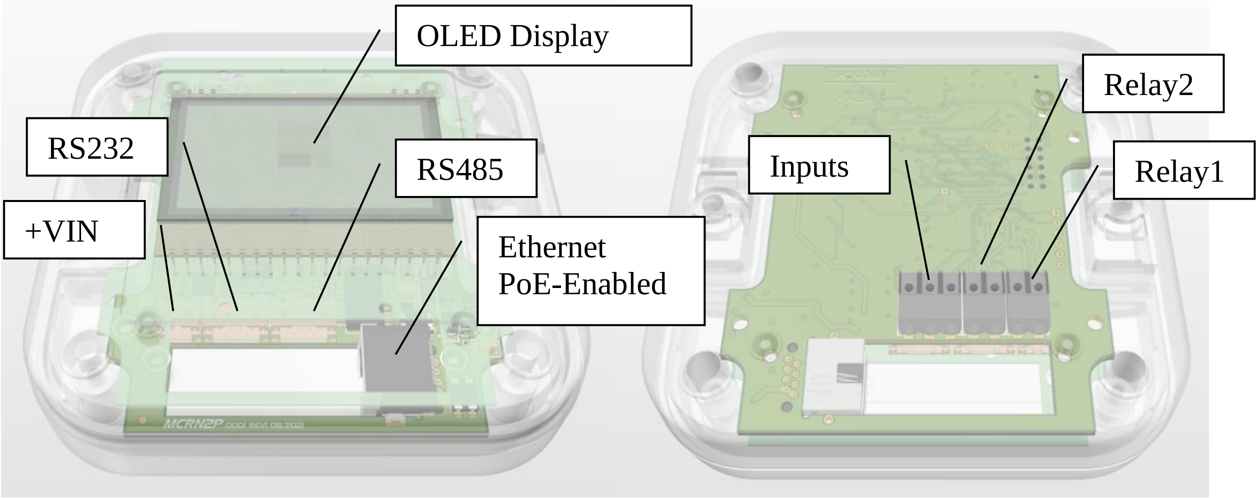
1 Precautions Before Setup & First Run

- **If your network contains managed/smart switches such as (Cisco, Allied Telesis etc.)**
    - RSTP, STP (Spanning Tree Protocols) and related protocols must be turned off or disabled from the management console of the switch. These protocols may cause the terminals to start to gain IP late at first power-on or unable to take an IP address on the network properly.

- **If your network contains a Firewall**
    - Make sure that your network does not have a MAC-Filter.
    - Make sure that UDP 65535 port (terminal discover port i.e miFinder Config) should not be blocked.
    - If your device is unable to gain an IP address from the DHCP server, please define or give freedom to the MAC ID of the terminal in your network (via management console of firewall, router etc.)
    - Make also sure that TCP ports used by the terminal should not be blocked.

2 Introduction

The MCRN2P RFID reader has an Ethernet interface, serial ports, inputs and outputs.



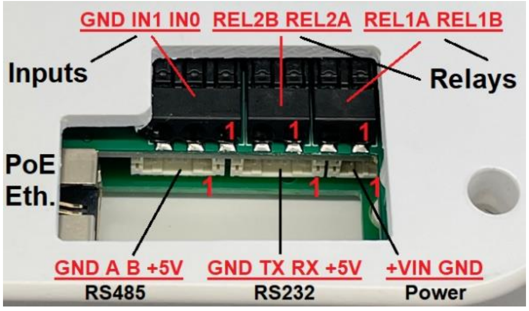
Top view

Bottom view

Blind lids for wall mounting

Waterproof variant

Standard variant



Ports and IOs

The Relay and Input terminal blocks are easy for inserting/removing fine-stranded conductors by lightly depressing the push-button.

The serial port connectors are WR-WTB type 2.00 mm headers.

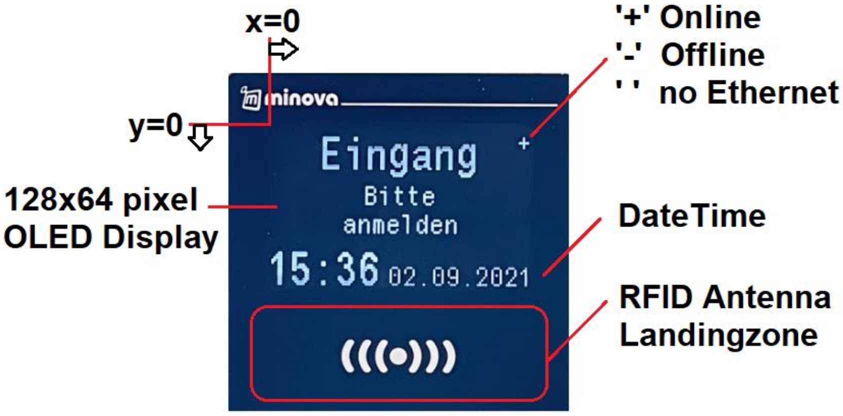
Waterproof variants with relay cable

3 Features

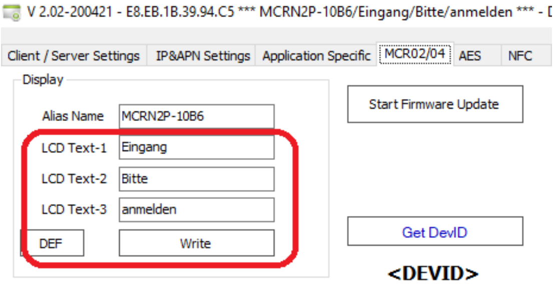
- 128x64 pixel OLED display
- 10/100Mb Ethernet with PoE (Power-Over-Ethernet) interface
- Full NFC support
- ISO14443 A/B, ISO15693 RFID standards
- Supported Tags
  - MIFARE® DESFire/Plus, Classic/Ultralight
  - NTAG and NFC Forum Tags
  - I-Code and other vicinity tags
- IP67 waterproof enclosure
- Easy wall mount brackets
- RS232 or RS485 up to 230K Baud
- USB 2.0 Full-Speed interface (optional)
- 2 relay outputs 1A/30VDC
- 2 opto-isolated inputs
- Buzzer and Real Time Clock
- 4MBit external flash memory
- Bootloader for firmware update
- +8V to +60V DC power supply (optional +5V version)
- 200mA$_{max}$ @ +12V current consumption
- -40 to +85 ºC ambient Temperature
- Crypto Functions (optional)
  - 256-Bit ECDSA Elliptic Curve Digital Signature Algorithm (SECP256R1)
  - 128-Bit AES Advanced Encryption Standard (ECB Mode) SHA256 Secure Hash Algorithm

4 Reader Display

The OLED display can be fully controlled by the host. Line status, date time and main texts can be displayed.



The default texts may be changed using miFinder.exe



V 2.02-200421 - E8.EB.1B.39.94.C5 *** MCRN2P-10B6/Eingang/Bitte/anmelden *** - [

Alias Name: MCRN2P-10B6

LCD Text-1: Eingang

LCD Text-2: Bitte

LCD Text-3: anmelden

<DEVID>

Server can display messages using LCDSET command. The display returns to the default texts after 5s (default) of timeout.

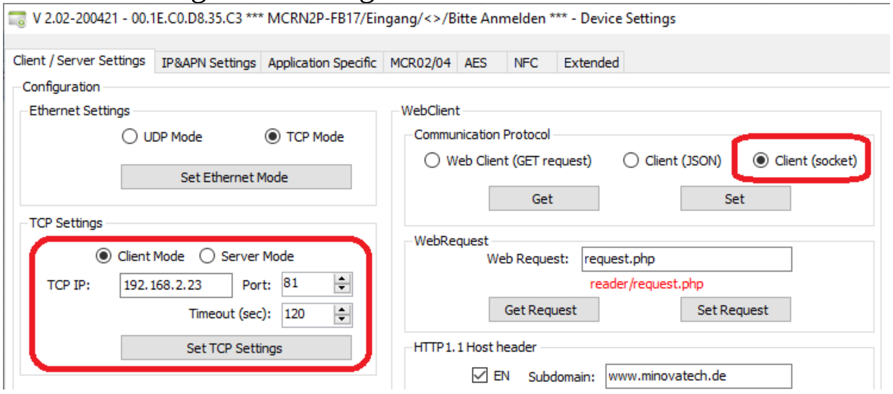
5 Supported Protocols

5.1 ASCII Protocol

The reader connects to the defined IP/Port and keeps the connection alive.

Reader to Host	MCRN2P-1000,UID=F543A9B8
Host answer	MCRN2P-1000,LCDCLR;127,LCDSET;0;0;1;Access approved,BUZZER;50;2

Standard configuration using miFinder.exe



V 2.02-200421 - 00.1E.C0.D8.35.C3 *** MCRN2P-FB17/Eingang/<>/Bitte Anmelden *** - Device Settings

Ethernet Settings: ○ UDP Mode ● TCP Mode

TCP Settings: ● Client Mode ○ Server Mode

TCP IP: 192.168.2.23 Port: 81

Timeout (sec): 120

Communication Protocol: ○ Web Client (GET request) ○ Client (JSON) ● Client (socket)

Web Request: request.php

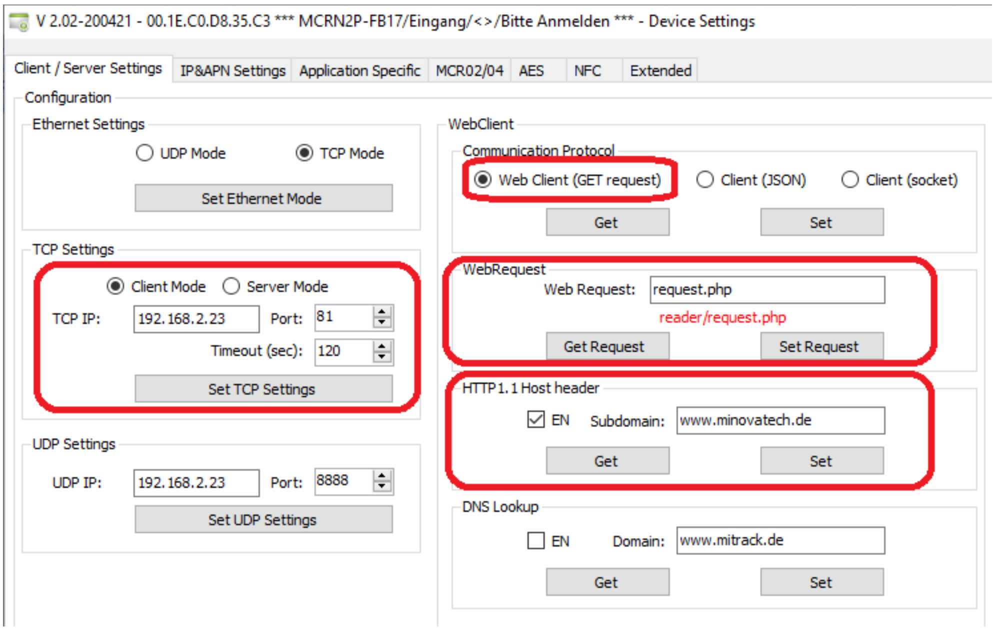
reader/request.php

HTTP1.1 Host header: ☑ EN Subdomain: www.minovatech.de

5.2 HTTP Get Request (Web-Mode)

The reader makes an http Get-Request on the defined web server.

