MCP040 Four Door Controller Configuration Manual

Version 2.01 (ENG)

UNION COMMUNITY

Disclaimers

Information in this document is provided in connection with UNION COMMUNITY products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in UNION COMMUNITY's Terms and Conditions of Sale for such products, UNION COMMUNITY assumes no liability whatsoever, and UNION COMMUNITY disclaims any express or implied warranty, relating to sale and/or use of UNION COMMUNITY products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

UNION COMMUNITY products are not intended for use in medical, life saving, life sustaining applications, or other applications in which the failure of the UNION COMMUNITY product could create a situation where personal injury or death may occur. Should Buyer purchase or use UNION COMMUNITY products for any such unintended or unauthorized application, Buyer shall indemnify and hold UNION COMMUNITY and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that UNION COMMUNITY was negligent regarding the design or manufacture of the part.

UNION COMMUNITY reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." UNION COMMUNITY reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Please contact UNION COMMUNITY, local UNION COMMUNITY sales representatives or local distributors to obtain the latest specifications and before placing your product order.

About UNION COMMUNITY

With regard to any fingerprint-related issues, UNION COMMUNITY is always in readiness to find out well fitted solutions, depending on customers' requirements and needs.

As a leading provider of fingerprint core technology, UNION COMMUNITY has set up wide variety of fingerprint product lines from fingerprint OEM modules to several choices of fingerprint finished products including access control, time & attendance, door lock, PC peripherals, safety box, etc, that incorporate UNION COMMUNITY's groundbreaking biometrics technology. Based on its proprietary algorithm, its own

sensor and in-house one-stop processing capability regarding hardware, software, product design, etc., our services to government sector and various commercial sectors like security, construction and enterprise are in full swing through fast problem-solving approach to meet market trends or demands. As a result, UNION COMMUNITY exports its market-proven fingerprint products to over 40 countries including Japan, USA, Europe and China.

As the biggest and the most promising company in the commercial sector of biometrics industry in Korea, UNION COMMUNITY was awarded “Korean World-class Product Award” for its excellent performance by Minister of Commerce, Industry and Energy in December 2005.

To be the world-class company in biometrics field, UNION COMMUNITY and all the members continue to do all-out efforts for the world-best quality product, creation of new paradigm and customers’ satisfaction through accumulated expertise and working experience from various reference sites and versatile hardware & software development.

About This Manual

This User Guide will provide the user with the easiest and fastest setup possible from the factory settings. It should be followed in order, with System Design and then System Setup. Additional settings are only needed for special setup procedures.

< Glossary>

● Zone

A 'zone' is a monitored area. An external contact device either Normally Open or closed can be connected to the controller for monitoring its state as (open/closed/shorted).

● Partition

A 'partition' is usually a larger area that may include a group of zones.

● Door

A door is a zone which is usually connected to the controller for monitoring the open/close state. A door is the same as a zone but is specific as an entry/exit area.

● Reader

A reader is an external device which is used for controlling access to a protected area. A reader can be a 'card reader' or 'fingerprint reader'.

● EOL (End of Line)

- The controller can monitor external physically connected Normally Closed or Normally Open contacts (zones).
- A resistor can be used in-line (series) with the device to allow a 3rd state (open/shorted/restored)

● Armed/Disarmed

When a partition is 'Armed' and a zone is violated (open/troubled) the controller will indicate an alarm condition (Bell output) and UNIS. When a partition is disarmed it is in a normal state and no alarm condition will occur. (Exception is forced alarm events and 24-hour zone types)

● Alarm

When a partition is in alarm it will sound a local siren and report an event to the server for notification.

● Bell or Siren

An external sounder or indicator can be connected for a local alarm notification

● Monitoring

This refers to all external events/hardware that are connected to the controller. When a device is connected to the controller it is said to be monitored by the MCP040.

Table of Contents

1. Introduction

1.1. Specification & Features

The MCP040 (Main Control Panel – 4 Lock) is an access controller and security system.

- 8 external RS485 Virdi Readers (4 lock – 2 Readers per door)
- 4 Wiegand Input Ports (v2.00 hardware supports 4 Wiegand Input)
- 4 Lock Outputs
- 4 Programmable Inputs
- 4 Programmable Outputs (v2.00 hardware supports 8 Outputs)
- 8 Zone Inputs
- 1 TCP/IP Ethernet Port (UNIS Server Software/ Webserver)
- Backup lithium battery for Real-time clock
- User Access Time Period
- 50,000 users
- ***5 cards per user, maximum 50,000 cards (new V2.00)***
- ***Anti-pass back (new V2.00)***
- ***UNIS server authentication (new v2.00)***
- ***Integrated Mini Web server (new v2.00)***
- 51,200 log events
- 1024 Access Groups
- 255 Schedules (outputs/arm/disarm)
- Backup battery monitoring (low battery, no battery)
- Monitored Bell/Siren Output

ITEM	SPEC	COMMENT
CPU	32Bit M3 Cortex	
MEMORY	128K SRAM	
	8MByte Serial Flash	~~100,000 fingerprints~~
Communication Port	TCP/IP(1), Wiegand (2)/(4)	
	RS-485 (19200BPS) (2)	
Temperature / Humidity	-20 ~ 60c / Lower than 90% RH	
Power Adapter	15VDC 6 A	
Power Supply	12VDC Maximum 6A +- 10%	
Lock Output (4)	12VDC Maximum 750ma each	
PGM (4)/(8)	12VDC open collector outputs	

1.2. Out of the Box

Verify the following components are included in the MCP040 package.

- Main Control Board (1)
- 15V/6A Power Adapter
- Hardware package includes:
  - 5 End of line resistors (2200ohm)
  - 4 End of line resistors (3900ohm)
  - Battery connector

2. System Design

The MCP040 factory settings allow for easy setup and minimal configuration. It is important to consider your system design and planning before beginning.

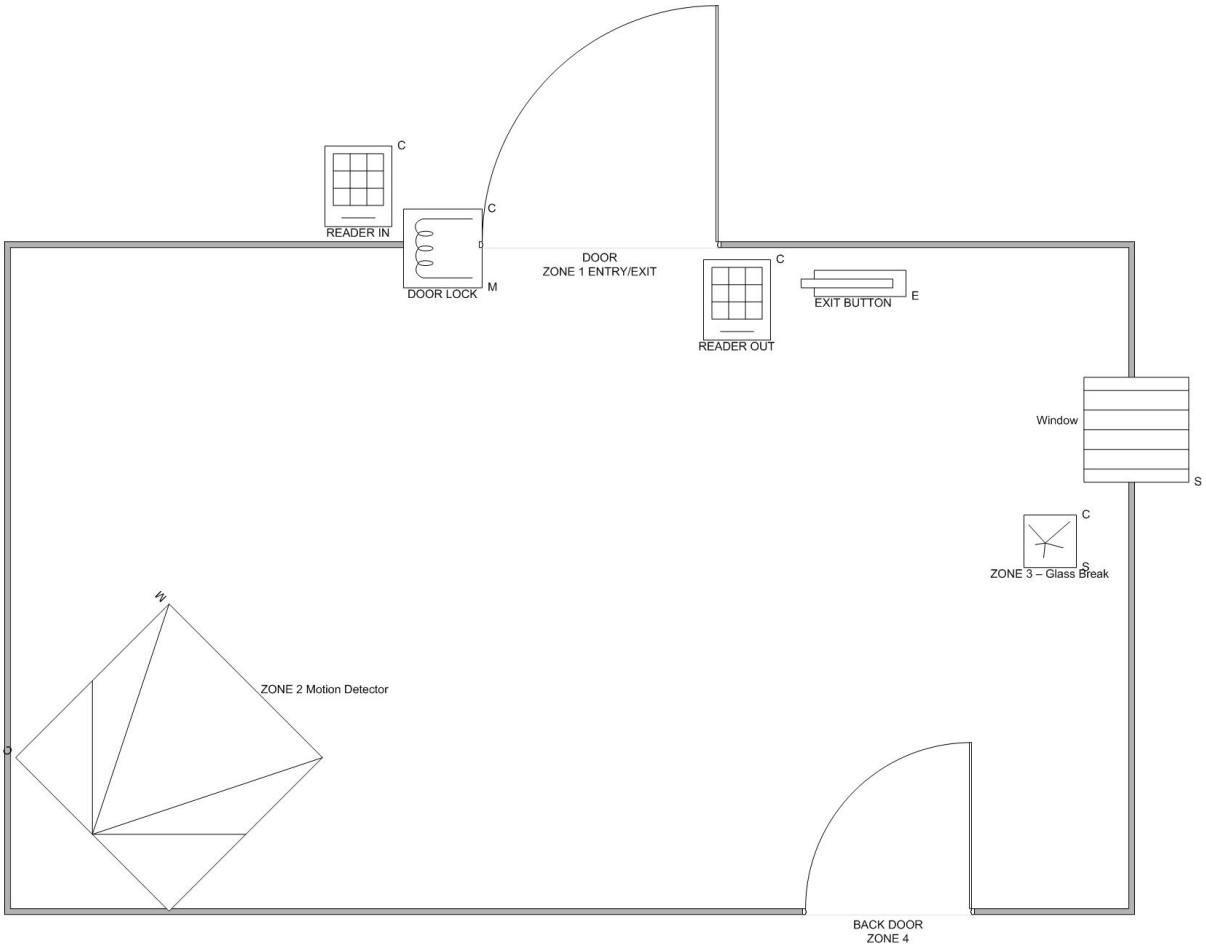
- Draw a layout diagram of the system showing all possible externally connected devices (readers, locks, zones, bell, etc)
- Determine the total current draw of the system.

MCP040 System Current Calculation (Maximum)

Supply Voltage	Maximum Current	Total Devices	Total (calculated)
12VOutput (J251/J252/J253)	2500mA		
Lock 1	750 mA		
Lock 2	750 mA		
Lock 3	750 mA		
Lock 4	750 mA		
PGM 1~8	30 mA each		
Bell/Siren	750 mA		
Other			
System Total	6000 mA (Maximum)		

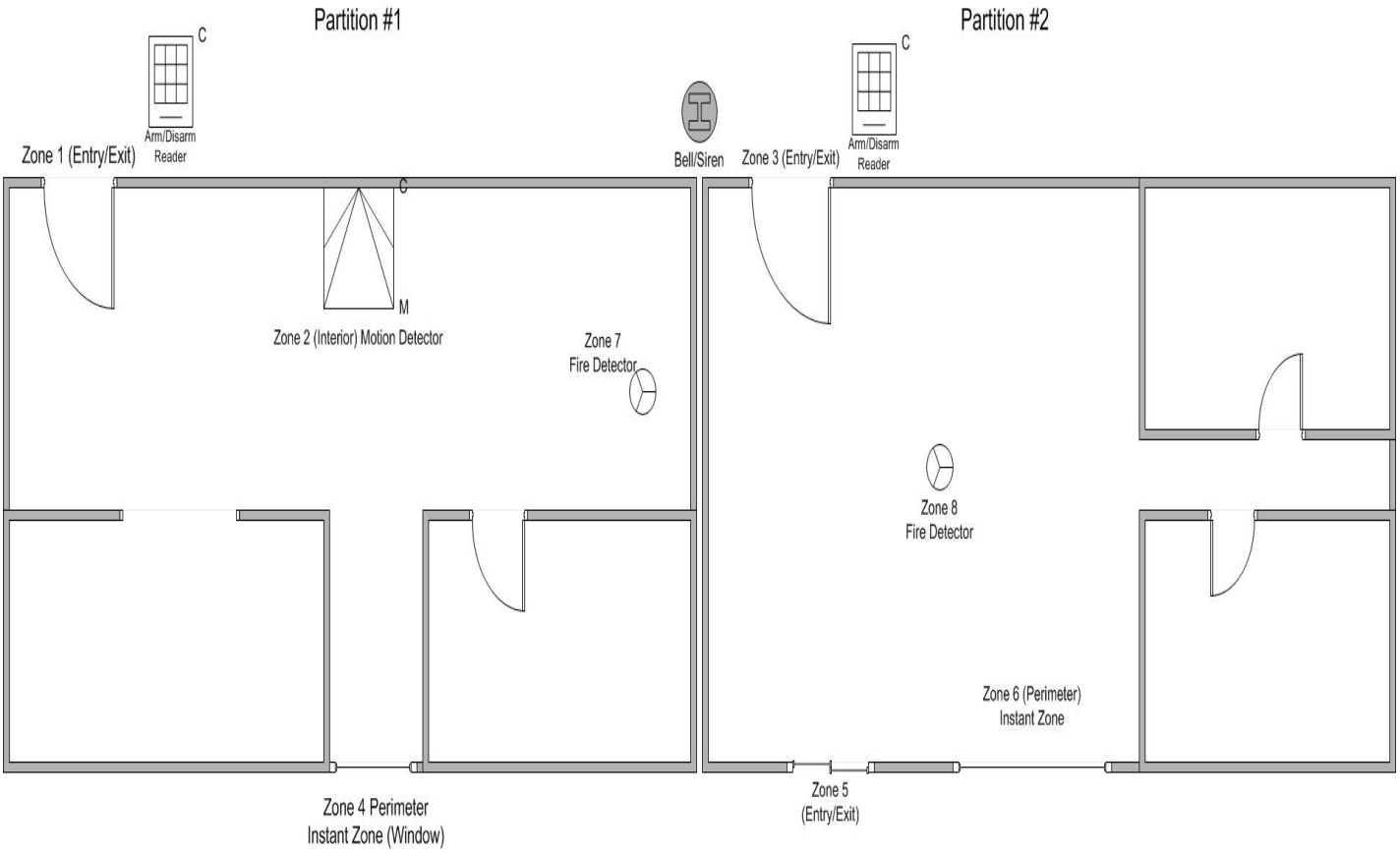
2.1. Access Control

Readers can be Virdi card readers, Virdi fingerprint readers or Wiegand readers. Normally all readers are located near an entry or exit point to allow access in or out.
Locks are located at the entry or access point. The electric locks will automatically open and close when the MCP040 accepts valid access.
Zones are areas throughout the building or room that will be monitored by the MCP040. Normally electric locks have a door monitoring signal 'Normally open or normally closed', this will sense when the door has been open or closed. This door monitoring feature should also be connected to the MCP040 ZN1~ZN8 zone input. If you choose to monitor other zone types (Glass break detectors, motion detectors or door contacts, they should also be connected to the ZN1~Z8 Inputs on the MCP040.
Exit Buttons are used to open the lock when leaving the building/room. The exit buttons should be connected to the IN1~IN4 on the MCP040.