Reader to Host	GET /request.php?devID=MCRN2P-1000&UID= F543A9B8 HTTP/1.1 Host: www.minovatech.de
Host answer	MCRN2P-1000,LCDCLR;127,LCDSET;0;0;1;Access approved,BUZZER;50;2



V 2.02-200421 - 00.1E.C0.D8.35.C3 *** MCRN2P-FB17/Eingang/<>/Bitte Anmelden *** - Device Settings

Ethernet Settings: ○ UDP Mode ● TCP Mode

TCP Settings: ● Client Mode ○ Server Mode

TCP IP: 192.168.2.23 Port: 81

Timeout (sec): 120

UDP Settings: UDP IP: 192.168.2.23 Port: 8888

Communication Protocol: ● Web Client (GET request) ○ Client (JSON) ○ Client (socket)

Web Request: request.php

reader/request.php

HTTP1.1 Host header: ☑ EN Subdomain: www.minovatech.de

DNS Lookup: □ EN Domain: www.mitrack.de

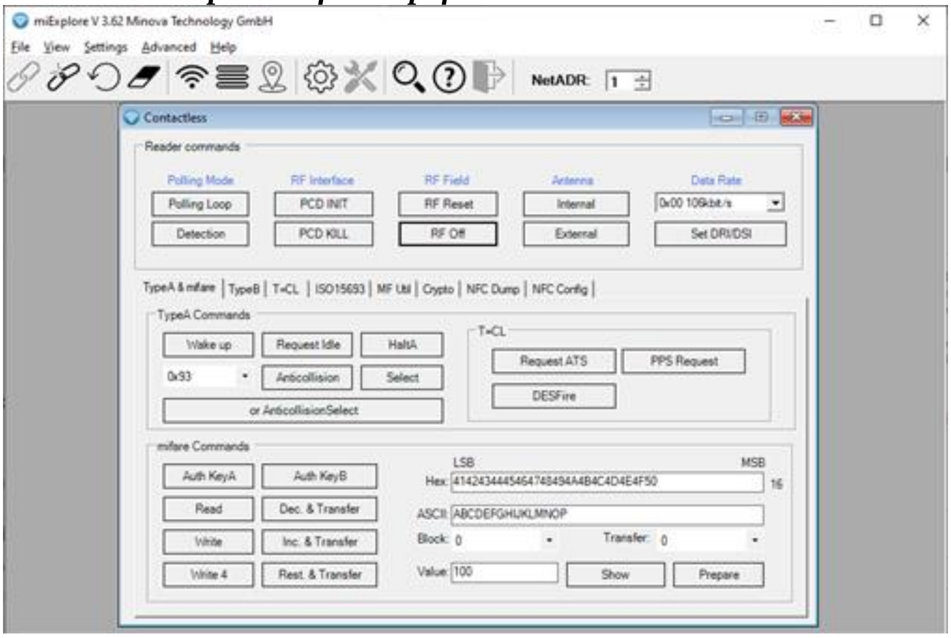
5.3 Binary Protocol

The reader supports a binary protocol, for details refer to the following document

MCRNX Protocol&Cmd Ref.pdf

Reader to Host	01 01 00 09 31 40 4C 3C 3C D5 04 00 08 ED // Card activated event
Host answer	01 01 00 02 5D 01 5E // Polling command

miExplore test software can be used for testing the binary protocol. For details refer to the following document ***miExplore Software.pdf***



NetADR: 1

Data Rate: 0x00 106kbit/s

0x93

Hex: 4142434445464748494A4B4C4D4E4F50

ASCII: ABCDEFGHIJKLMNOP

Block: 0

Transfer: 0

Value: 100

6 Operating Modes

6.1 Server & Client Protocols

The MCRN2P reader can be used in either client or server mode. In client mode the terminal connects to a remote server that it is listening the TCP/UDP port. The server may accept multiple connections.

The MCRN2P reader can also be used as a server. The reader listens own port and can accept a connection request from outside.

The reader opens always a server port automatically. The port is +1 of the defined port. For example, if you set the port to 80, a second server port is automatically opened on port 81.

6.2 Terminal Setup & Settings

The terminal can be configured on a network (LAN). To start setup terminal must be in a network that supports DHCP. The terminal needs to acquire an IP from a DHCP server on your network. Configuration is made through and UDP protocol so it advisable to use a firewall free network. Most of the firewalls filter UDP.

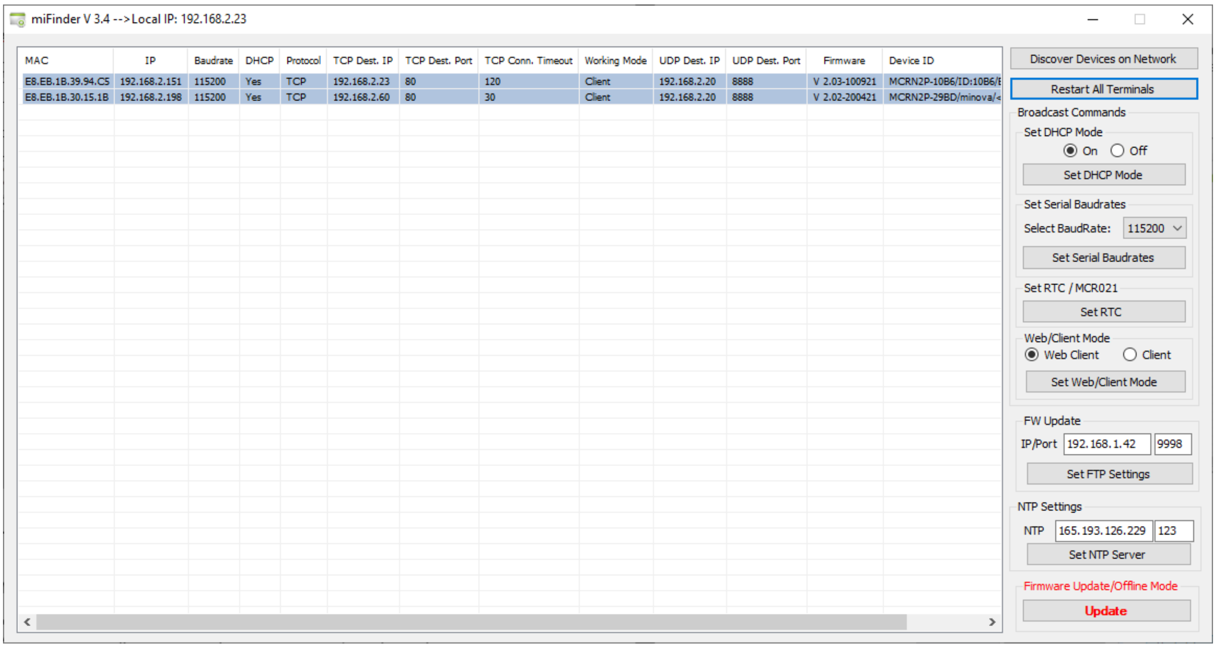
For the first time setup you can use miFinder software. miFinder can discover all terminals on your network. After MCRN2P is up i.e. (after gained an IP from your network) you can use miFinder. It is also advisable to turn off any firewall & antivirus software before running miFinder. As stated before, firewalls on PC may prevent to discover the network.

6.3 miFinder Configuration Software

Using miFinder you can set various parameters related to terminals. Some parameters are specific to each terminal and some parameters are global to all terminals. After all setup, your device is listed or discovered as given below.

If your terminal is not discovered, press Discover button again.

For security reasons, this configuration port only works for 10 minutes after power-up.



miFinder V 3.4 -->Local IP: 192.168.2.23

MAC	IP	Baudrate	DHCP	Protocol	TCP Dest. IP	TCP Dest. Port	TCP Conn. Timeout	Working Mode	UDP Dest. IP	UDP Dest. Port	Firmware	Device ID
E8.EB.1B.39.94.C5	192.168.2.151	115200	Yes	TCP	192.168.2.23	80	120	Client	192.168.2.20	8888	V 2.03-100921	MCRN2P-10B6/ID:10B6/E
E8.EB.1B.30.15.1B	192.168.2.198	115200	Yes	TCP	192.168.2.60	80	30	Client	192.168.2.20	8888	V 2.02-200421	MCRN2P-29BD/minova/<

Broadcast Commands

Set DHCP Mode: ● On ○ Off

Set Serial Baudrates: Select BaudRate: 115200

Set RTC / MCR021

Web/Client Mode: ● Web Client ○ Client

FW Update: IP/Port 192.168.1.42 9998

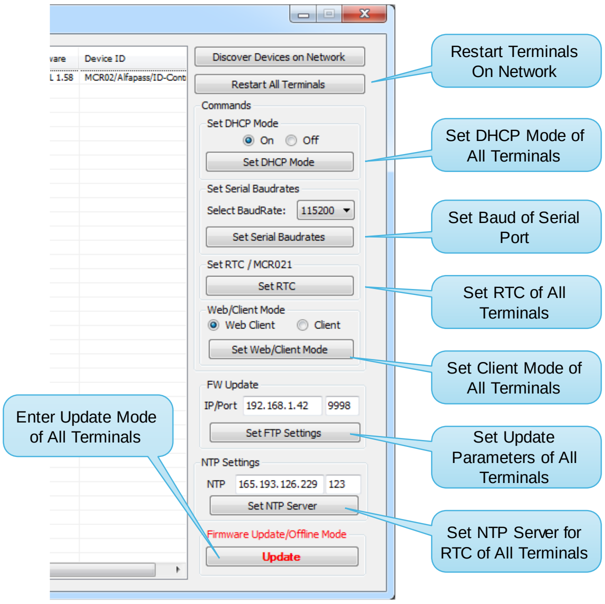
NTP Settings: NTP 165.193.126.229 123

Firmware Update/Offline Mode

miFinder Main Screen

In main window of miFinder you can the following parameters

- Restart or Reset all terminals connected to network.
- Setting DHCP parameter of all terminals connected to network.
- Setting the baud-rate of RS232 / RS485 port.
- Setting the Real Time Clock of all terminals connected to network.



vare	Device ID
L 1.58	MCR02/Alfapass/ID-Cont

Commands

Set DHCP Mode: ● On ○ Off

Set Serial Baudrates — Select BaudRate: 115200

Set RTC / MCR021

Web/Client Mode: ● Web Client ○ Client

FW Update — IP/Port 192.168.1.42 9998

NTP Settings — NTP 165.193.126.229 123

Firmware Update/Offline Mode

Restart Terminals On Network

Set DHCP Mode of All Terminals

Set Baud of Serial Port

Set RTC of All Terminals

Set Client Mode of All Terminals

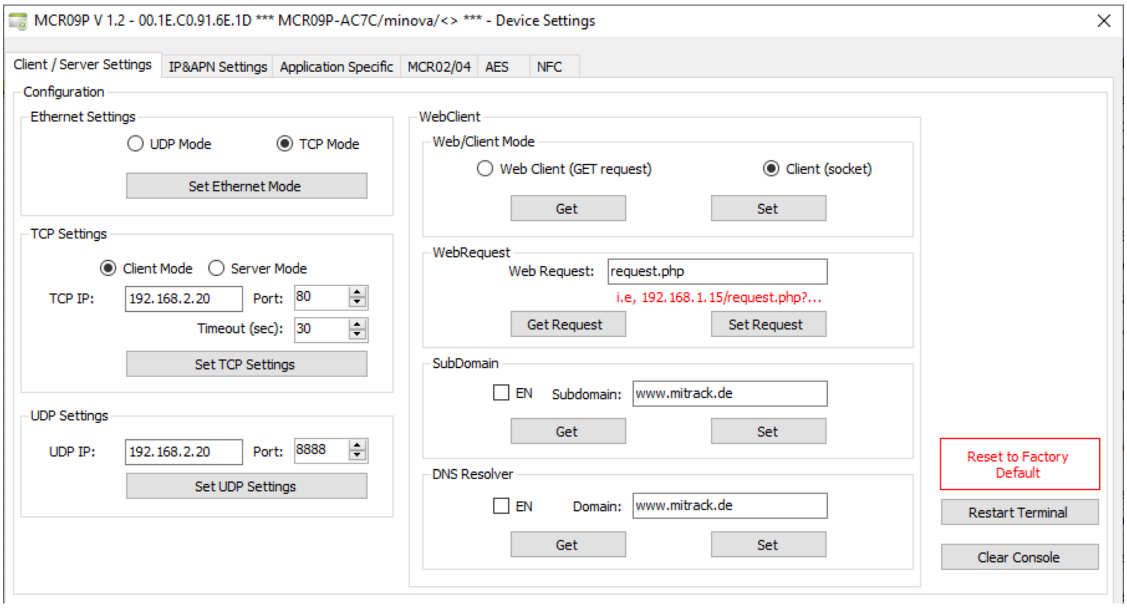
Set Update Parameters of All Terminals

Set NTP Server for RTC of All Terminals

Enter Update Mode of All Terminals

miFinder main window view

To enter a detailed setup of a particular terminal select a device from the list and double click to see a particular terminal setting window in miFinder. This window gives you a detailed setup of each terminal. Please note that these settings are specific to each terminal. Below given a snapshot of detailed settings window of miFinder.



MCR09P V 1.2 - 00.1E.C0.91.6E.1D *** MCR09P-AC7C/minova/<> *** - Device Settings

Configuration

Ethernet Settings: ○ UDP Mode ● TCP Mode

TCP Settings: ● Client Mode ○ Server Mode

TCP IP: 192.168.2.20 Port: 80

Timeout (sec): 30

UDP Settings

UDP IP: 192.168.2.20 Port: 8888

WebClient

Web/Client Mode: ○ Web Client (GET request) ● Client (socket)

WebRequest

Web Request: request.php

i.e, 192.168.1.15/request.php?...

SubDomain

□ EN Subdomain: www.mitrack.de

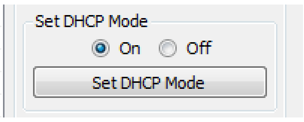
DNS Resolver

□ EN Domain: www.mitrack.de

miFinder Terminal Setting Window

6.3.1 Automatic IP (DHCP) Mode

In miFinder's main screen, in Set DHCP Mode section, select ON and press Set DHCP Mode button. Then all terminals restart and try to access a DHCP server to get an IP address from your network. Please note that your network must have a DHCP enabled management device.

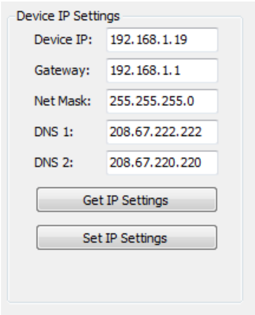

Set DHCP Mode

● On ○ Off

DHCP Mode Setting

6.3.2 Constant / Static IP Mode

To set a terminal to be run in static IP mode, in miFinder’s main window enter the desired terminal’s settings screen. Then enter your desired IP, GW, Mask and DNS values in Device IP Settings section.


Device IP Settings

Device IP: 192.168.1.19

Gateway: 192.168.1.1

Net Mask: 255.255.255.0

DNS 1: 208.67.222.222

DNS 2: 208.67.220.220

IP Parameters Settings Section

Note that, after opening settings screen, this section gives your terminal’s current IP parameters. After entering the values as above figure, then press Set IP Settings button. Then the terminal restarts again.

The last step is to set DHCP mode to OFF in main window of miFinder as given in above figure. The terminal restarts again in Static IP mode. Please note that you can skip this step if your terminal is already operating in static IP mode.

6.3.3 Message Format

The message format from server to terminal is given by the following syntax.
<Device ID>,<CMD1;parameter1;…;parameterN>,<CMD2;parameter1;…;parameterN>,…

This packet can be sent by a specific TCP server via socket_send API’s or simple echo statements defined in a web server protocol.

Max. 20 commands can be sent, and each command can have max. 50 chars.

Example:
MCRN2P-1000,RELAY1=1000,RELAY2=2000

The message format from terminal to server is given by the following syntax.
<Device ID>,<ANSWER;VALUE1;VALUE2>
or
<Device ID>,ACK
<Device ID>,NAK

Example:
MCRN2P-1000,UID=4FA20135

7 Messages and Command Set

Terminal to server (events)

Message	Description	Example
ALIVE	Send periodically every 30s	*MCRN2P-1000,ALIVE*
UID	Card ID	*MCRN2P-1000,UID=F543A9B8*
Offline UID	Offline card ID with UNIX time	*MCRN2P-1000,OID=F543A9B8,UTIME=1628946795*
INPUTS	Input change	*MCRN2P-1000,IN=0F*

Server to terminal (command)

Command	Description	Example
VERSION?	Gets the firmware version	*MCRN2P-1000,VERSION?* *Answer: MCRN2P-1000,VERSION=V 2.02-200421*
RELAY1=ON/OFF **RELAY2=ON/OFF** **LED1/2/3=ON/OFF** **LEDx;DURATION;COUNT**	Set/release a relay Set/clr LEDs Flash LEDs	*MCRN2P-1000,RELAY1=ON* *MCRN2P-1000,*LED2=ON,DELAY;500,LED2=OFF *MCRN2P-1000,*LED3;100;5
RELAY1=ms **RELAY2=ms**	Activate relay by a delay in ms	*MCRN2P-1000,RELAY1=1000*
TSYNC=UNIXTIME	Set RTC	*MCRN2P-1000,TSYNC=1412625197*
BUZZER;DURATION;COUNT	Play a sound (buzzer)	*MCRN2P-1000,BUZZER;200;2*
IOSTAT?	Get IO status	*MCRN2P-1000,IOSTAT?* *Answer: MCRN2P-1000,IN=1F,OUT=01*
TRST	System reset	*MCRN2P-1000,TRST*
COM1TX;DATA	Transmit data via comport	*MCRN2P-1000,COM1TX;Test print*
COM1RX	Get data from comport	*MCRN2P-1000,COM1RX*
RFID Commands		
GETUID or RESETCARD	Activates an RFID tag	*MCRN2P-1000,GETUID* *Answer; MCRN2P-1000,UID=FA523C84*
LOADKEYS;TYPE;KEYA;KEYB	Load mifare keys	*MCRN2P-1000,LOADKEYS;0;A0A1A2A3A4A5;* *B0B1B2B3B4B5*
BLOCKREAD;BLOCKNR **BLOCKREADX;BLOCKNR**	Read 16 bytes mifare block Read 16 bytes in HEX mode	*MCRN2P-1000,BLOCKREAD;2* *Answer: BLOCKDATA=Test string 1* *Answer: BLOCKDATAX=000102030405060708090A0B0C0D0E0F* *Answer: NAK block authentication error*
BLOCKWRITE;BLOCKNR;DATA **BLOCKWRITEX;BLOCKNR;DATA**	Write max 16 bytes mifare block Write max 16 bytes in HEX mode	*MCRN2P-1000,BLOCKWRITE;2;Test* *MCRN2P-1000,BLOCKWRITEX;2;000102030405..*
FORMATSECTOR;SECTORNR;DATA	Format a sector	*MCRN2P-1000,FORMATSECTOR;1;* *FFFFFFFFFFFFFF078069FFFFFFFFFFFF*
SECTORREAD;SECTORNR **SECTORREADX;SECTORNR**	Read 48 bytes of sector data Read 48 bytes in HEX mode	*MCRN2P-1000,SECTORREAD;1* *MCRN2P-1000,SECTORREADX;1*
SECTORWRITE;SECTORNR;DATA **SECTORWRITEX;SECTORNR;DATA**	Write max 48 bytes of sector data Write max 48 bytes in HEX mode	*MCRN2P-1000,SECTORWRITE;1;MAX MUSTERMAN* *MUSTERSTRASSE 2 MUSTERSTADT*
CAPDU;APDU[0]..APDU[n]	Send APDU DESFire or Bank Card	*SELPPSE: MCRN2P-1000,CAPDU;* *00A404000E325041592E5359532E444446303100* *Anser: MCRN2P-1000;RAPDU=06675041259000*
WAIT;TIME	Time in milliseconds	*WAIT;1000 (Waits one seconds as a delay)*
ISO15693 Commands		
VICCGETINFO	Get VICC Information	*MCRN2P-1000,VICCGETINFO* *MCRN2P-1000,* *VICCINFO=000f0d55a32f500104e000001b0301*
VICCBLOCKREADX;BLOCKNR	Block read (4 byte)	*MCRN2P-1000,VICCBLOCKREADX;0* *MCRN2P-1000,VICCBLOCKDATA=e1400e00*
VICCBLOCKWRITEX;BOCKNR;DATA	Block write (4 byte)	*MCRN2P-1000,VICCBLOCKWRITEX;3;6E303738* *MCRN2P-1000,ACK*
VICCSEND;DATA	Transparent data exchange	*MCRN2P-1000,VICCSEND;22200D55A32F500104E000* *MCRN2P-1000,VICCRECEIVE=00e1400e00*
NTAG Commands		
NTAGCMD;DATA	Transparent NTAG command int.	*GET VERSION: MCRN2P-1000,NTAGCMD;60* *Answer: MCRN2P-1000,DATA=0004040502011303*
NTAGREAD16;BLOCKNR	Read 16 bytes of NTAG data in HEX	*MCRN2P-1000,NTAGREAD16;6* *Answer* *NTAGREAD16=00010203000000000000000000000000*
NTAGWRITE4;BLOCKNR;DATA	Write 4 bytes in HEX mode	*MCRN2P-1000,NTAGWRITE4;6;00010203*