2.2. Security Control

In a normal security application an area is referred to as a partition. Zones are assigned to each partition for monitoring intrusion. When a user enters their partition they will ‘Disarm’ the partition so no alarm occurs. When a user exits their partition; they will ‘Arm’ their partition so all zones are ready for monitoring. If any zone is opened during an armed period a local Bell/Siren will be activated and an alarm event will be reported to the server software.



2.3. System Default Settings

The following configurations are factory settings.

Reader IN/OUT Access
Reader#1 Assigned to Lock#1
Reader#2 Assigned to Lock#2
Reader#3 Assigned to Lock#3
Reader#4 Assigned to Lock#4
Reader#5 Assigned to Lock#1
Reader#6 Assigned to Lock#2
Reader#7 Assigned to Lock#3
Reader#8 Assigned to Lock#4
Wiegand Reader#1 Assigned to Lock#1
Wiegand Reader#2 Assigned to Lock#2
Wiegand Reader#3 Assigned to Lock#3
Wiegand Reader#4 Assigned to Lock#4

Door Monitoring
Lock#1 Assigned to Zone/Door#1
Lock#2 Assigned to Zone/Door#2
Lock#3 Assigned to Zone/Door#3
Lock#4 Assigned to Zone/Door#4

Exit Button
Exit Button#1 Assigned to Lock#1
Exit Button#2 Assigned to Lock#2
Exit Button#3 Assigned to Lock#3
Exit Button#4 Assigned to Lock#4

All Lock Open Period = 5 seconds

Example:
When a registered card is scanned at Reader#1 OR Exit Button#1 is activated, Lock#1 will unlock for 5 seconds. If door monitoring is used and the door is forced open or left open after access, an alarm will be indicated on zone#1

These settings can be changed from the UNIS -> Terminal Management-> Setup Options. See Section 4.5 Configuration Settings in UNIS.

3. System Setup

This section describes the basic steps for setting up your system. From the factory settings you do not need to change any additional settings from UNIS.

- Network Setup
- Reader Setup
- Lock Setup
- Zone Monitoring Setup
- Exit Button Setup

3.1. Network Configuration

3.1.1. Network Setup

The MCP040 does not have a user interface for system setup. Setup can only be done using the UNIS software. It is important to follow these steps to connect the MCP040 to the UNIS server software.

From the factory these are the following defaults for the MCP040 network.

MCP040 IP: 192.168.0.6
MCP040 Gateway: 192.168.0.1
MCP040 Subnet: 255.255.255.0
Server IP: 192.168.0.2
Terminal ID: 00000040

You can choice 1 of 3 methods for network setup of the MCP040 (Router/Direct PC/ UDP). In all cases if a connection is not possible disable in your PC the 'Windows Firewall' option.

3.1.1.1. Using a Router

1) In UNIS 'Terminal Management' -> Add Terminal, add the terminal ID of the MCP040 and click add.
2) Connect the MCP040 to your network using a standard CAT-5 network cable to the router.
3) Connect your PC using a standard CAT-5 network cable to the router.
4) Setup your router with a gateway address of 192.168.0.1
5) Setup your PC with a static IP address of 192.168.0.2
6) You should now see the device connected to UNIS. (If the device is not connected try disabling 'Windows Firewall' option)

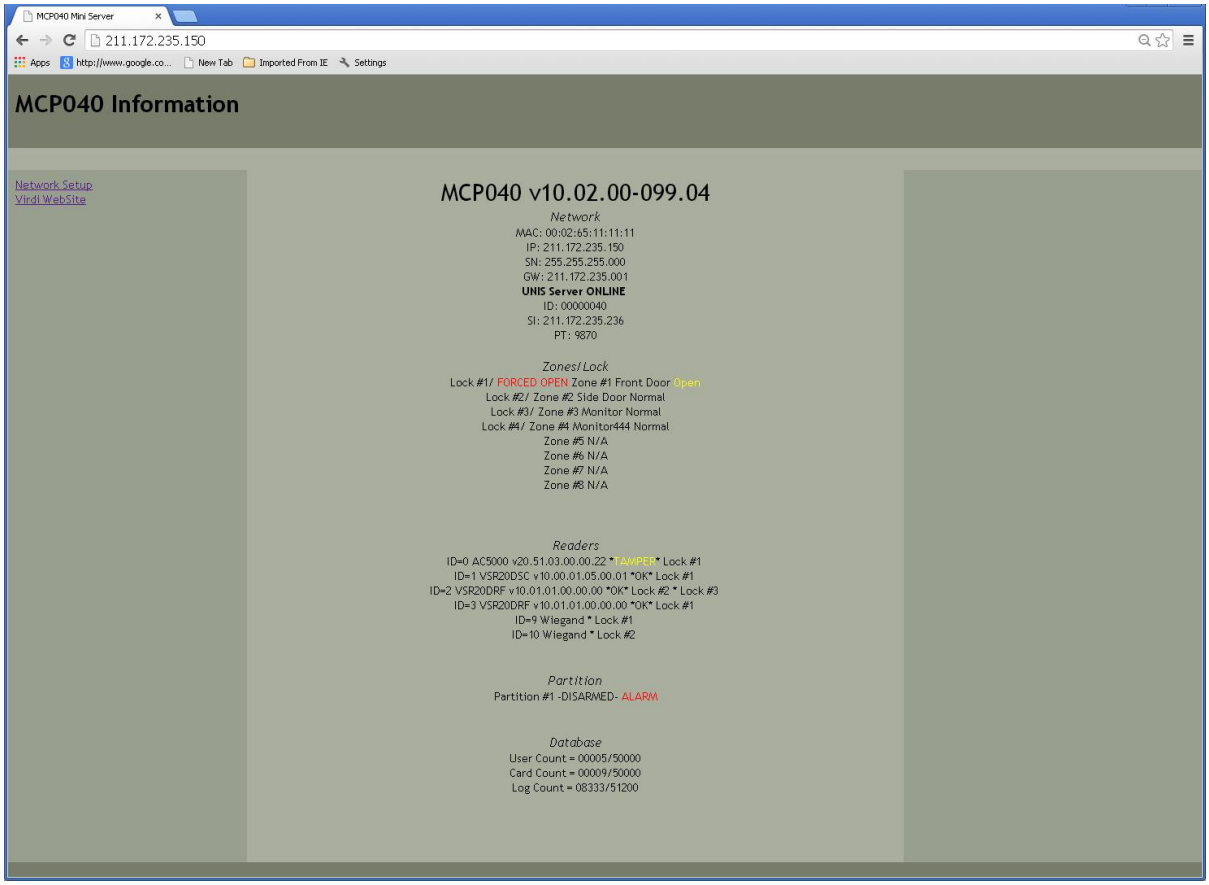
3.1.1.2. Direct to PC

1) In UNIS 'Terminal Management' -> Add Terminal, add the terminal ID of the MCP040 and click add.
2) Connect the MCP040 using a cross-over CAT-5 network cable to your PC.
3) Setup your PC with a static IP address of 192.168.0.2
4) You should now see the device connected to UNIS.

3.1.1.3. Web Server (Browser)

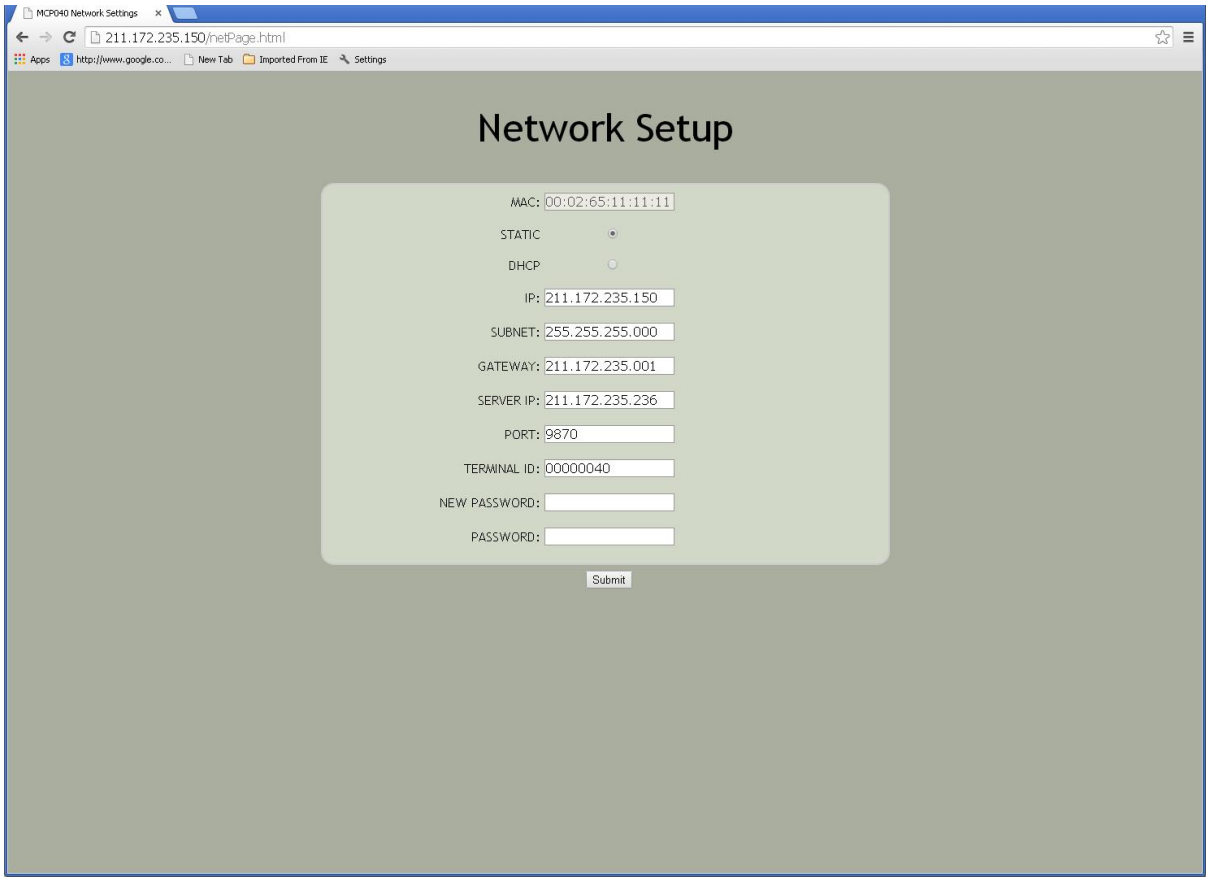
MCP040 has an integrated mini web server with basic network setup and status viewing. MCP040 should be connected to the same route as the PC you type in the address from.

1) Connect the MCP040 using a CAT-5 network cable to your PC.
2) Setup your PC with a static IP address of 192.168.0.2
3) In your PC web browser (best supported on Google Chrome or IE 8), type in the MCP040 default IP address 192.168.0.6
4) Status webpage should show, click on the link on the left side 'Network Setup'



5) Type in the information for your network requirements (IP, Gateway, DHCP, Terminal ID, etc)
6) Type in the default password, 0842650, and then click submit.
7) If you require changing the default password, you can enter the new password in the 'New PASSWORD' field. (16 characters maximum)
8) MCP040 will disconnect from the current network and setup the new information that was set.

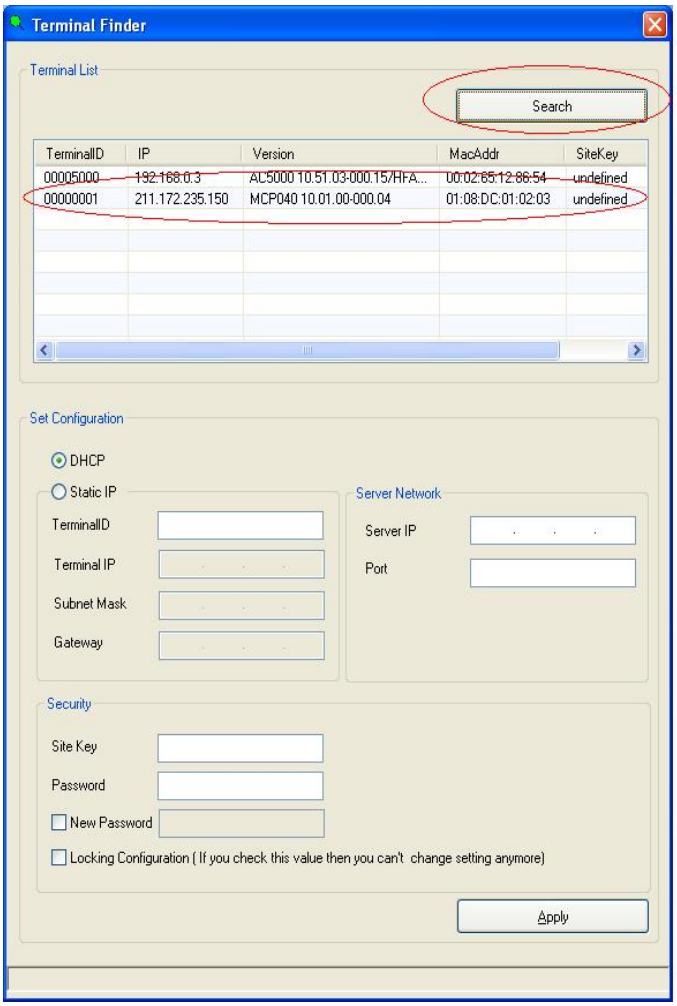
NOTE: PC should be on the same network as the MCP040 for browsing to work, or Port forwarding may need to be enabled in the router.