NTAGWRITE16;BLOCKNR;DATA	Write 16 bytes in HEX mode	*MCRN2P-1000,NTAGWRITE16;4;00010203040506..*

* Write commands: Remaining blocks will be filled with spaces in ASCII mode and with 0x00s in HEX mode

Display Commands

Message	Description	Example
LCDCLR	*Clears the LCD*	None
LCDSET;Left;Top;Font;Text	*Writes text on LCD*	*LCDSET;0;0;0;Hello World* Fonts: 0 to 3 Left: 0 to 127 Right: 0 to 63
LCDTEXT;Line1;Line2;Lline3	Define texts for all lines	*LCDTEXT;Hallo or LCDTEXT;Minova;Guten;Tag* *This command changes the default texts on the display until next restart or display command*

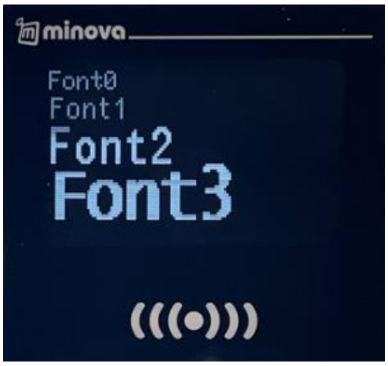
LCD Fonts Example

4 commands are sent: 1x clear LCD and 3x set LCD

LCDSET command: <cmd>;<left pixel>;<right pixel>;font (0-to-3);Text to display

Example: LCDSET;0;10;1;Font1

MCRN2P-1000,LCDCLR,LCDSET;0;0;0;Font0,LCDSET;0;10;1;Font1,LCDSET;0;20;2;Font2,LCDSET;0;35;3;Font3



* Default display will be loaded back after 5 seconds of timeout.

Configuration Commands

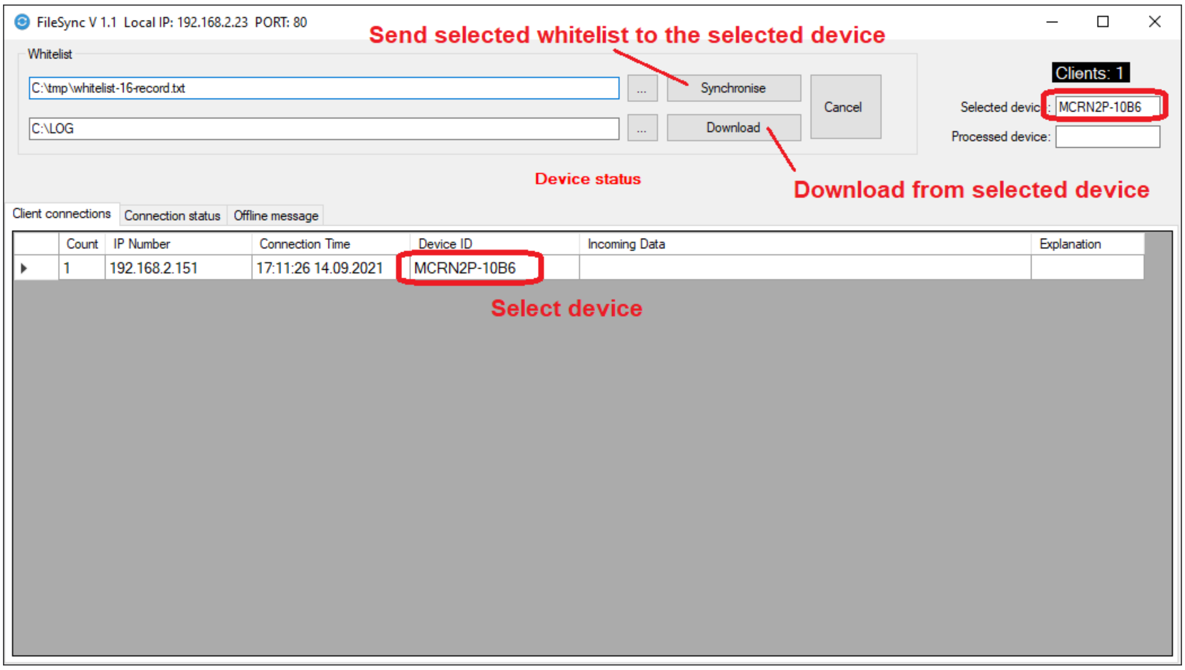
Command	Description
SETWEB	Sets the web-client settings ***MCRN2P-1000,SETWEB;<par1>;<par2>;<par3>;>par4>*** *par1: Enable/disable (0/1) web-client mode* *par2: Get-request path* *par3: Enable/disable (0/1) HTTP 1.1 header* *par4: HTTP1.1 host header (virtual domain name)* ***Examples:*** *(up to 4 parameters)* ***Send:*** *MCRN2P-1000,SETWEB;0;* ***Send:*** *MCRN2P-1000,SETWEB;1;api/rfid.php;* ***Send:*** *MCRN2P-1000,SETWEB;0;api/rfid.php;0;* ***Send:*** *MCRN2P-1000,SETWEB;0;api/rfid.php;1;login.mitrack.de*
GETWEB	Gets the web-client settings ***Send:*** *MCRN2P-1000,GETWEB;* ***Answer:*** *MCRN2P-1000,GETWEB;0;api/rfid.php;0;login.mitrack.de*
SETALIVE	Sets the alive message period ***Send:*** *MCRN2P-1000,SETALIVE;60* ***Answer:*** *MCRN2P-1000,ACK*
GETALIVE	Gets the alive message period in seconds ***Send:*** *MCRN2P-1000,GETALIVE* ***Answer:*** *MCRN2P-1000,GETALIVE;60*
SETTCP	Sets the server TCP settings ***MCRN2P-1000,SETTCP;<par1>;<par2>;<par3>;>par4>*** *par1: Server IP* *par2: Server Port*

	par3: Enable/disable (0/1) DNS lookup (connect using domain name) *par4: Server domain name* *Examples: (up to 4 parameters)* ***Send:** MCRN2P-1000,SETTCP;85.214.201.95;* ***Send:** MCRN2P-1000,SETTCP;85.214.201.95;80;* ***Send:** MCRN2P-1000,SETTCP;85.214.201.95;80;0;* ***Send:** MCRN2P-1000,SETTCP;85.214.201.95;80;1;login.mitrack.de;* *Terminal restarts after this command!* ***Answer:** MCRN2P-1000,ACK,RESTART*
GETTCP	Gets the TCP/IP settings ***Send:** MCRN2P-1000,GETTCP* ***Answer:** MCRN2P-1000,GETTCP;85.214.201.95;80;0;login.mitrack.de;*

Offline/Whitelist Commands

Message	Description	Example
ACK_STR;DATA	Set commands to execute for ACK	ACK_STR;LCDCLR,LCDSET;0;0;1;Access granted,BUZZER;50;2
NAK_STR;DATA	*Set commands to execute for NAK*	NAK_STR;LCDCLR,LCDSET;0;0;1;Access denied,BUZZER;1000;1
WLIST_ADD;0;UID *or* ***WLIST_ADD;1;UID ;START;END***	Add an UID to the whitelist	*Type 0 no time limitation* *WLIST_ADD;0;041C9742344981* *Type 1 with start and end unixtime* *WLIST_ADD;1;041C9742344981;1420074061;422842522*
WLIST_CLR	Clear the whole whitelist	*WLIST_CLR*
WLIST_GET=ITEMNR	Get an item from whitelist	*WLIST_GET=5*
ACT_CLR	Clear the activity file	*ACT_CLR*
LIST_INFO	Get activity and whitelist count	*MCRN2P-1000,LIST_INFO* *Answer: Whitelistcount, Checksum, 0, Activity list count* *MCRN2P-1000,LIST_INFO,100,238,0,5*
FILESYNC	Start whitelist synchronization	*Filesynch software command*
FILEUPLOAD	Start file upload	*Filesynch software command*

The ***FileSync*** software can be used to upload/download of whitelist files


FileSync V 1.1 Local IP: 192.168.2.23 PORT: 80

Whitelist: C:\tmp\whitelist-16-record.txt

C:\LOG

Clients: 1

Selected device: MCRN2P-10B6

Processed device:

Count	IP Number	Connection Time	Device ID	Incoming Data	Explanation
1	192.168.2.151	17:11:26 14.09.2021	MCRN2P-10B6		

This software uses a TCP socket to exchange the whitelist. To initiate a synchronization, the software waits to an ***ALIVE*** message from the reader.