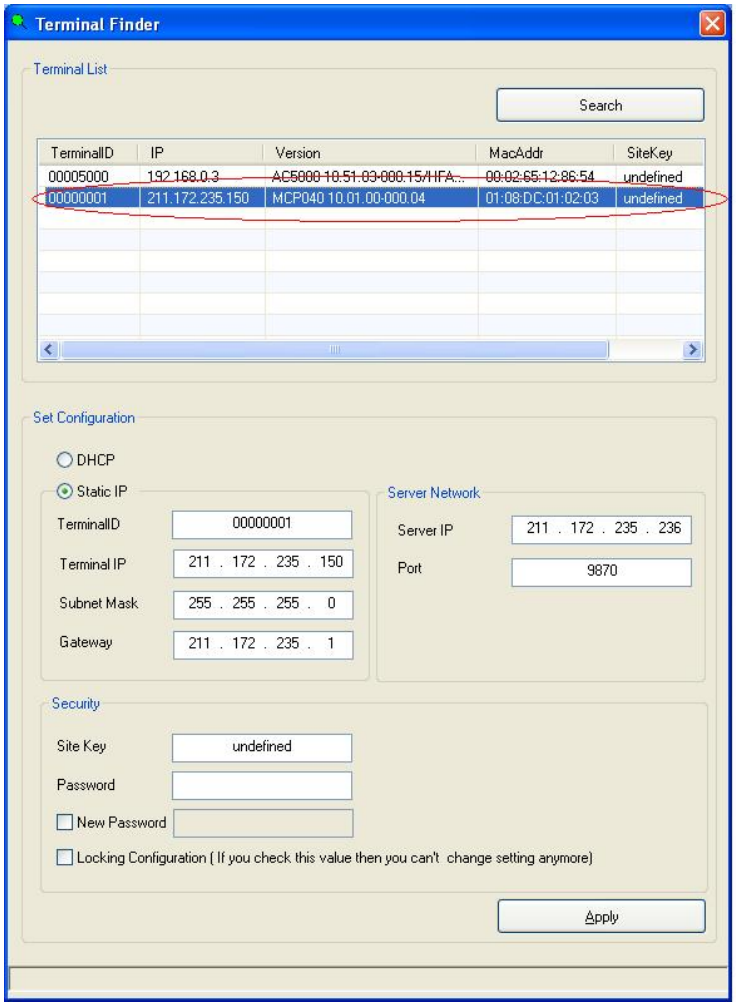
3.1.1.4. UDP Setup

In some cases, you may want to setup the MCP040 with a different IP or Terminal ID before connecting to the UNIS software. You will need an external program located in the Program Files->UNIS->Patch directory called 'terminal finder'. This program will allow you to search all Virdi devices on the network and setup (Terminal IP, Server IP, and Terminal ID)

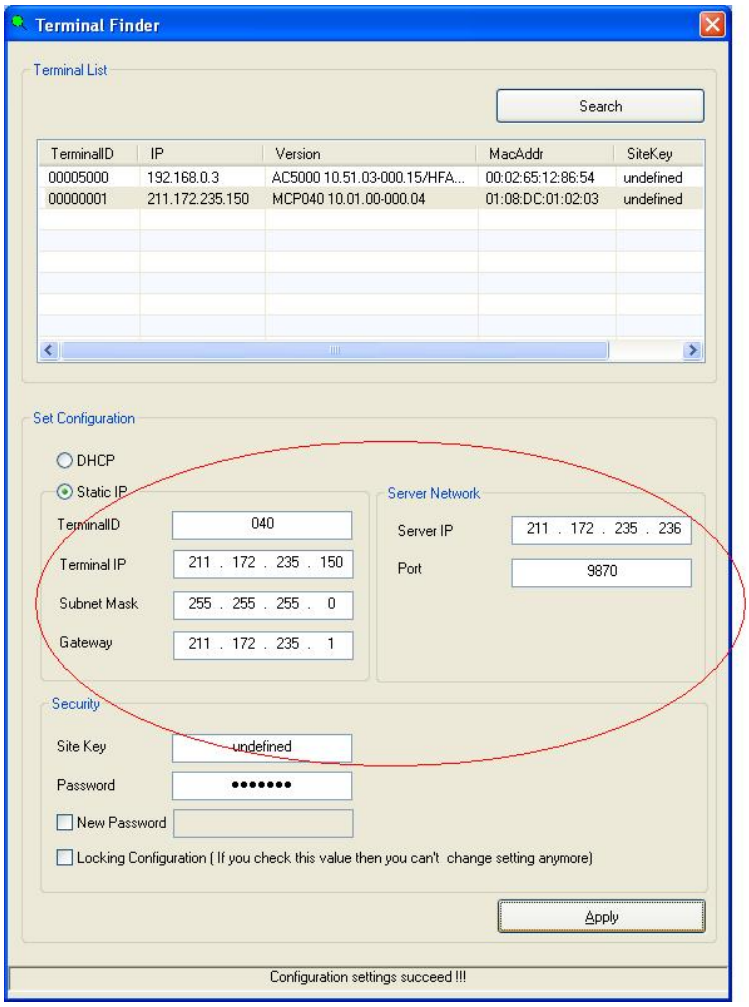
1) In UNIS 'Terminal Management' -> Add Terminal, add the terminal ID of the MCP040 and click add.
2) Connect the MCP040 to your network using a standard CAT-5 network cable.
3) Open the terminal finder program
4) Click 'Search' – a device list of all devices on the network will appear



5) Select the device in which you would like to modify. It should be highlighted and the current settings of that device will appear.



6) Modify the parameters you wish to change.



7) For greater security you must enter a password to change the values before you click ‘apply’, the default password is 0842650. This password can be changed. Also you can lock-down the controller so that future changes cannot be setup by UDP method. CAUTION, as you may not be able to setup the controller after this value is set from the Terminal Finder program.
8) Click ‘Apply’ and you should see ‘configuration settings success’ in the bottom of the screen.

3.2. Reader Setup

The MCP040 can support up to eight external Virdi readers connected to the RS485 (RDR+/RDR-) connection terminals. Additionally, 2/4 external Wiegand readers can be connected to the DO and D1 connectors

Supported Virdi Readers

- VSR20D-SC (Virdi Smart Reader SC) – Smart Card /Mifare Card Reader
- VSR20D-RF (Virdi Smart Reader RF) – RF Card Reader (125Khz)
- AC5000
- AC2100

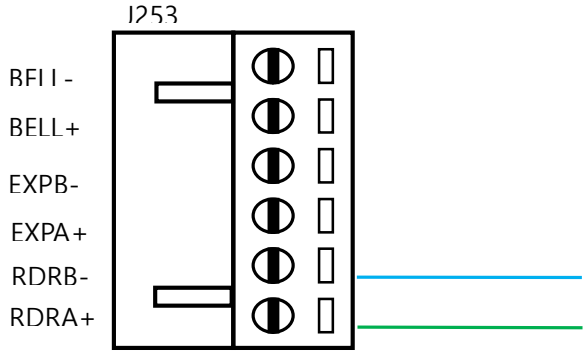
All readers require 4 wires for connection. All four wires should be home-run directly to the MCP040 controller.

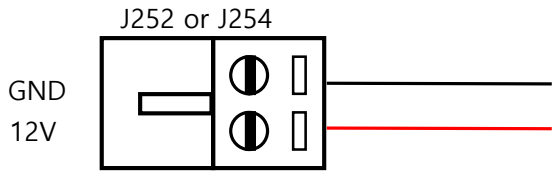
+12V
GND
RS485A+
RS485B-

Each reader connected to the 485 bus requires a unique ID to identify itself. All Virdi readers have a software or hardware programmable ID. On the VSR20 readers set the dipswitches to the desired ID number 0-7 (Reader 1~8). See the VSR20 installation manual.
Once the controller is re-powered all readers will automatically enroll with the controller. The controller has an auto-enroll procedure for all readers. This will take approximately one minute for all readers to be enrolled after power up.

Follow this procedure for connecting readers

1) Power down the MCP040 controller
2) Set the desired ID on the reader (dipswitches OR software programmed in the Virdi Reader)
3) Connect the 4 wires from the reader to the MCP040 controller.





4) Connect all readers
5) Power up the MCP040 controller.
6) The MCP040 will search for all readers connected to the RDR+/RDR- inputs for up to one minute
7) Scan a card on the reader and the reader should produce an error sound. If there is no communication the reader will emit one single beep.
8) See section 4.5.13 (UNIS MCP040 Status/Functions) for reader status.
9) Readers are considered enrolled when they are connected on power up and respond to the MCP040 polling. Their status will show as OK in the UNIS status screen. If a reader is enrolled and disconnected from the MCP040, the MCP040 will recognize the reader fault after 30 seconds. At this time the trouble will be reported to UNIS Real-Time event monitoring.

For detail wiring setup please refer to the MCP040 Installation & Wiring Guide.

The RX and TX LEDs for the Readers can be used for troubleshooting. After the auto-enroll process both LEDs will flicker normally at a constant rate if the readers are connected correctly.

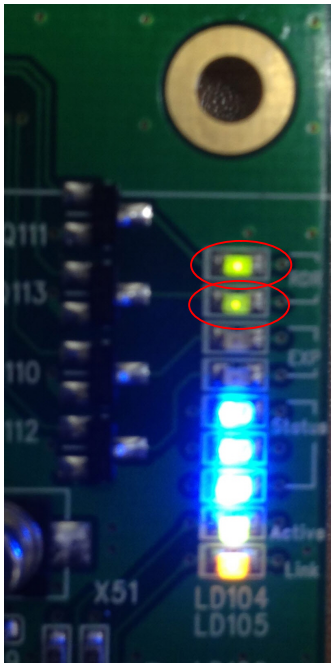
1) Observe the correct polarity when connecting the reader to RDR+/RDR-
2) Ensure the terminal is tightly securing the wire
3) Wire distance length and wire size should be considered.

Reader Notification

If the reader is connected correctly, the MCP040 will monitor the reader for connectivity.

1) If the reader loses communication to the MCP040 for 30 seconds, the reader will emit a double beep repeatedly every 30 seconds.
2) During the auto-enroll process the reader will flash its LEDs every 1 second.
3) If the MCP040 loses communication with the reader a notification will appear in the Event monitoring list (UNIS) after approximately 30 seconds. A trouble condition is reported.
4) If there is a door left open after the door warning period, the reader will emit a beep every 1 second.

LD104 = 485 RX
LD105 = 485TX



3.3. Lock Setup

The MCP040 can support up to four (4) external electronic locking devices.

Follow this procedure for connecting an electronic locking device.

1) Power down the MCP040
2) Connect the Power (RED) on the lock to the LOCK – NO/NC connector.
3) Connect the GND (BLK) on the lock to the GND Terminal
4) To verify the lock is working you should have a valid user to scan the card at the reader or you can use an exit button to open the lock.

For detail wiring setup please refer to the MCP040 Installation & Wiring Guide.

3.4. Zone/Door Monitoring Setup

A zone is an area in the system that requires monitoring. There are two types of zone monitoring circuits than can connect to the MCP040.
Normally Open (NO)
Normally Closed (NC)

Most electronic locks have a monitoring output for the door sensor (NC or NO). The purpose of monitoring is to sense when the door has opened/closed. This can be used for alarms, forced open events or door open too long events.
MCP040 has three configuration types for zone monitoring.
The hardware package will include the resistors needed for the below configuration(s).

No End of Line Zone Monitoring (No EOL)

This is the basic setting for monitoring zones. Only normally closed NC loops can be used for No EOL. The zone can be monitored for two states (opened and closed/restored)

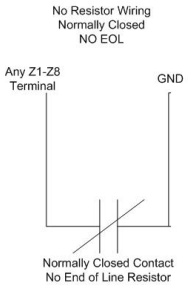
Single End of Line Zone Monitoring (EOL)

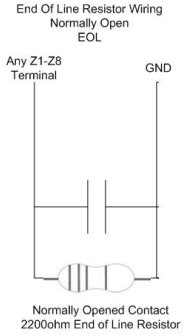
This configuration is used when you need to monitor three states of the zone (open, closed, and shorted) A 2200ohm 5% resistor is required. In order to make full use of this feature the resistor should be placed at the end of the wire run, at the monitoring device. The resistor should not be placed at the MCP040 terminal. An option in the System Settings should be enabled.
The zone can be monitored for three states (open,close,short)
Note: *EOL (End of Line Resistor) must be enabled for this feature – see Section 4.5.8*

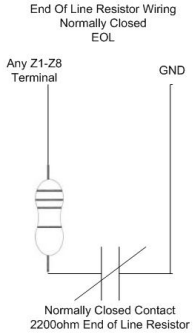
Zone Expansion End of Line (ZXEOL)

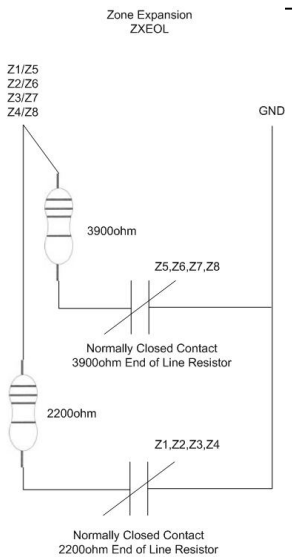
This configuration should only be used when you require more than four (4) zone inputs to be individually monitored. This configuration will allow two (2) zone inputs to be connected to 1 terminal input and still identify each input separately. You must enable Zone Double for the zone you wish to expand. This can be expanded up to 8 zones.
Note: *EOL (End of Line Resistor) must be enabled for this feature – see Section 4.5.8*

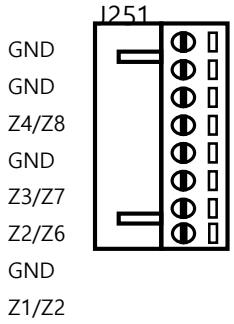
NOTE: After the EOL settings have changed and zones have been connected to the system it is recommended a normal walk test of each door/zone on the system, and confirm the open/restore state from the web server or UNIS status.