7.1 NTAG21X Command Interface

NTAG card operations can be done by using the NTAGCMD command

NTAGCMD command format

Server to terminal
NTAGCMD;<CMD><DATA0><DATA1>…

<CMD>: NTAG command (Please refer to NTAG datasheet for more info)

GET_VERSION	0x60
READ	0x30
WRITE	0xA2
READ_CNT	0x39
PWD_AUTH	0x1B
READ_SIG	0x3C

<DATA>: NTAG command parameter

Terminal to server
ACK or NAK or DATA=<DATA0><DATA1>…

Examples:

GET_VERSION	Retrieve information from the NTAG
Send	*MCRN2P-1000,NTAGCMD;60*
Receive	*MCRN2P-1000,DATA=0004040502011303*

READ	Retrieve 16 bytes (4 pages) of data
Send	*MCRN2P-1000,NTAGCMD;3006 (Read 16 bytes starting from page 6)*
Receive	*MCRN2P-1000,DATA=00000000000000000000000000000000*

WRITE	Write 4 bytes into defined page
Send	*MCRN2P-1000,NTAGCMD;A20600010203 (write on page 6)*
Receive	*MCRN2P-1000,ACK or MCRN2P-1000,NAK*

PWD_AUTH	Verify password for protected memory
Send	*MCRN2P-1000,NTAGCMD;1BFFFFFFFF (Auth with default password)*
Receive	*MCRN2P-1000,DATA=0000 (PACK data) or MCRN2P-1000,NAK*

READ_SIG	Retrieve ECC signature
Send	*MCRN2P-1000,NTAGCMD;3C00*
Receive	*MCRN2P-1000,DATA=580ebc4156bb1e17c59ee8a.. (32 bytes of data)*

7.2 Loading mifare® Keys

The terminal needs the sector keys in order to read/write the related blocks. There are two keys (KeyA and KeyB) for each sector.

MCRN2P-1000,LOADKEYS;TYPE;KEYA;KEYB

Example; MCRN2P-1000,LOADKEYS;0;FFFFFFFFFFFF;FFFFFFFFFFFF

The key usage is defined in the following table.

TYPE	READ	WRITE
0	Key A	Key A
1	Key A	Key B
2	Key B	Key A
3	Key B	Key B
5	No-Auto	No-Auth

7.3 Formatting mifare® Sectors

Blocks 3,7,11,15,..63 are sector trailer blocks and store the KEYA, KEYB and the access conditions.

The sector trailer data must be defined correctly.

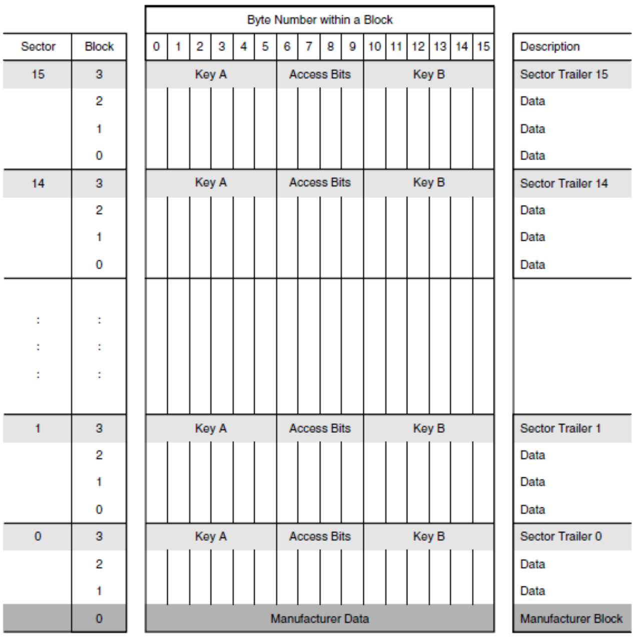
MCRN2P-1000,FORMATSECTOR;SECTORNR;DATA
SECTORNR = 0 to 15
DATA = KEYA-ACCESSBITS-KEYB

Examples:

```
MCRN2P-1000,FORMATSECTOR;1;FFFFFFFFFFFFFF078069FFFFFFFFFFFF    // Transport config R&W with KEYA
MCRN2P-1000,FORMATSECTOR;1;FFFFFFFFFFFF78778800FFFFFFFFFFFF    // R/W-Blocks read: KEYA, write: KEYB
MCRN2P-1000,FORMATSECTOR;1;FFFFFFFFFFFF08778F00FFFFFFFFFFFF    // INC/DEC-Blocks
MCRN2P-1000,FORMATSECTOR;1;FFFFFFFFFFFF7F00F800FFFFFFFFFFFF    // DEC-Only-Blocks
MCRN2P-1000,FORMATSECTOR;1;FFFFFFFFFFFF68778900FFFFFFFFFFFF    // B0;INC/DEC, B1-2 R/W blocks
```

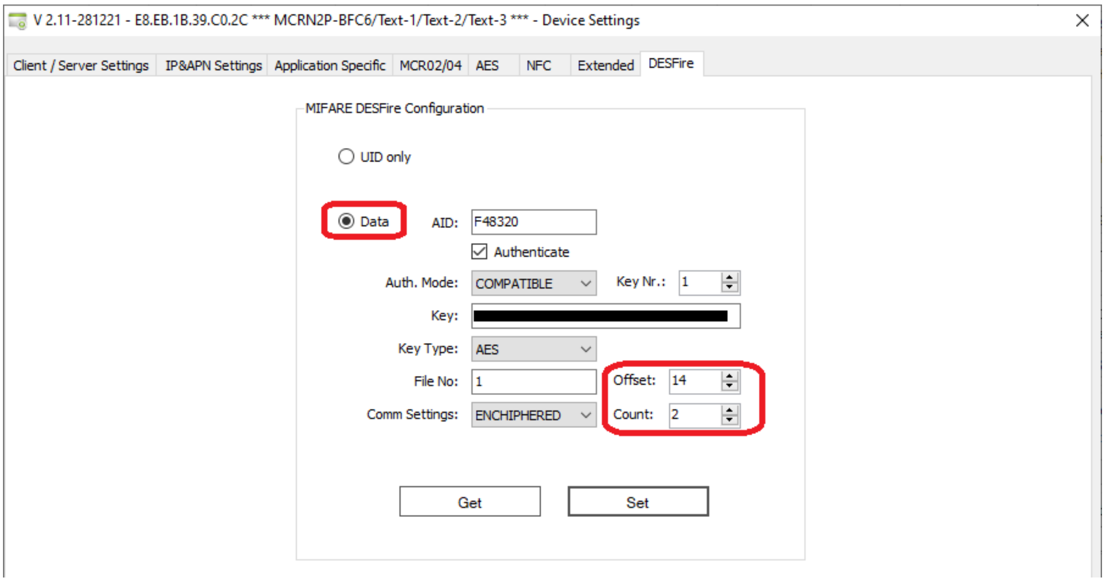
7.4 Mifare Card Memory Layout

1024 × 8 bit EEPROM memory



8 DESFire Authentication and Auto Read

Internal serial number of a DESFire card can be read using the following configuration. The authentication settings should be defined according to the card schema. The reader will perform a DESFire Authentication by selecting the defined Application ID. The read and parsed data will be returned or used in offline mode.


V 2.11-281221 - E8.EB.1B.39.C0.2C *** MCRN2P-BFC6/Text-1/Text-2/Text-3 *** - Device Settings
Client / Server Settings
IP&APN Settings
Application Specific
MCR02/04
AES
NFC
Extended
DESFire
MIFARE DESFire Configuration
Get
Set

○ UID only

● Data AID: F48320

☑ Authenticate

Auth. Mode: COMPATIBLE Key Nr.: 1

Key: [redacted]

Key Type: AES

File No: 1 Offset: 14

Comm Settings: ENCHIPHERED Count: 2

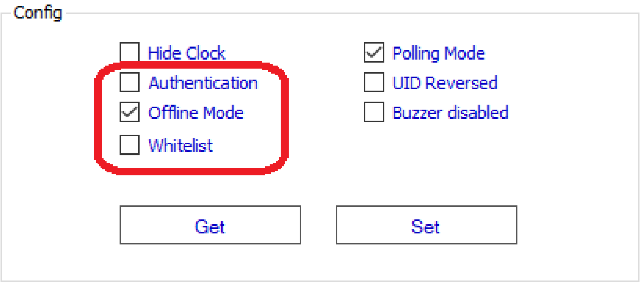
9 Offline Modes

If the offline mode is activated, the reader logs the activities and sends after it is online again. Following rules apply:

1- No Authentication, no whitelist. All cards are accepted.
  a. Mifare DESFire Card: If authentication settings are defined, the internal serial number is read and saved. Otherwise, the 7-Byte UID is used.
  b. Mifare Classic or other technologies: The 4/7-Byte UID is used.

2- Whitelist activated. In this mode, the serial number or UID is checked.
  a. Mifare DESFire Card: If authentication settings are defined, the internal serial number is read and searched in the whitelist. Otherwise, the 7-Byte UID is used.
  b. Mifare Classic or other technologies: The 4/7-Byte UID is searched in the whitelist.

3- Authentication Mode. In this mode, all successful authenticated cards are accepted.
  a. Mifare DESFire Card: If authentication settings are defined, the internal serial number is read. Otherwise, the 7-Byte UID is used.
  b. Mifare Classic or other technologies: The 4/7-Byte UID is used.



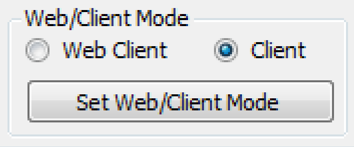
☐ Hide Clock
☐ Authentication
☑ Offline Mode
☐ Whitelist

☑ Polling Mode
☐ UID Reversed
☐ Buzzer disabled

10 Test Connection with Hercules

Hercules Setup Utility can be used to test the terminals behavior.

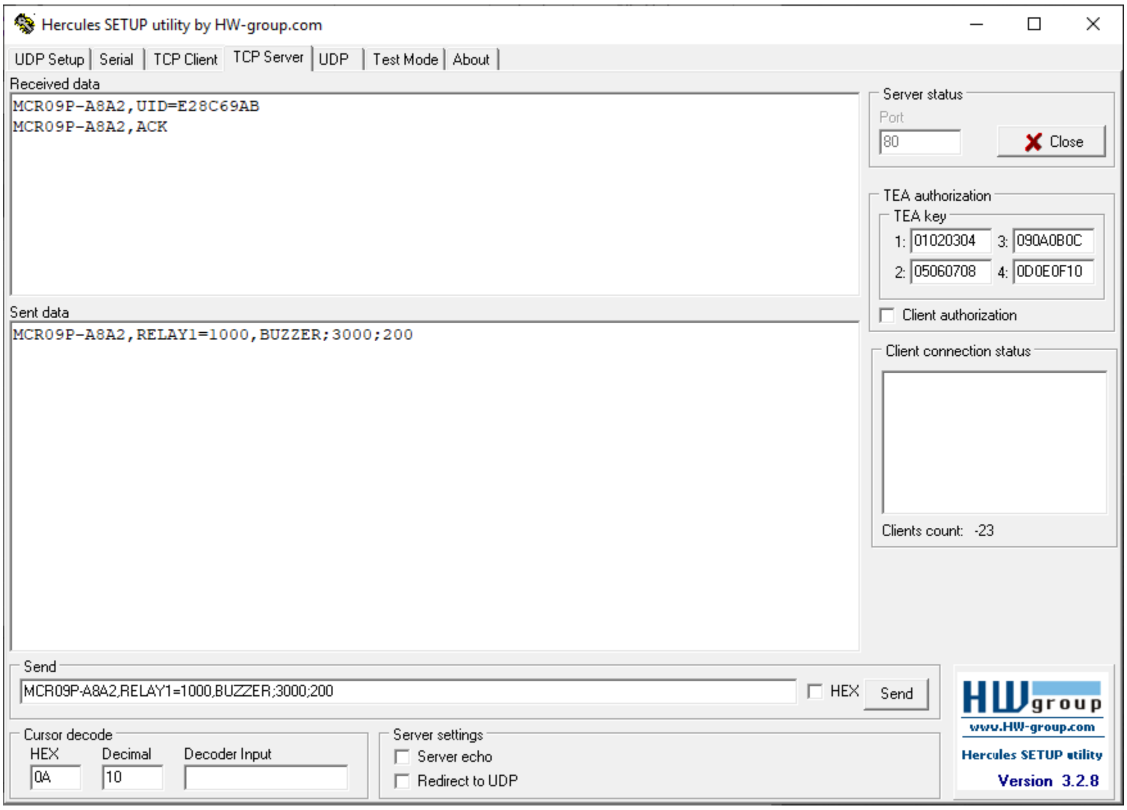
- Set the terminal in Client mode (skip this step if the terminal is already in client mode)



Web/Client Mode

○ Web Client ● Client

- Select TCP Server and enter the Terminals port number
- Click on ***Listen***
- The terminal will connect automatically as seen in the connection status
- After presenting a card, the message will be displayed in the ***Received data*** window
- Enter the response message and send to the terminal. The device ID must be the same in the received and sent data
- As the TCP connection is open, we can send commands directly to the terminal



Hercules SETUP utility by HW-group.com
UDP Setup | Serial | TCP Client | TCP Server | UDP | Test Mode | About
Close
Send
HW group
www.HW-group.com
Hercules SETUP utility
Version 3.2.8

Received data

```
MCR09P-A8A2,UID=E28C69AB
MCR09P-A8A2,ACK
```

Sent data

```
MCR09P-A8A2,RELAY1=1000,BUZZER;3000;200
```

Server status

Port: 80

TEA authorization

TEA key

1: 01020304 3: 090A0B0C

2: 05060708 4: 0D0E0F10

□ Client authorization

Client connection status

Clients count: -23

Send: MCR09P-A8A2,RELAY1=1000,BUZZER;3000;200 □ HEX

Cursor decode

HEX: 0A Decimal: 10 Decoder Input:

Server settings

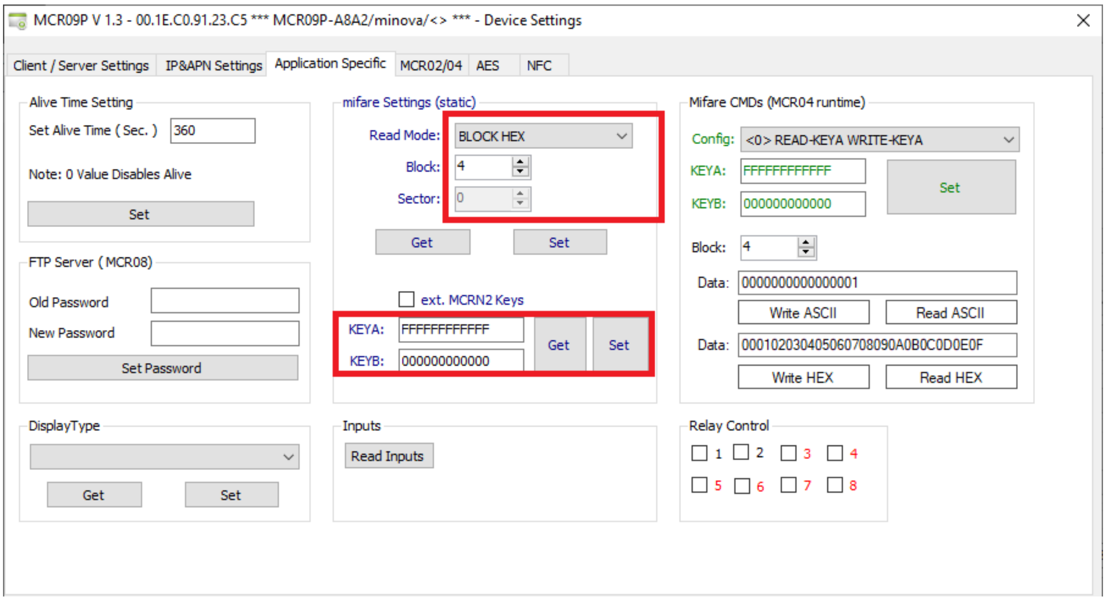
□ Server echo

□ Redirect to UDP

Use the ***TCP Client*** tab if the terminal is configured as a server.

11 MIFARE Classic Auto Read Function

The reader can be configured to read automatically a block or sector whether in HEX or ASCII format.



MCR09P V 1.3 - 00.1E.C0.91.23.C5 *** MCR09P-A8A2/minova/<> *** - Device Settings

Set Alive Time (Sec.): 360

Note: 0 Value Disables Alive

mifare Settings (static): Read Mode: BLOCK HEX; Block: 4; Sector: 0

KEYA: FFFFFFFFFFFF

KEYB: 000000000000

Mifare CMDs (MCR04 runtime): Config: <0> READ-KEYA WRITE-KEYA

KEYA: FFFFFFFFFFFF

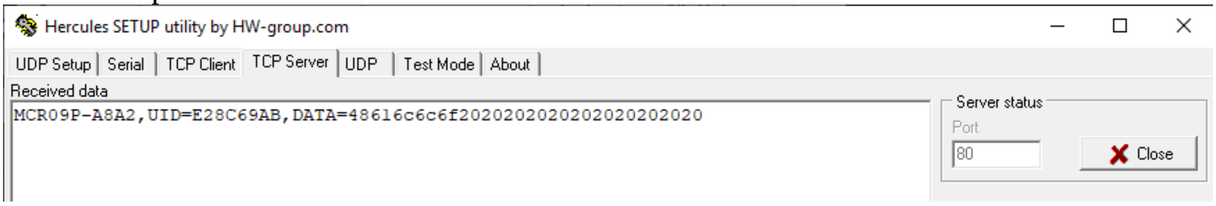
KEYB: 000000000000

Block: 4

Data: 0000000000000001

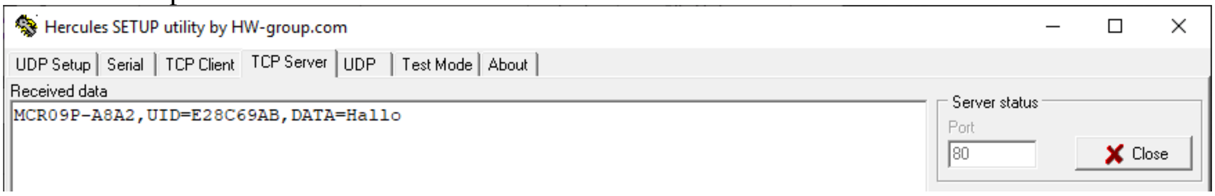
Data: 000102030405060708090A0B0C0D0E0F

HEX Example



```
MCR09P-A8A2,UID=E28C69AB,DATA=48616c6c6f2020202020202020202020
```

ASCII Example



```
MCR09P-A8A2,UID=E28C69AB,DATA=Hallo
```

To write back, following commands can be sent

ASCII -> MCRN2P-1000,BLOCKWRITE;4;Test
HEX -> MCRN2P-1000,BLOCKWRITEX;4;000102030405060708090A0B0C0D0E0F

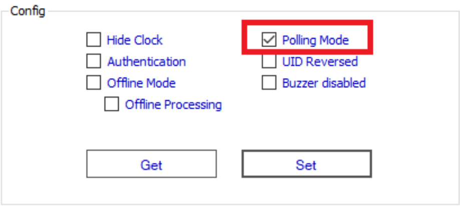
In case of sector change, the new mifare KEYs and access conditions should be loaded

MCRN2P-1000,LOADKEYS;0;A0A1A2A3A4A5;B0B1B2B3B4B5

12 NFC Configuration

Polling Mode

If polling mode is activated, the readers polls for cards and reports automatically the UID.



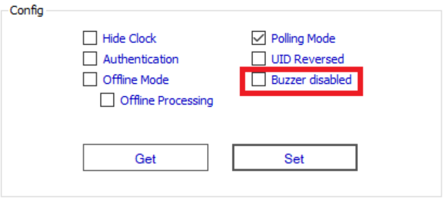
Config

☐ Hide Clock
☐ Authentication
☐ Offline Mode
☐ Offline Processing

☑ Polling Mode
☐ UID Reversed
☐ Buzzer disabled

Buzzer enable/disable

If buzzer is not deactivated, on each card detection a beep sound will be generated.