Notes:

1) Only Normally Closed circuit loops can use Zone Expansion EOL (ZXEOL).
2) Fire Zones cannot be used with Zone Expansion EOL (ZXEOL). Only 1 single fire zone per zone input with a 2200ohm resistor.

Follow this procedure for connecting a zone or door monitoring device to the MCP040.

5) Power down the MCP040
6) If you are using EOL, install the resistor at the device.
7) Connect the monitoring wire (NC or NO) to the ZNX terminal
8) Connect the COM/GND of the monitoring device to the GND terminal

For detail wiring setup please refer to the MCP040 Installation & Wiring Guide.

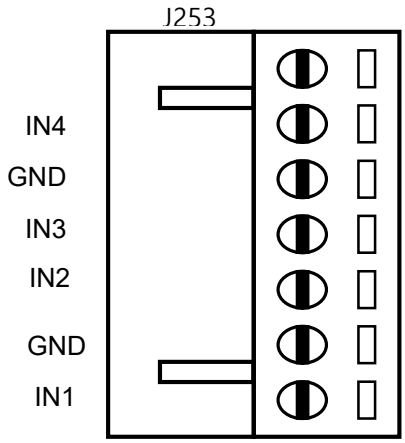
3.5. Exit Button Setup

Exit buttons are used at door exit areas only (opposite side of the access reader). When you need to unlock a door without requiring access authentication a simple push button can be used to allow access. Up to four (4) exit buttons can be connected to the MCP040.

Follow this procedure for connecting an exit button to the MCP040.

1) Power down the MCP040
2) On the switch (exit button) connect the NC or NO to the IN1-IN4 of the MCP040
3) Connect the COM/GND of the switch (exit button) to the GND terminal
4) To verify the connection simply press the exit button and the lock will open.

IN1 – Lock #1
IN2 – Lock #2
IN3 – Lock #3
IN4 – Lock #4



For detail wiring setup please refer to the MCP040 Installation & Wiring Guide.

3.6. Partitioning

A partition is a group of zones that function independently of each other. This may be useful in situations where there is more than one customer installation in a building with (1) MCP040.

Example (MCP040 #1)
Partition 1 – Store #1 – Reader 1, 2, zones 1, 2, lock 1, Users 1,2,3,5
Partition 2 – Store #2 – Reader 3, 4, zones 3, 4, lock 2, Users 10,11,12,13
Partition 3 – Store #3 – Reader 3, 4, zones 5, 6, lock 3, Users 5, 8,9,23
Partition 4 – Store #4 – Reader 5, 6, zones 7, 8, lock 4, Users 7, 6

Partitions can be individually armed and disarmed for security.
See Section 2.2 Security Control

To use partitioning the following is required:

1) Reader Mode = ACCESS+SECURITY
2) User management (ACU Partition), user should be enabled for the partition they are assigned.
3) Zone Assigned to Partition.

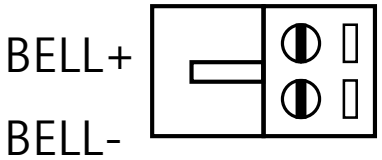
If a reader is set for Access Mode only and a user does not have any partitions assigned, the partition will always disarm first before access/opening the door (providing the reader has locks assigned), in order to prevent false alarms.

If a lock (1-4) has a zone assigned to a partition that is arming (UNIS, reader or schedule arming), the lock will always close when arming. See UNIS Lock Configuration.

4. Additional Setup Options

4.1. Bell/Siren Output

An external bell, light or sounder can be connected to the MCP040 for a local alarm annunciation. If no bell or siren is connected a 2200-ohm resistor should be connected across the BELL+ and BELL- terminals. This input is supervised, a trouble condition at UNIS will be generated if no bell or siren is connected. The bell output will activate during any alarm condition.
- Door Forced Events (Steady Output) – Turn off after all forced zones are restored.
- Zone Alarm (Steady Output) – Turn off after bell sounder period OR system is disarmed
- Fire Alarm (Pulsed Output 1 second ON, 1 second OFF)



4.2. Wiegand Input(s)

The MCP040 can support (2-4) external wiegand readers.

The default wiegand format is 26/34bit. If you wish to customize this bit format to another type, this can be done in UNIS -> Tools->Management->Set Wiegand Input Format. A detail help guide is available in UNIS for setting up the bit formats.
For detail wiring setup please refer to the MCP040 Installation & Wiring Guide.

4.3. Battery Monitoring

The MCP040 will monitor the backup battery voltage and report the Low Battery condition to the UNIS server.

Low Battery Voltage = 11.3VDC +/- 10%
Battery Cut-Off Voltage = 10.8VDC +/- 10%

The MCP040 will check the battery 30 seconds after power up and approximately every 4 minutes 30 seconds afterwards.

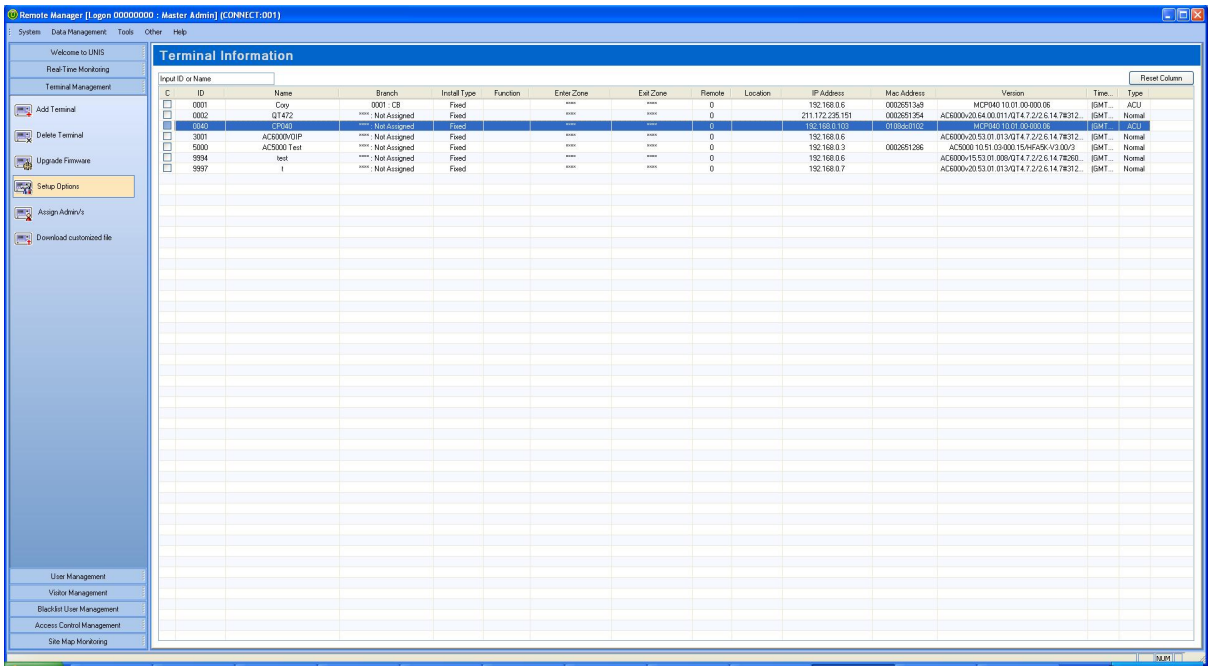
4.4. AC (Power Supply Monitoring)

The MCP040 will monitor the status of the AC (Main power) connected to the PWR+, PWR- terminals. When AC is disconnected for longer than 10 seconds a AC Loss trouble condition will be reported to the UNIS server and the MCP040 will be powered from the battery back-up.

4.5. Configuration Settings in UNIS

After a connection with the UNIS server software is established detail setup parameters may be customized or changed depending upon your application. You should ensure section 3 ‘System Setup’ is fully complete, all readers, exit buttons, external devices are connected and working before you continue with detail setup parameters.

In UNIS select the ‘Terminal Management’ TAB on the left column, then highlight, by selecting, the MCP040 you wish to setup. Next, select the ‘Setup Options’ on the left column.



The MCP040 is a stand-alone access control device. It does not require the UNIS server for normal operation. It only requires setup by the server. User setup, configuration and/ or real-time monitoring can be used for UNIS.

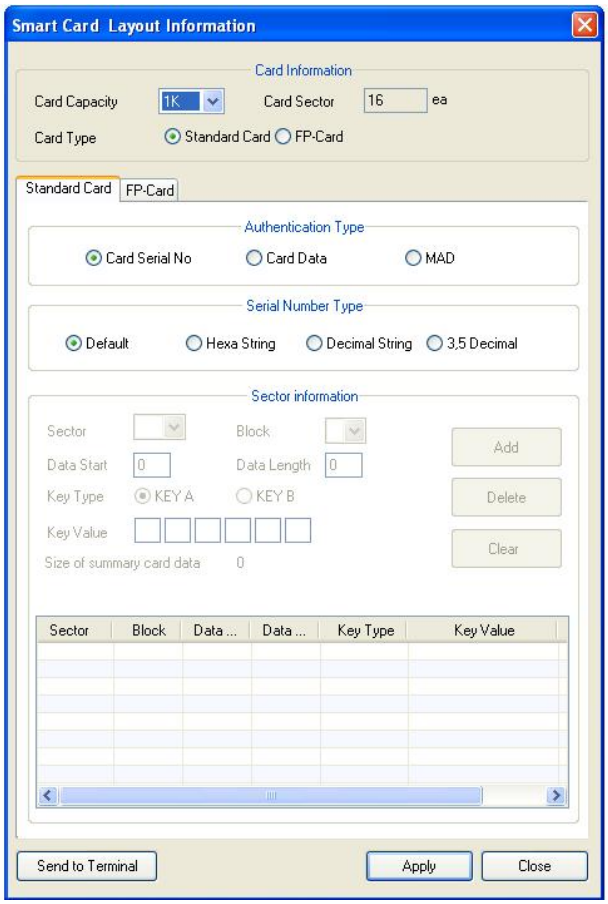
4.5.1. Card Format Setup

In the MCP040 users are identified by card numbers, for fingerprints the user id is used. It is important that the card format you use to register the card at UNIS (Hamster device) is the same format in the MCP040 card format. In UNIS->Tools->Design Card Layout the 'Standard Card Tab' should be selected, select the 'Serial Number Type', choose the card serial number type you wish to use and send to MCP040.
Dummy Readers (VSR20DSC, VSR20DRF) will convert the card number according to the MCP card format setting.
AC2100 and AC5000 already convert the card according to their card format setting. MCP will not convert the card again.

Type	RF Readers	Smart Card Readers
Default	3/5 Digit Decimal	X byte HEXA
Hexa String	5 byte HEXA Reversed	X byte HEXA Reversed
Decimal String	10 Digit Decimal	10 Digit Decimal
3/5 Digit Decimal	3/5 Digit Decimal (same as default)	3/5 Digit Decimal

X = variable card length

After you select the card serial number format click 'Send to Terminal' and then select the MCP040.



4.5.2. UNIS Reader Configuration

Reader configuration allows you to assign a lock to the reader, open period for the lock and other variables.

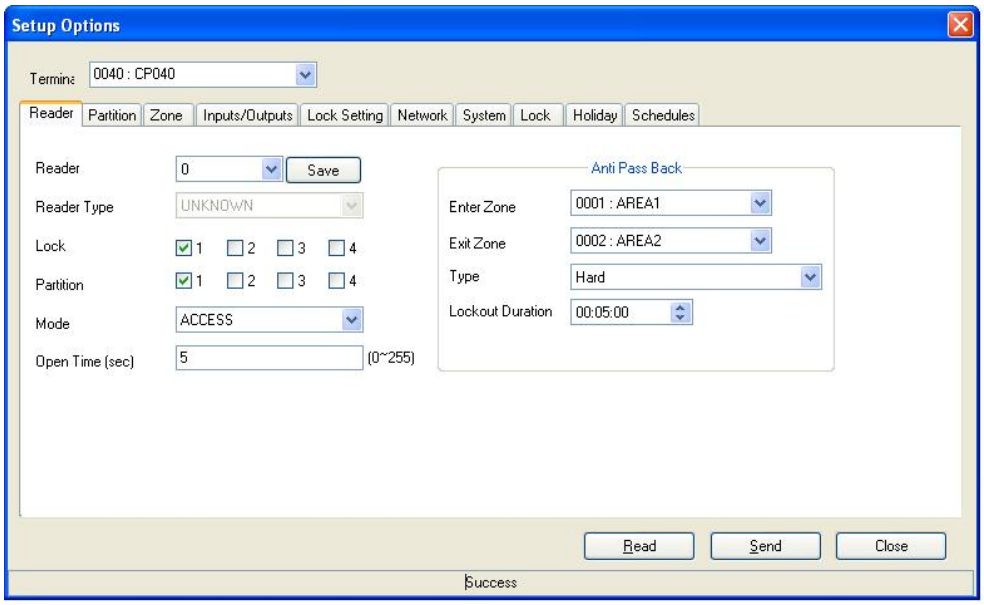
Select the reader in which you would like to read or setup (0-7, Wiegand 1-4), then click ‘Read’. After any changes have been made to the reader, click ‘Save’, then click ‘Send’, this will send the parameters to the MCP040.
Reader Number (0-7) – This number is the 485 ID set on the reader.