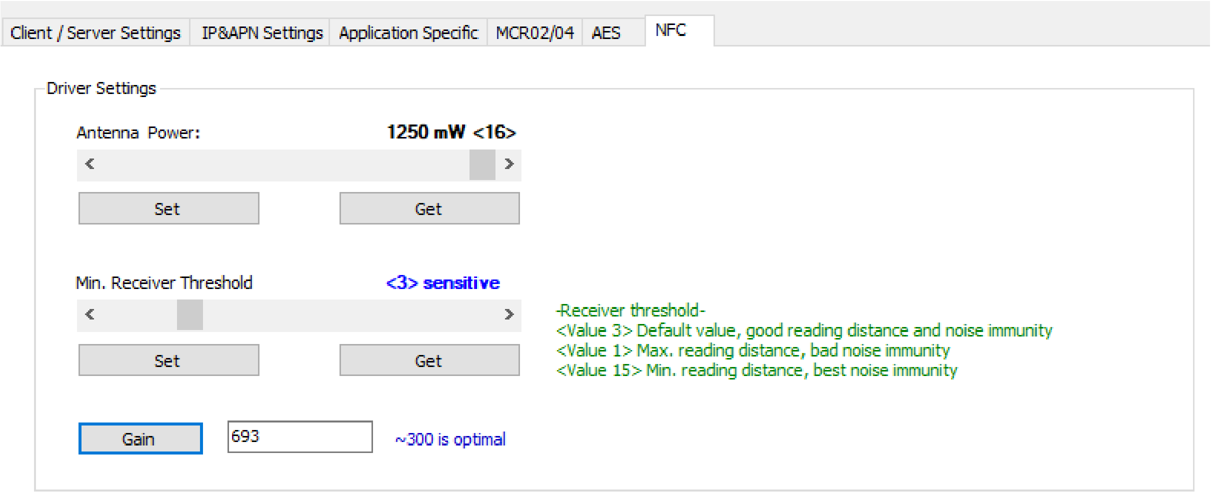
Config

☐ Hide Clock
☐ Authentication
☐ Offline Mode
☐ Offline Processing

☑ Polling Mode
☐ UID Reversed
☐ Buzzer disabled

RF Driver Settings

Output power and reading threshold can be set (not recommended to change)



Driver Settings

Antenna Power: 1250 mW <16>

Min. Receiver Threshold <3> sensitive

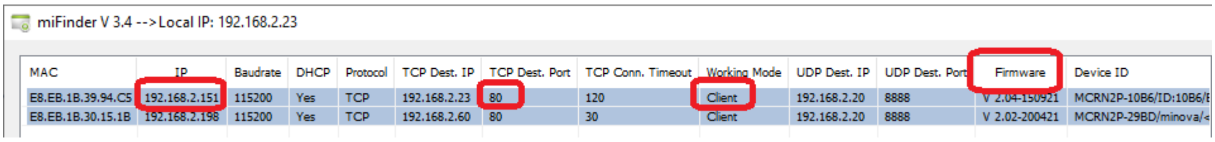
-Receiver threshold-
<Value 3> Default value, good reading distance and noise immunity
<Value 1> Max. reading distance, bad noise immunity
<Value 15> Min. reading distance, best noise immunity

Gain 693 ~300 is optimal

13 Firmware Update

First, we need to establish a TCP connection to the reader. In case of RS232 or USB, you can jump to 3 and select the appropriate interface.

1. Check the IP of the reader and working mode via miFinder.exe.

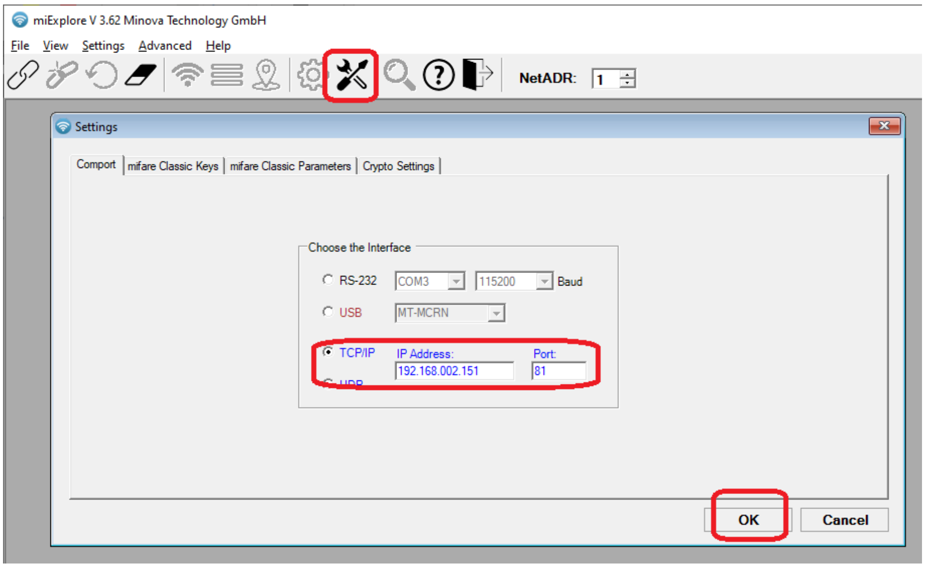


miFinder V 3.4 -->Local IP: 192.168.2.23

MAC	IP	Baudrate	DHCP	Protocol	TCP Dest. IP	TCP Dest. Port	TCP Conn. Timeout	Working Mode	UDP Dest. IP	UDP Dest. Port	Firmware	Device ID
E8.EB.1B.39.94.C5	192.168.2.151	115200	Yes	TCP	192.168.2.23	80	120	Client	192.168.2.20	8888	V 2.04-150921	MCRN2P-10B6/ID:10B6/E
E8.EB.1B.30.15.1B	192.168.2.198	115200	Yes	TCP	192.168.2.60	80	30	Client	192.168.2.20	8888	V 2.02-200421	MCRN2P-29BD/minova/<

2. In case of ***Server*** mode, we can use the ***TCP Dest. Port*** defined.
   In case of ***Client*** mode, we need to set +1 of the above port. In this case 81. This is because the reader always opens a server port with a port number +1 of the defined port. The updater software is a client and needs the server socket to communicate.

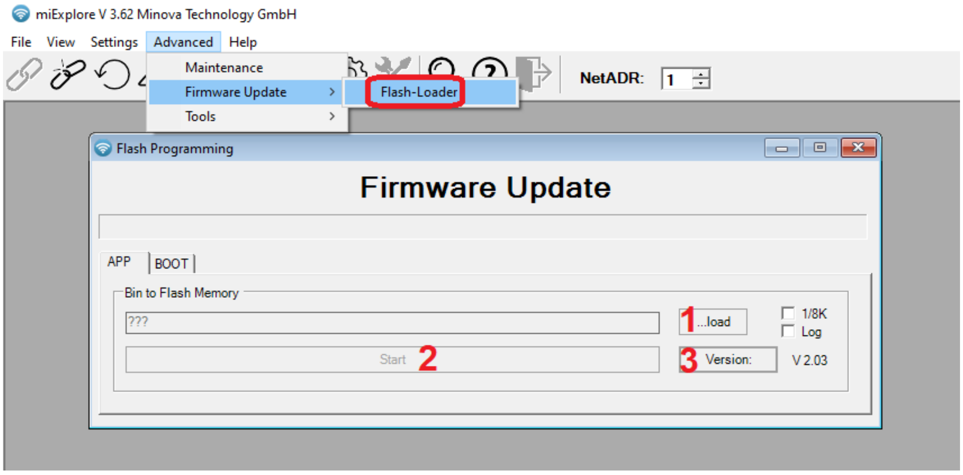
3. Set the communication settings as below and click on ***Ok.***



miExplore V 3.62 Minova Technology GmbH
File View Settings Advanced Help
NetADR: 1
Settings
Comport
mifare Classic Keys
mifare Classic Parameters
Crypto Settings
Choose the Interface
OK
Cancel

○ RS-232 COM3 115200 Baud
○ USB MT-MCRN
● TCP/IP IP Address: 192.168.002.151 Port: 81
○ UDP

4. Click on Connect and open the following form and load the firmware by following 1-2-3.



14 Slave Devices

The net address on the TCP protocol can be used to communicate with the slave devices attached on the serial interfaces.

NetAdr	Device	Description
1	Master device	The MCRN2P itself
2	Forward to RS232 interface	Slave device e.g. Relay board
3	Forward to RS485 interface	Slave device e.g. second reader

In this case, the data frame received will be forwarded to the serial interface and the answer will be written back to the socket. This works only in client mode (server is host).

Example:

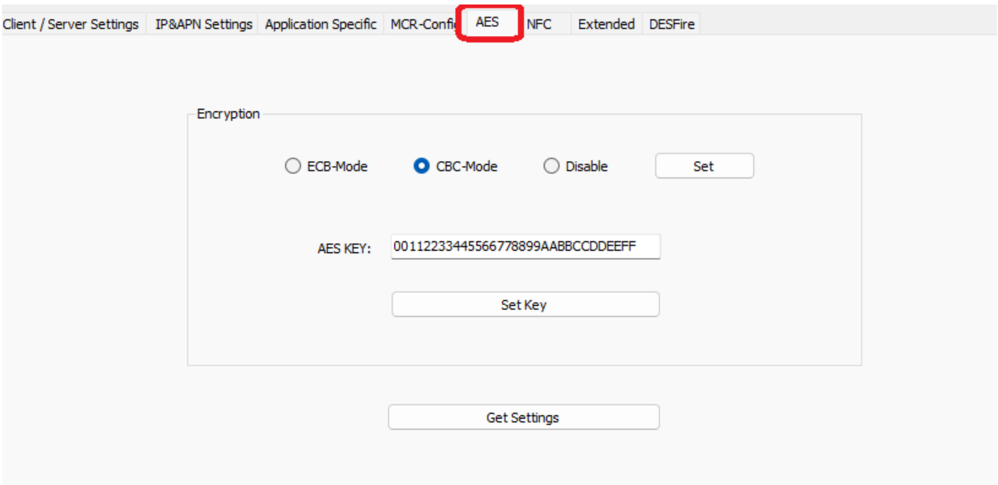
MCRN2 connected with Ethernet as TCP client and the relay board as RS232 slave.