If the reader is connected correctly, you will see the reader type of the reader. This field cannot be changed; the MCP040 determines the reader type.

Reader Types:

VSR20RF – RF 125 KHz Card Readers
VSR20SC – Smart Card 13.56MHz Card Reader
AC2100
AC5000
Wiegand

If the reader is not connected correctly or unused you will see ‘UNKNOWN’ in the reader type field.



Lock: 1-4. A Reader can be assigned to multiple locks. When a registered card is scanned at this reader, the Lock number that is assigned will unlock.

Partition: 1-4. A Reader can be assigned to multiple partition areas. Default Partition 1. At least 1 partition should be assigned.

NOTE: *If a reader is assigned to multiple partitions, the reader will only display the (arm/disarm/exit) status of the first assigned partition. The reader cannot display the status of more than 1 partition.*

Mode: ACCESS, ACCESS+SECURITY. This value determines how the reader will operate when a user is successfully authorized.

> **ACCESS**: When a valid user is authorized the lock assigned to the reader will open for the duration of the Open Time.
>
> **ACCESS+SECURITY**: When a valid user is authorized the lock assigned to the reader will open for the duration of the Open Time.
> If the F1 key is pressed (AC2100/5000) and a valid card/user is authorized, the partition assigned to the reader and user will ARM. If the partition is already armed the partition assigned to the reader and user will automatically disarm and unlock the door.

Open Time (Lock Open Time).
When a valid user is authorized at this reader the lock will unlock for the programmed open time.
The relay can be triggered to remain open from 100ms up to 250 seconds (4 minutes, 10 seconds)

To setup this function, use the following examples:

E.G.
If you want to trigger the relay for 1 second, insert 1 into the “Open Time” field.
If you want to trigger the relay for 5 seconds, insert 5 into the “Open Time” field.
If you want to trigger the relay for 60 seconds, insert 60 into the “Open Time” field.

However, if you want to trigger the relay for less than 1 second, please use a value from the table below.

100ms	= 255	
300ms	= 254	
500ms	= 253	
700ms	= 252	
Always Active	= 251	(Lock always opened)
Toggle	= 0	(Lock always opened, next authorization Lock closed)

E.G.
If you want to trigger the relay for 100 ms, insert 255 into the “Open Time” field.
If you want to trigger the relay for 500 ms, insert 253 into the “Open Time” field.

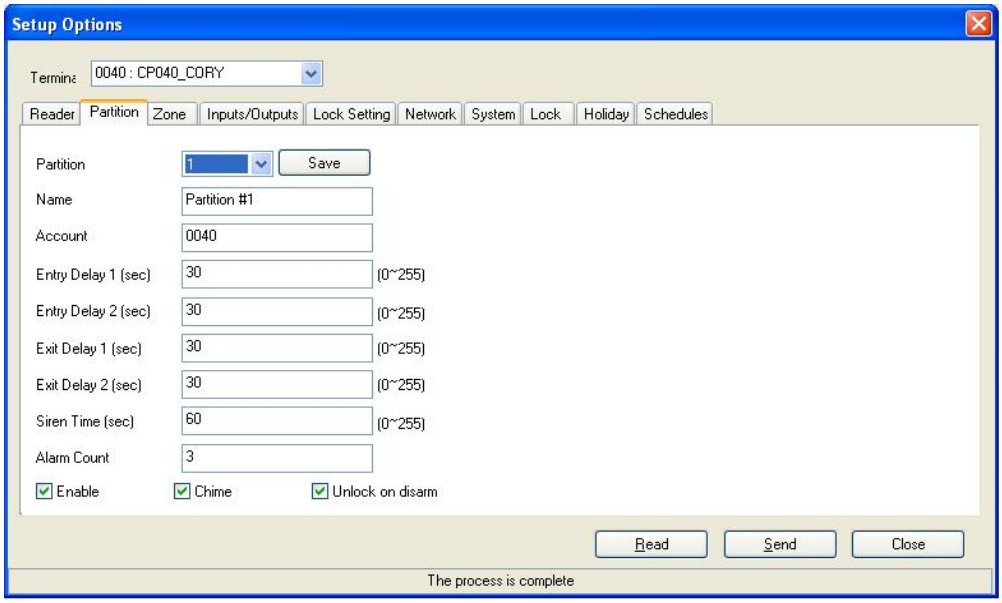
NOTE: *When the lock and partition settings are changed verify the lock is connected to the correct NC/NO lock output on the terminal connectors. See configuration manual.*

Anti-passback:

See 4.5.9 Anti-passback for detail setup information.

4.5.3. UNIS Partition Configuration

Partition setup applies to security mode. For normal access control these settings do not need to change. A partition is an independent group of zones. You can assign multiple zones (see zone setup) to a partition area. A partition area may be useful in situations where two separate offices in one central building. The MCP040 will allow up to four partitions.



Partition: 1-4. Select the partition (1-4) you wish to change, then click ‘Save’ and ‘Send’

Name: (ASCII 16 digits). The maximum length is 16 ASCII Characters. This name is only used for display purposes so you can easily identify your partition.

Account: (Hexadecimal 4 digits). For CMS (Central Monitoring Service) reporting an account number is needed per partition. This value is currently viewable in UNIS when a reporting event occurs. Each digit is programmed as 0-F Hexadecimal. The default account number is the same as the terminal ID ‘0040’
All system events (AC, low battery, etc will always use the terminal id last four digits)

Entry Delay 1/2: (0-255 seconds). Default 30 seconds
Exit Delay 1/2: (0-255 seconds). Default 30 seconds
Entry/Exit 1 delay is for all EXIT1 type zones.
Entry/Exit 2 delay is for all EXIT2 type zones.
Zones defined as EXIT1 or EXIT2 type will have an entry and exit delay. The exit delay will start as soon as arming is initiated. All EXIT1 or EXIT2 type zones can be opened or closed during the exit delay without causing an alarm. This will give the user time to arm the system and leave the premises. After the exit delay has expired the zone is armed. Opening the zone will start the entry delay, allowing the user to enter the premises and disarm. If the partition is disarmed before the entry delay expires no alarm will be generated. During Exit Delay all readers assigned to the partition will beep

every second and flash the LED. This is indication for exiting. During the armed state all readers will flash their LED every 1 second.

Siren Time: (0-255 seconds). Default 60 seconds. When any zone alarm occurs on this partition the BELL output will turn on for this period. If the system is disarmed before the siren time has expired the BELL output will turn off.

Alarm Count: (0-255). Default 3: This alarm count is the maximum amount of times the partition will sound the siren and report the alarm event to UNIS during an armed period. In cases where there may be a faulty zone that is constantly alarming and restoring, this period will ensure only a maximum count per zone. This value may be useful in reporting to UNIS, to prevent false alarm reporting.
If this value is 0 the alarm count is unlimited (no limit).
NOTE: This alarm count only applies to zone types EXIT1, EXIT2, INTERIOR and INSTANT.

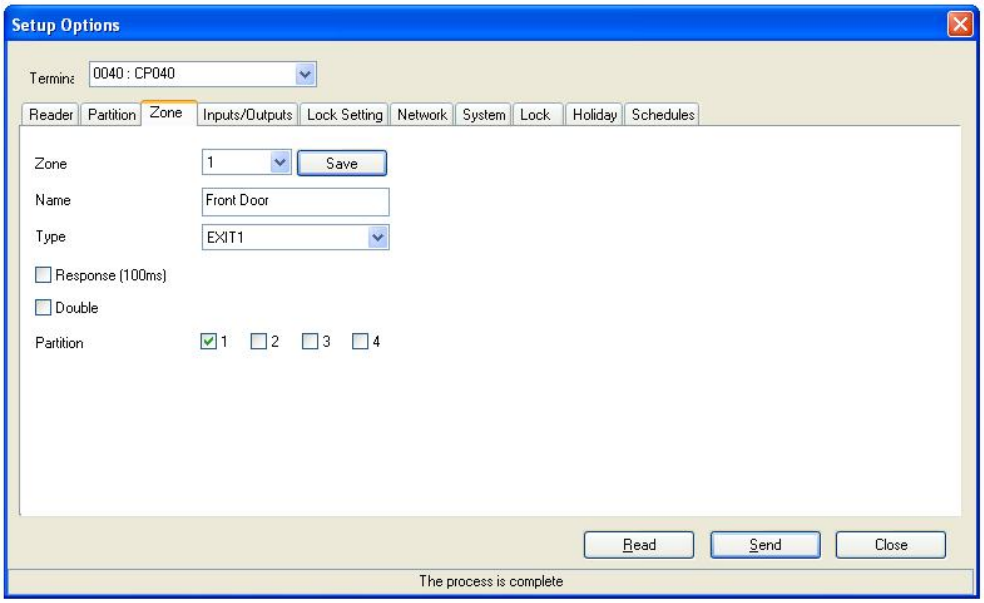
Enable: Check this box if you want to use this partition.

Chime: If this box is checked, when the system is disarmed only, all zones that are of type EXIT1, EXIT2 or INSTANT and are assigned to this partition, the reader will sound 2 short beeps when the zone is opened. This can be used as an indicator when the door is opened. This is not an alarm indicator, only an indicator that the zone is open.

Unlock on Disarm: If this box is checked, the lock assigned to the reader's partition will automatically unlock when the partition is disarmed. The lock will always be opened until the partition is re-armed again or the next authorized user access the partition.
Note: This only applies to reader access, UNIS disarming and zone arm/disarm.

4.5.4. UNIS Zone Configuration

Zone configuration is related to door/monitoring or alarm monitoring. When the zone is opened or closed the MCP040 will react differently depending on the type of zone.



Zone: 1-8. Select the zone (1-8) you wish to change and then click 'Save and Send' after all setup is completed.

Name: (ASCII 10 digits). The maximum length is 10Ascii Characters. This name is only used for display purposes so you can easily identify your zone.

Type: (List).

UNUSED – if nothing is connected to the Z1/Z5 terminal on the MCP040 select this option

Burglary Type Zones

These types of zones are active and alarm only when the partition is armed. These should be used for Lock monitoring.

EXIT1 – This zone type will have an exit and entry delay when opened. The exit and entry delay will follow the times that are programmed in the partition programming EXIT1 Entry/Exit Delay
Normally an entry or exit door will have this type. (Bell Active and Reporting)

EXIT2 – This zone type will have an exit and entry delay when opened. The exit and entry delay will follow the times that are programmed in the partition programming EXIT2 Entry/Exit Delay. Normally an entry or exit door will have this type, if you have a secondary door which requires a different delay than the EXIT1 type you can choose this type. (Bell Active and Reporting)

INSTANT - This zone type is used when monitoring a perimeter area. This zone will have no entry or exit delay and will initiate an alarm immediately if the partition is armed and the zone is opened. (Bell Active and Reporting)

INTERIOR – This zone type is used when monitoring an interior area. This zone type will follow the entry/exit delay. If the partition is armed and there is NO entry or exit delay active this zone will initiate an alarm immediately (Bell Active and Reporting). An example is a motion detector or inside door.

24 Hour Type Zones

These zone types are active all the time, whether or not the partition is armed or disarmed.

EMERGENCY24 – Bell Active and Reporting
SILENTPANIC – No Bell (Silent) reporting only.
WATER/GAS – Bell Active and Reporting. When reporting the event code for CMS is different, so the zone can be identified at the monitoring point (UNIS)
FIRE – Normally a fire zone is monitored for alarm state and trouble state. Trouble state will occur if the fire zone is disconnected. An alarm will occur if the fire zone is shorted. A 2200ohm resistor must be used for monitoring fire zones.
Fire zone restore = 2200ohm resistor
Fire alarm = short, loop shorted condition
Fire trouble = no resistor, loop open

Bell Active – pulsing 1 second ON and 1 second OFF and Reporting

ARMDIS – An external push button or external controller signal can arm or disarm the MCP040 when this zone is opened and closed.

Zone Response: (Check Box). Normally the default state for loop response is monitored at 400ms. If the zone is open/closed within 400ms a state change will occur (alarm or restored).
Some external zone devices require faster response periods for capturing the state change, if this box is checked the zone response will be at 100ms.

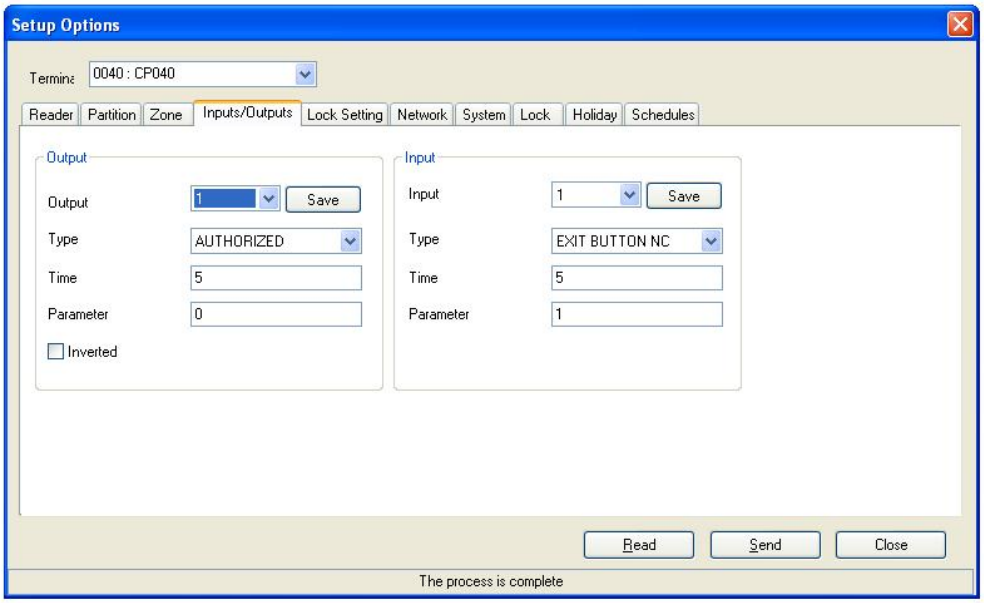
Zone Double: (Check Box).
See section 3.4 Zone/Door Monitoring Setup. If you require more than the standard 4 hardware zone inputs, the zone can be setup to connect two zones to the ZX input on the MCP040. This will identify each zone connected to the ZX input separately. i.e. Zone 1 and Zone 5.
Select this option only if you require more than the 4 standard hardwire zone inputs.

Zone Partition: (Check Box 1-4).
Select the partition in which you want to assign this zone.

4.5.5. UNIS Input/Output Configuration

The MCP040 has four inputs for monitoring external devices/equipment (IN1-IN4). All four inputs are setup at default for 'Exit Buttons'. When the exit button is activated the lock will open.
If a third party device/controller is needed for fire alarm monitoring, the output of the controller can be connected to the MCP040 input for monitoring of a fire alarm condition.

The MCP040 has four/eight outputs for signalling external devices/equipment.



Output: 1-8. Select the output (1-8) you wish to change and then click 'Save and Send' after all setup is completed.

Inverted: (Check Box) Normally the output is active low, if this box is check the output switch from HIGH state to LOW state.

4.5.5.1. Output Setup

Depending on which ***'Type'*** is selected the ***'Parameter'*** value will have a different meaning. See chart below for ***'Type'*** and ***'Parameter'*** description for Output Settings.

Output Type	Activation Period	Parameter Value	Time (seconds)
Authorized	Any user is successfully authorized	Lock #1~4	See Below Activation Period.
Unauthorized	Any user is unsuccessfully authorized	Lock #1~4	
Schedule	See 4.5.11 **UNIS Schedule Configuration**	Not Used	
Alarm	When an alarm occurs	Partition #1~4	
Trouble	When any system trouble occurs (fire trouble, AC trouble, battery trouble, bell trouble, reader trouble)	Not Used	
Fire Alarm	When a fire alarm occurs	Partition #1~4	
Silent Alarm	When a silent alarm occurs	Partition #1~4	

4.5.5.2. Input Setup

Depending on which ***'Type'*** is selected the ***'Parameter'*** value will have a different meaning. See chart below for ***'Type'*** and ***'Parameter'*** description for Input Settings.

Input Type	Activation	Parameter Value	Time (seconds)
Exit Button NC/NO	Open lock for time period when activated	Lock #1~4	See Below Activation Period.
Fire NC/NO	Fire Bell will activate for partition	Partition #1~4	Not Used
Security NC/NO	Arm/Disarm selected partition	Partition #1~4	Not Used

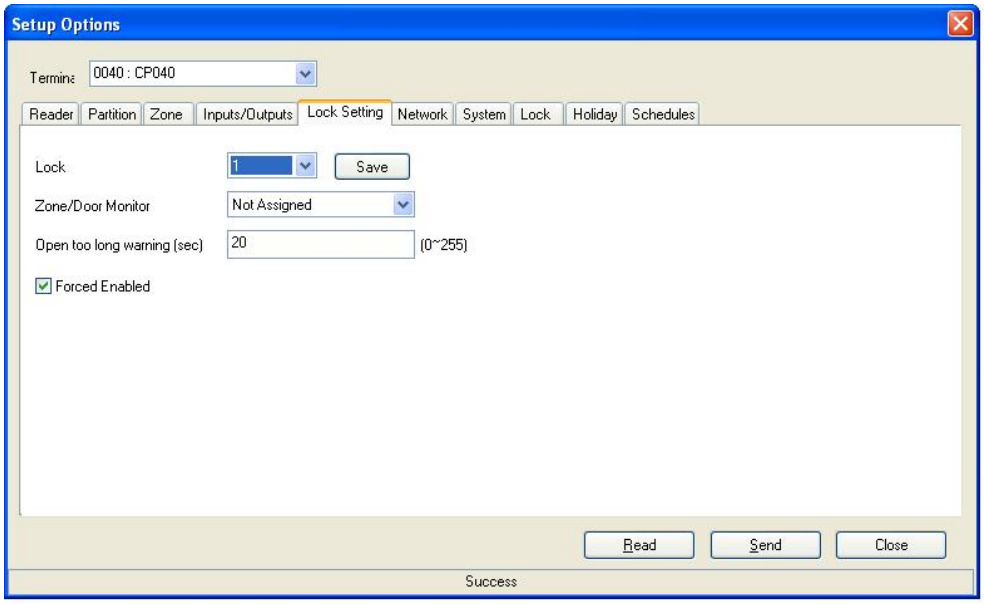
Input: 1-4. Select the input (1-4) you wish to change and then click 'Save and Send' after all setup is completed.

Activation Period

255 = 100ms
254 = 300ms
253 = 500ms
252 = 700ms
251 = Always Active
250~1 = seconds
0 = not activate.

4.5.6. UNIS Lock Configuration

The lock settings apply to the four locks on the MCP040. Each lock can be assigned a zone number for monitoring the door status, open too long period and forced open events.



Lock: 1-4. Select the lock (1-4) and then click 'Save' and 'Send' after all setup is completed.

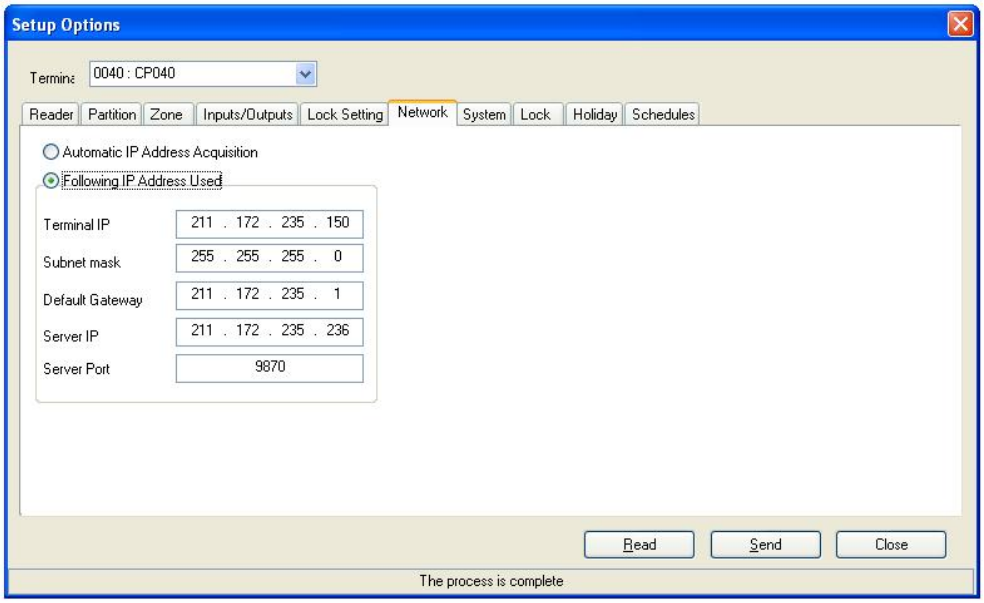
Zone/Door Monitor: 1-8. Select the zone (1-8) you wish to assign to the lock. Most door strike type locks have a door monitoring sensor wire (Normally Closed or Normally Open). You can monitor the door status by connecting this wire to the selected zone input Z1~Z8. If the lock does not require monitoring, select 'Not Assigned'

Open Too Long Warning: (0-255 seconds). Default 20 seconds. After a user is successfully granted access the lock will open for the Lock Open period (See 'Open Time' in Reader programming). If the door remains open after the lock open period, the open too long warning period will start. After the open too long warning expires; the reader in which the lock is assigned to will emit a fast beep tone every 1 second to alert the user as a warning that the door remains open. When the door is closed the beeping will stop.
NOTE: This feature only applies if the door sensor wire is connected to the zone input on the MCP040. The zone type must be EXIT1, EXIT2, INSTANT or INTERIOR type.

Forced Enabled: (Check Box). If selected and the door is forced opened without granting access an alarm is generated. The bell output will activate for the Siren Time OR if the door is closed the siren will turn off. A forced open event will be sent to UNIS.

4.5.7. UNIS Network Configuration

After establishing a connection with UNIS detail network settings can be changed. It is important to verify the network settings are correct before selecting 'Send'. The MCP040 will use the changed settings for reconnecting to UNIS, if the settings are incorrect you will not be able to establish a connection with UNIS. If you cannot re-establish a connection please follow section 3.1.1.4 UDP Setup.



Automatic IP Address Acquisition: Select this if you have a router that has DHCP enabled and you wish to automatically assign an IP, Subnet Mask and Gateway. If this option is selected you cannot select (Terminal IP, Subnet mask, Default Gateway), the router will automatically have assigned these addresses. Default OFF.

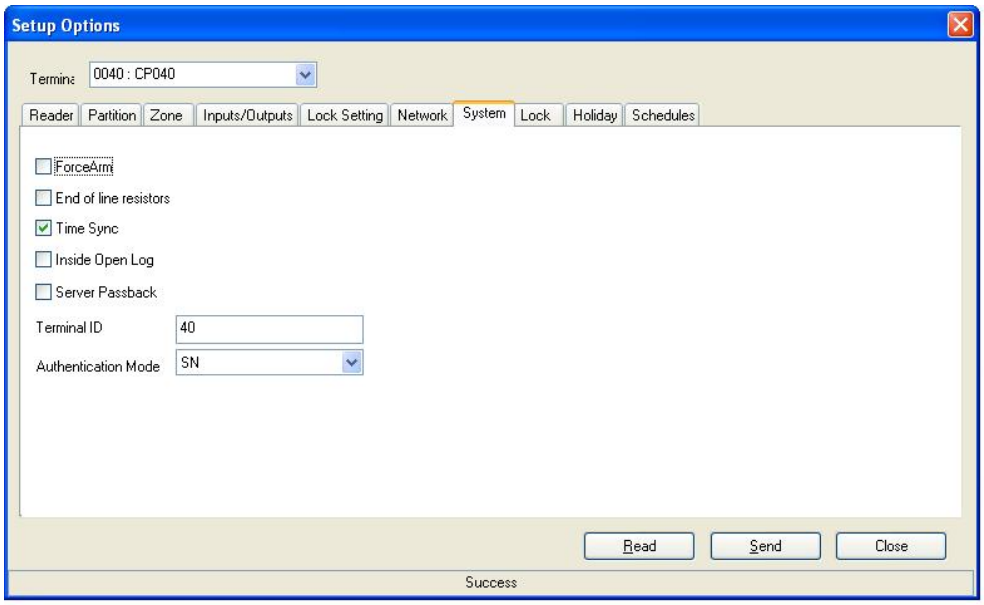
Following IP Address Used: Select this if you have a fixed, Static IP that you are using.

Terminal IP, Subnet Mask, Default Gateway: Enter the fixed IP addresses for these selections. Default 192.168.0.6, 255.255.255.0, 192.168.0.1

Server IP and Server Port: Enter the server IP and server port. Default: 192.168.0.26 Port: 9870

4.5.8. UNIS System Configuration

System configurations apply to all areas of the MCP040. These settings are global and are included for all partitions.



Force Arm: (Check Box). This option is for security mode only. Normally a partition should not be armed if a zone (door) is opened. All zones on the partition should be in a restored state before arming. If you wish to override this functionality and allow any zone to be open when arming, then check this option.

End of Line Resistors: (Check Box). This option applies to monitoring zones in the MCP040. See Section **3.4** 'Zone/Door Monitoring Setup**'**

Time Sync: (Check Box). If you wish to receive periodic time updates from the UNIS server select this setting. If this is not set, then the MCP040 will use the internal RTC (Real-Time Clock) for time keeping. ***NOTE****: Due to hardware inaccuracies and drifting the RTC time may not be 100% reliable and will MAY require time updates from the server for accurate time keeping. This option should be selected if you need accurate timing from the server.*

Inside Open Log: (Check Box). If you wish to log all events from EXIT Buttons (Inside open) then select this option. When an exit button is connected to the IN1~IN4 of the MCP040 and a user exits with the button a log event will be generated and sent to the UNIS Server. Normally exit buttons produce a lot of traffic and events.

Terminal ID: This is the MCP040 terminal ID in the UNIS server program. In UNIS if you do not add a terminal with the ID that you programmed then the MCP040 will not connect to UNIS. Always make sure the same ID you set here is added in UNIS. When you change this terminal ID and select 'Send' the MCP040 will disconnect from UNIS and reconnect.