TCP command: 010200024200040 // (NetAdr = 2)
RS232 forward: 010200024200040
Relay board answer: 010100010001
TCP answer: 010100010001

This way, any serial device using binary protocol can be controlled via TCP socket.

15 Encrypted Client-Server Communication

Encrypted communication can be activated using the miFinder tool.



○ ECB-Mode ● CBC-Mode ○ Disable

AES KEY: 00112233445566778899AABBCCDDEEFF

Cipher Type: AES **Mode:** ECB or CBC **Key Size:** 128 bits **Block Size:** 128 bits

15.1 ASCII Protocol

Input data should be a multiple of the block size (16 bytes), so messages may have to be padded with 0x00 to bring them to this length.

Server-to-Client example: *CIPHERDATA+CRLF(0D0A)*

ASCII	MCRN2P-1000,ACK;THANKS
HEX	4D43524E32502D313030302C41434B3B5448414E4B5300000000000000000000 (padded)
KEY	00112233445566778899AABBCCDDEEFF
IV	00000000000000000000000000000000 (example)
CIPHER	0A44993473297F48B85D042EFBDF9809D89313795635BBB57F1BF668CB3BD1DF

Client-to-Server example: *CIPHERDATA+CRLF(0D0A)*

CIPHER	A4BA60F1A043A4DD1CAABFE50E17B1C0B05812EFB125CC1E99BEFA345DAB9410 *0D0A*
KEY	00112233445566778899AABBCCDDEEFF
IV	00000000000000000000000000000000 (example)
HEX	4D43524E32502D313030302C5549443D45323843363941420000000000000000
ASCII	MCRN2P-1000,UID=E28C69AB

15.1.1 IV Initialization Vector

ECB-Mode

The initialization vectors are set to 00000000000000000000000000000000.

CBC-Mode

The initialization vectors are randomized and send to the server (in plain text) at the beginning of each new TCP session.

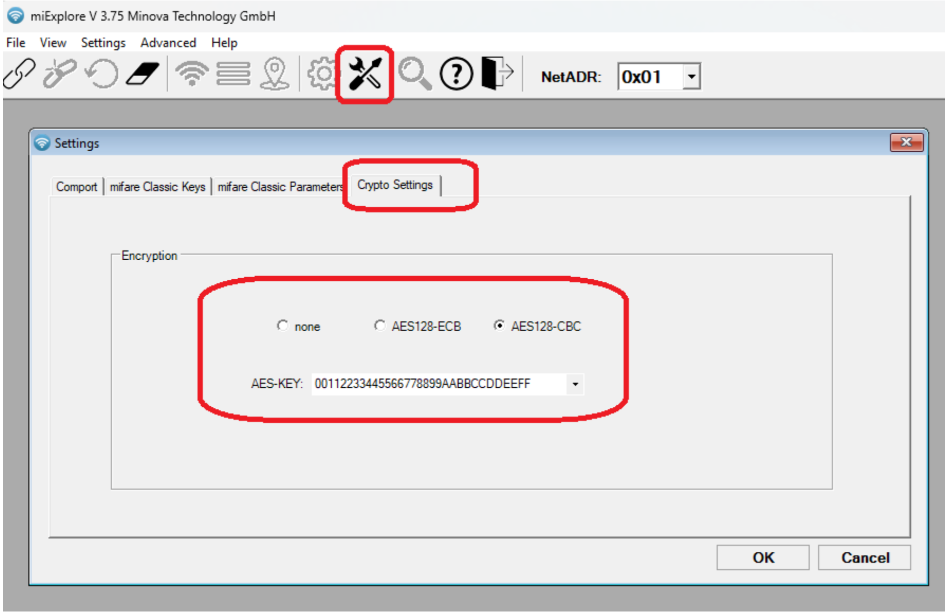
Example:

MCRN2P-1000,IV=903FA4E02A8931A55D4D0FF888BBCBFF

During the TCP session, all cipher blocks are chained with their own IVs (RX and TX). The initial IVs are the same.

15.2 Binary Protocol

miExplore Tool: Encrypted communication can be activated in the crypto settings.



miExplore V 3.75 Minova Technology GmbH

NetADR: 0x01

Settings

Encryption

○ none ○ AES128-ECB ● AES128-CBC

AES-KEY: 00112233445566778899AABBCCDDEEFF

Input data should be a multiple of the block size (16 bytes), so messages may have to be padded with 0x00 to bring them to this length. The first byte of the data content is the padding length of the last block.

All encrypted frames are structured as followed:

SOH	ADDR	LEN	PADDING	ENCYPTED DATA (16xn)	BCC
01	01	2 bytes	Data field, multiple of 16 bytes +1		BCC

Example:

Command GET_INFO + 0x02

Plain Text	7202
Padding	72020000000000000000000000000000
Padding length	0E
AES Key	000102030405060708090A0B0C0D0E0F
IV	00000000000000000000000000000000
Encrypted	E312F4DD5A52BFDCAD7AC0176341D02F
Data frame to send	

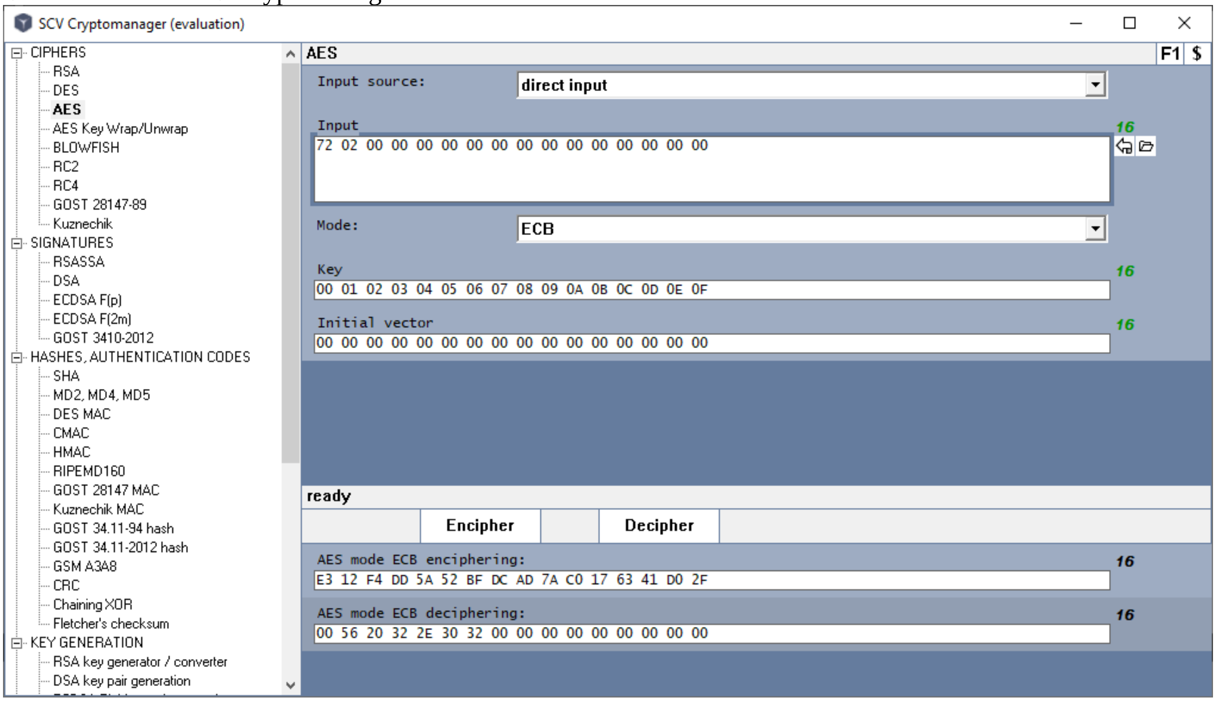
01 01 00 11 0E E3 12 F4 DD 5A 52 BF DC AD 7A C0 17 63 41 D0 2F 71

Answer

01 01 00 11 09 98 97 5A DE 88 36 E5 09 5D 90 0E E3 DD 7D 2B EB 81

Encrypted	98 97 5A DE 88 36 E5 09 5D 90 0E E3 DD 7D 2B EB
Padding length	09
AES Key	000102030405060708090A0B0C0D0E0F
IV	00000000000000000000000000000000
Plain Text	005620322E303200000000000000000000
Remove padding	005620322E3032

Verification via SCV Cryptomanager



Input source: direct input

Input
72 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Mode: ECB

Key
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Initial vector
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

AES mode ECB enciphering:
E3 12 F4 DD 5A 52 BF DC AD 7A C0 17 63 41 D0 2F

AES mode ECB deciphering:
00 56 20 32 2E 30 32 00 00 00 00 00 00 00 00 00

Read Config Example (without protocol bytes):

0B CD 69 FB E8 83 06 3E 9D FD D7 EB 8B DC DC 1C EB
➔ 30 00 00 00 16
09 A8 17 3A 02 CB B5 D1 11 60 D5 06 6A D2 10 2E 9C 1C F8 9E 81 61 68 D2 1C F6 91 01 46 17 58 FB 1C
➔ 00 71 01 00 00 00 00 00 00 00 00 14 10 10 60 07 80 40 00 8A 33 33 00

Write Config Example (without protocol bytes):

05 2A E3 65 C2 73 95 C6 AC DC 5C 87 47 B0 89 97 E4 23 9D 79 43 0A C4 BC D3 2C 77 EE 34 98 1C 74 53
➔ 31 00 00 00 16 71 01 00 00 00 00 00 00 00 00 14 10 10 60 07 80 40 00 8A 33 33 00
0F C6 A1 3B 37 87 8F 5B 82 6F 4F 81 62 A1 C8 D8 79
➔ 00

15.2.1 IV Initialization Vector

ECB-Mode

The initialization vectors are set to 00000000000000000000000000000000.

CBC-Mode

The initialization vectors are randomized and send to the host (in plain text) on power-up.

Example:
Event 0x41: Initialization Vector

01 01 00 11 41 90 3F A4 E0 2A 89 31 A5 5D 4D 0F F8 88 BB CB FF 00

During the TCP session, all cipher blocks are chained with their own IVs (RX and TX). The initial IVs are the same.