Authentication Mode:

This defines the authentication method between the MCP040 and UNIS server, and the default is '1' (SN). Each authentication method is described below:

- NS mode: When there is an active connection to the server, authentication is done through the UNIS server. If there is no active connection to the server, the authentication is done in the MCP040

- SN mode: Even if there is an active connection to the UNIS server, authentication is done at the MCP040 and the result is forwarded to the server in real time.
  However, in the case of 1:1 authentication, if the entered user ID is not registered in the server, authentication is done through the server.

- NO mode: Network only Mode. Authentication is always done at the UNIS server.
- SO mode: MCP040 only Mode. Authentication is always done at the MCP040.

NOTE: *When using arm/disarming function, i.e. reader is set as ACCESS+SECURITY, the authentication will always occur locally (at MCP040), there is no server authentication for arming or disarming.*
For fingerprint terminals (AC2100, AC5000) when a fingerprint is used for authentication, it will only send the user ID to the MCP040, if the fingerprint is not registered in the fingerprint terminal, no User ID is sent to the MCP040. If the fingerprint is registered in the terminal, the user ID will be sent to the MCP040 and only authenticated at the MCP040. In this case it is important to send all fingerprint users to the terminals (AC2100, AC5000) and the MCP040 so the user ID is same in all devices.

4.5.9. Anti-pass back

The MCP040 can be setup for local or global anti-passback verification.

Local: When only (1) MCP040 is used. Passback exceptions will be verified at the MCP040 controller only. If Virdi terminals are connected to the MCP040 (485), all passback exceptions and verifications will be done at the MCP040.

Server/Global: When UNIS is used to monitor multiple MCP040s or Virdi Terminals. Pass back exceptions will be verified at UNIS server only.

Each reader must be setup for passback (see UNIS Reader Configuration).

Enter Zone, Exit Zone:
These values are set in UNIS under 'Data Management' – Anti-passback. For a detail description on how to setup areas see UNIS Help 'antipassback' for a full description.

Type:

Disabled - Select this if passback is not used for this reader.

Hard – Hard passback, if a user is in passback violation the reader will not allow access.

Soft – Soft passback, if a user is in passback violation the reader will allow access; however UNIS will log the authentication as Passback Warning.

Timed – Timed passback, if a user is in passback violation the reader will not allow access until the 'Lockout duration' period. The lockout duration is started after the last successful transaction period. (NOTE: This mode is not available in server passback)

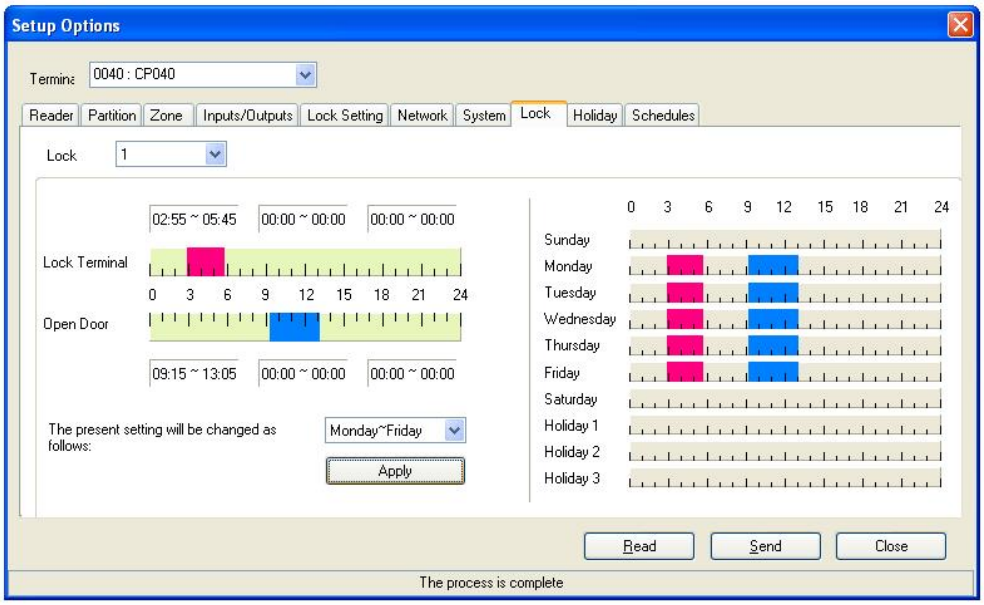
Lockout Duration:

This is the time period 00:00:00 ~ 23:59:59 in which the user will be locked out if in passback violation. The MCP040 will start the timer when the last successful transaction for that user occurred. The user cannot access the reader again until the time period has expired. This is a soft passback condition, allowing the user access after a period of time. UNIS will log the event as Passback Warning.

Note: *If using local anti-passback the user's location will be unknown in UNIS, and the location cannot be set. The user's passback status can be reset when the user is edited from UNIS and downloaded to the MCP040.*

4.5.10. UNIS Auto Lock/Unlock Configuration

A lock can be programmed to OPEN or LOCK on specific days, hours or holidays. This may be used in cases where the building may be closed on weekends and no access is allowed, or if strict access control is not important then a schedule can be setup to open the door during normal business hours.



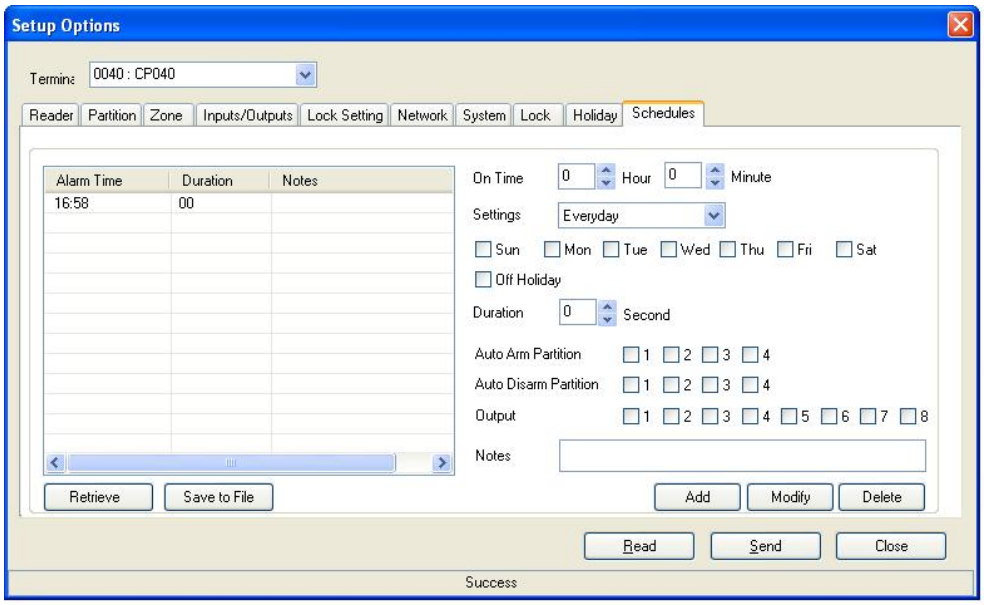
Lock: Select the lock you wish to setup (1~4)

Lock Terminal: Select the time period in which the selected lock will always be locked. Even normal access with a card will not unlock the lock. Select the period with the selection box (weekends, weekdays, holidays, etc) then select apply. A RED marking will appear during the times/days you selected. Select 'Send' to send these settings to the MCP040.

Open Door: Select the time period in which the selected lock will always be unlocked (opened). The door will not be locked again (normal state) until the time period has expired. Select the period with the selection box (weekends, weekdays, holidays, etc) then select apply. A BLUE marking will appear during the times/days you selected. Select 'Send' to send these settings to the MCP040.

4.5.11. UNIS Schedule Configuration

Schedules can be setup to activate an output on the MCP040 at specific times. PGM1-PGM4.



On Time: This is the time in which the schedule will activate.
Settings: Select the interval in which the schedule should activate (daily, weekly, etc)
Duration: This is the activation period for the output if the output is used.
Auto-arm Partition: Select the partitions that will auto-arm for this schedule
Auto-disarm Partition: Select the partitions that will auto-disarm for this schedule
Output: Select the outputs that will activate when this schedule is active.

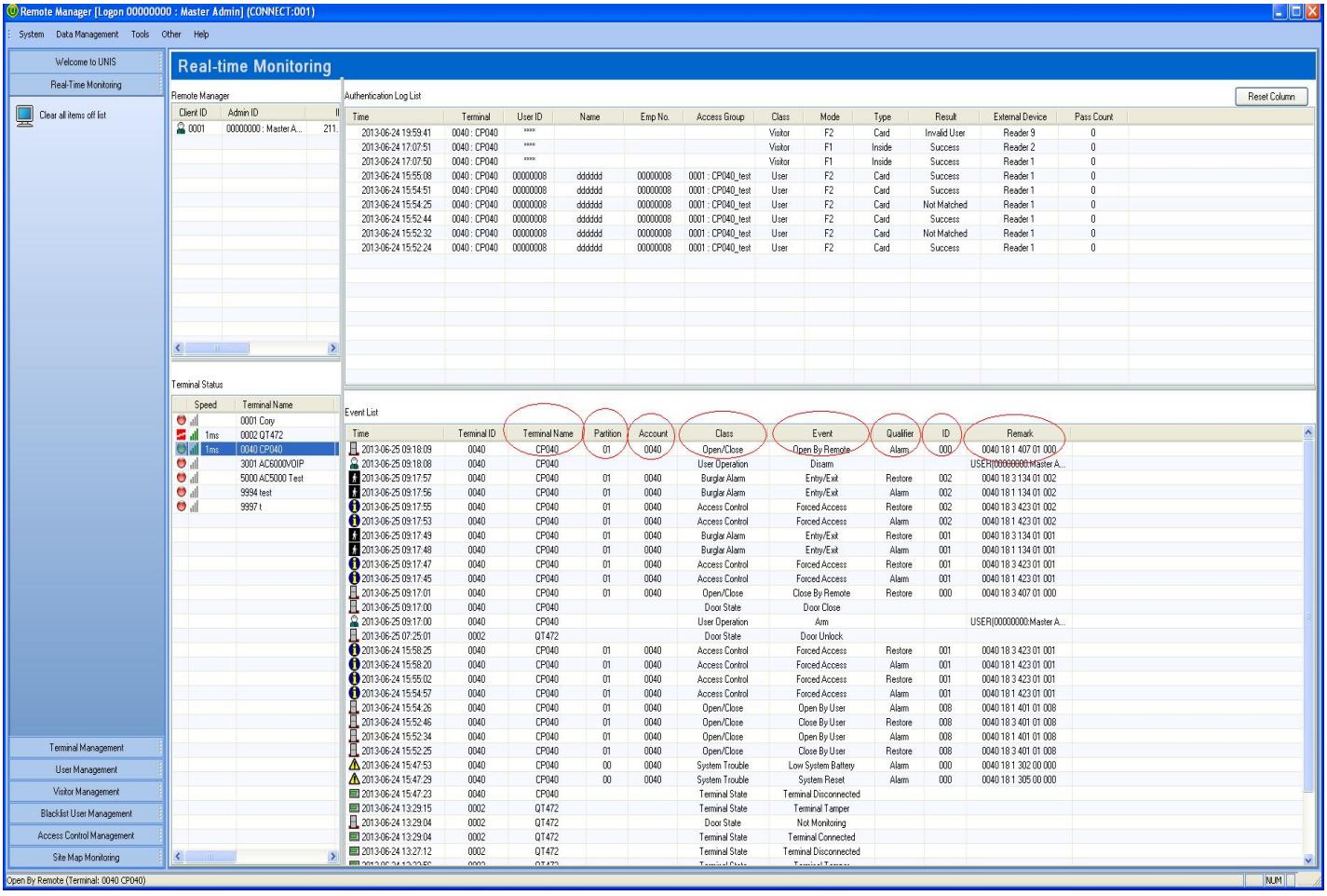
When the partition is Auto-arming, a 60 second warning will occur before the arming. The readers assigned to the partition will emit a warning tone. After the 60 seconds expires the partition will arm without any exit delay.

4.5.12. UNIS Real Time Event Reporting

The MCP040 will report all 'Access Events' and 'Alarm Events' real-time (as they occur) to UNIS.

- All Access Events will be in the 'Authentication Log List'
- All Alarm Events will be in the 'Event List'

The event list reports all UNIS events and MCP040 events. If there is a UNIS related event only (not reported by MCP040, then the 'Partition' and 'Account' column will be blank.
If the event is reported by the MCP040 the 'Partition' will be the Partition Number 1-4, and the 'Account' will be the account number which was programmed in the partition setup area. This reporting format is an industry standard contact ID format.



Partition: Partition #01~04

Account: Account number programmed in 'Partition Configuration'

Class: Event Category (Open/Close, Access Control, System Trouble, Alarm)

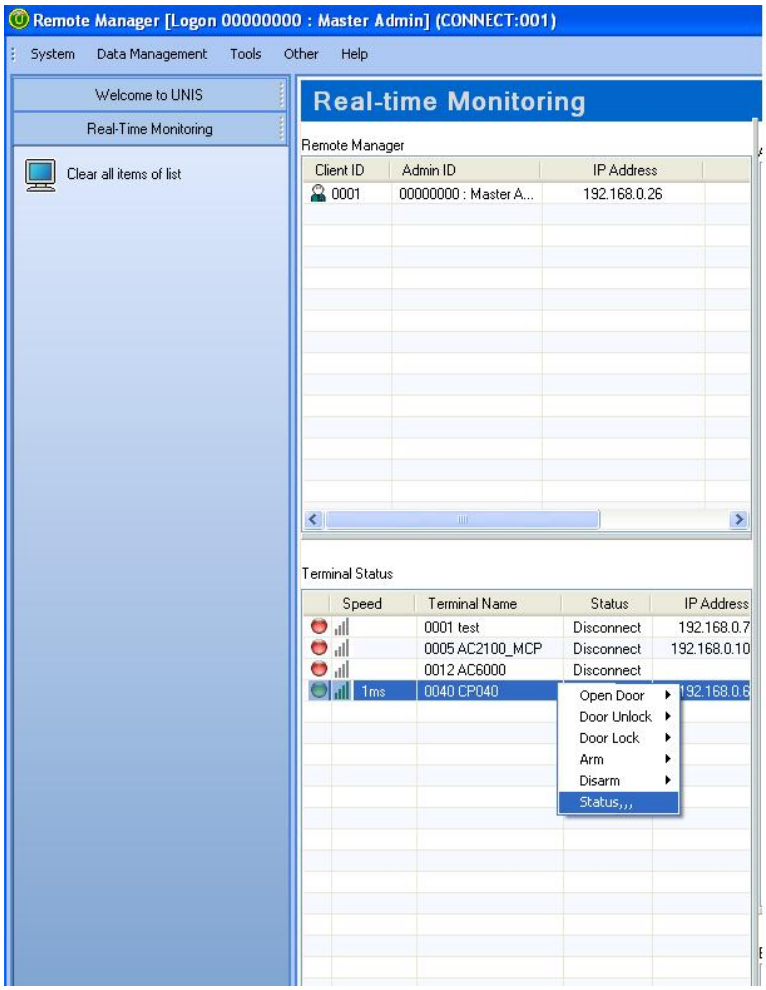
Event: Category Event Type

Qualifier: Alarm or Restoral

ID: Identify user, zone or area. 000-999 (System events, always 0). If user number is more than 999 the maximum will only be 999.

4.5.13. UNIS MCP040 Status/Functions

The current zone, reader, lock, partition state can be monitored from UNIS. These status updates are real-time.
In UNIS, select the 'Real-Time Monitoring' tab on the left, then right click on the controller.



Partition:

- Arm/Disarm Status – Partitions 1-4

Zone:

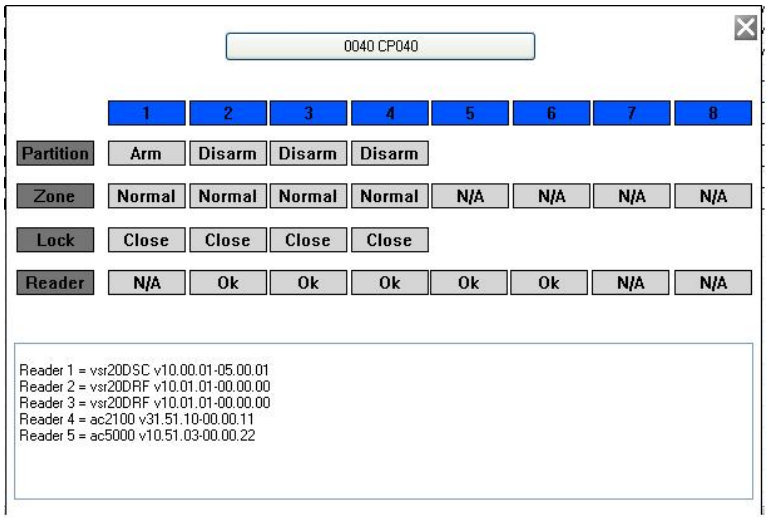
- Zone Status – Zones 1-8
- Normal (closed OK), Trouble (fault, shorted wire), Open (zone is opened), N/A (zone type set as unused)

Lock:

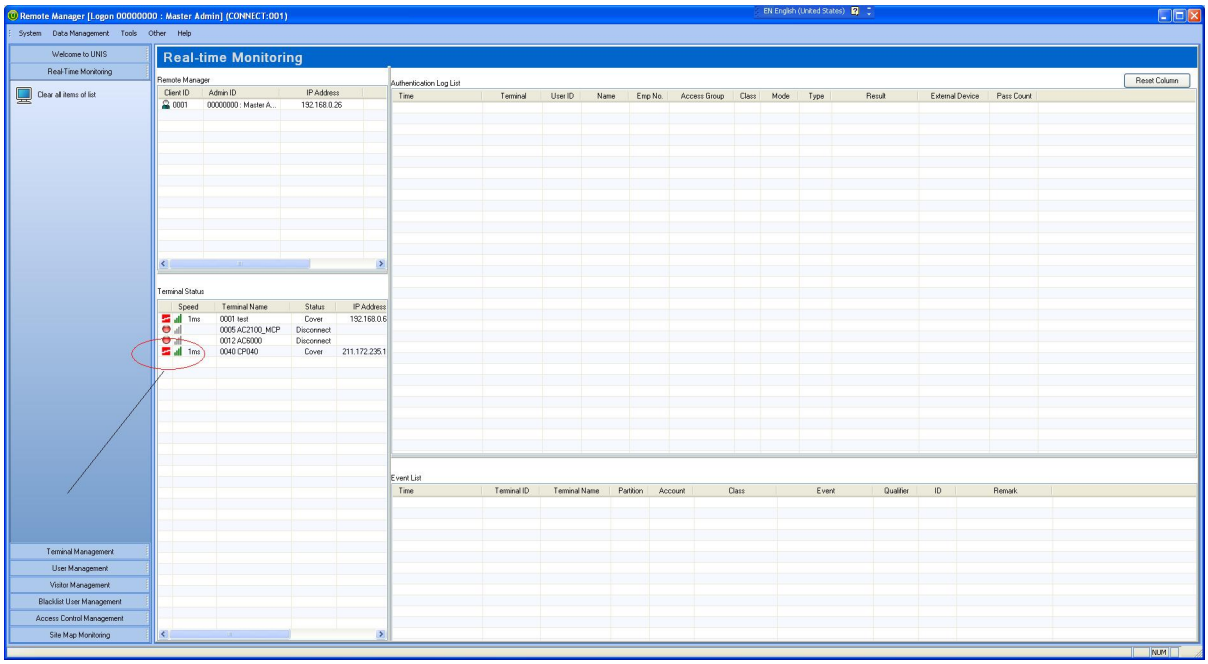
- Lock Open/Closed Status – Locks 1-4

Reader:

- Reader Status – Reader ID (0-7)
- N/A (not enrolled, OK), Fault (enrolled successfully however MCP040 cannot communicate), OK (normal state)



4.5.14. UNIS MCP040 Trouble Status



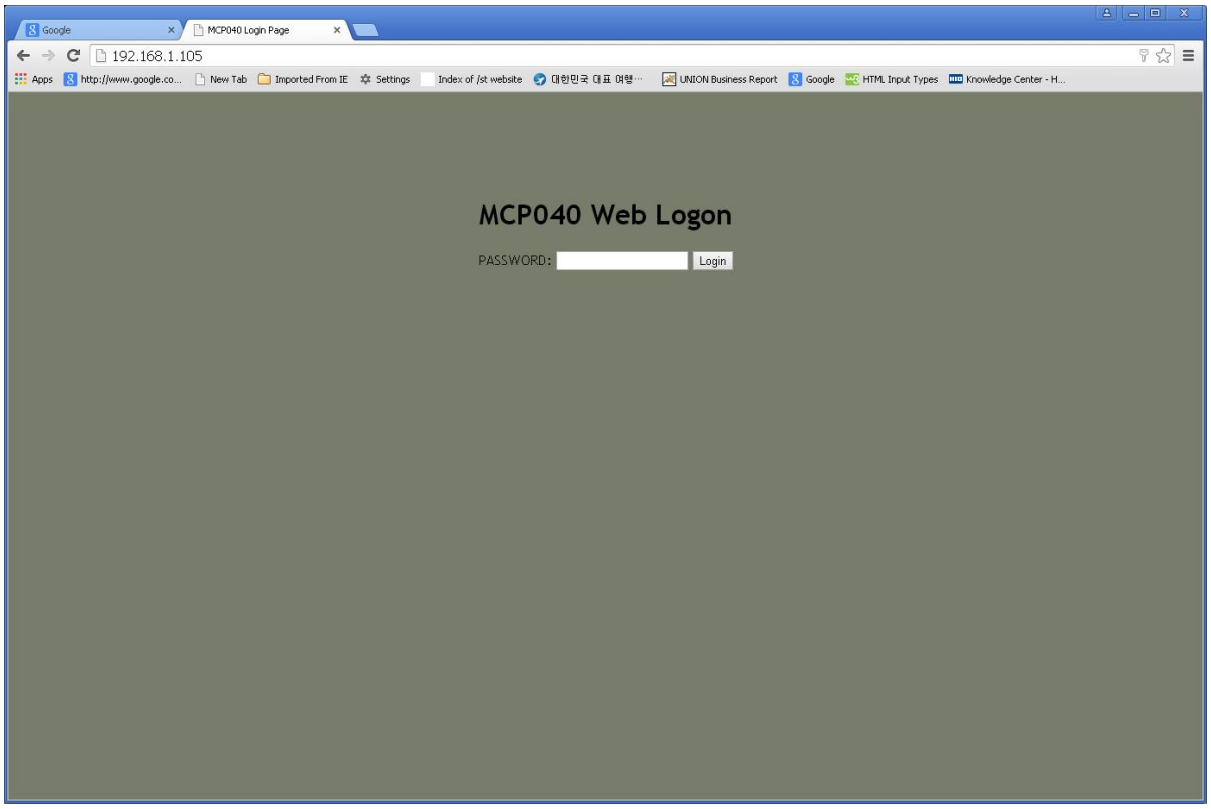
When the Status icon on the Terminal Status display shows a RED with WHITE broken line, this indicates a trouble on the MCP040. Check the Event List for detail trouble condition(s).
Troubles are:

AC Loss, Low Battery, Reader Tamper, Reader Fault, Bell Trouble or Fire trouble.

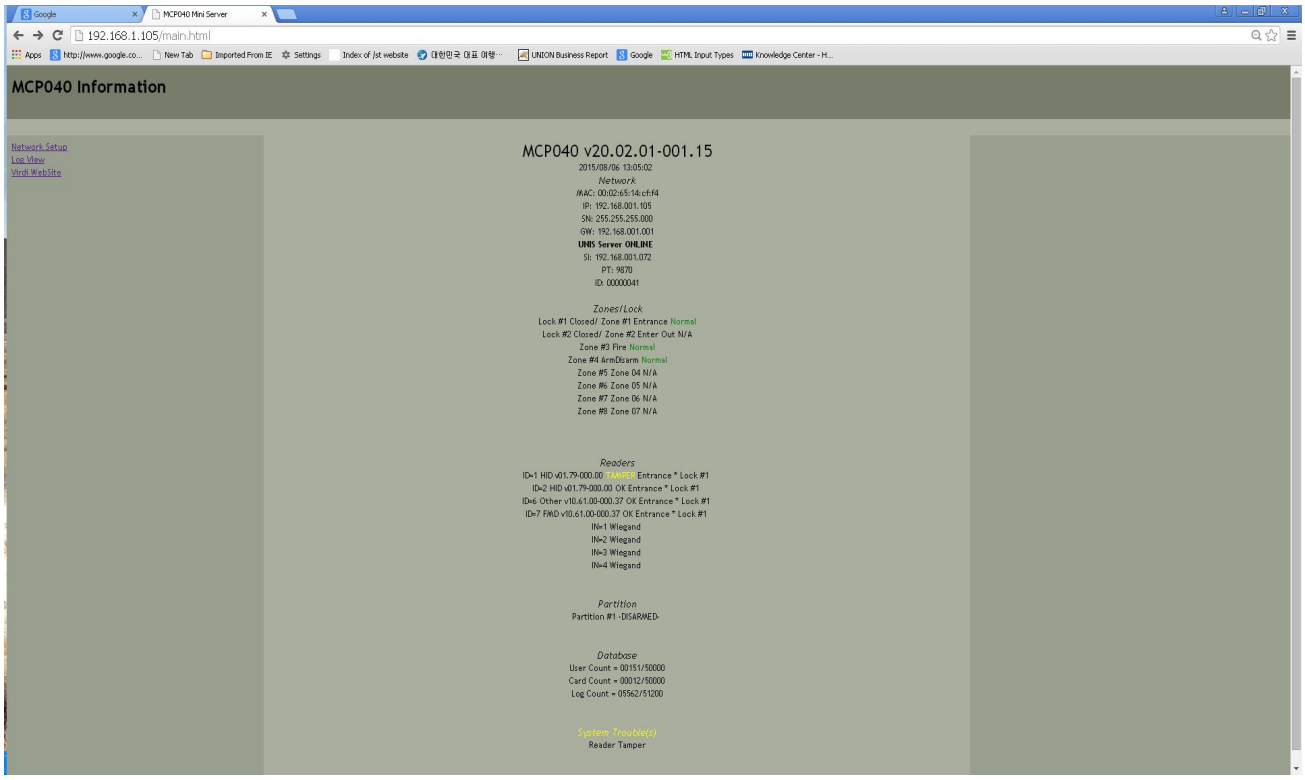
4.5.15. Web Browser Status

MCP040 has a mini web server with basic network setup, log and status viewing. This is best viewed in browsers that support HTML5. This has been tested on Internet Explorer 8.0 and Google Chrome.

A logon password is required. Use the same password as UDP and Network Settings



The status page is refreshed every 10 seconds.



Network
- IP configuration
- Server Status

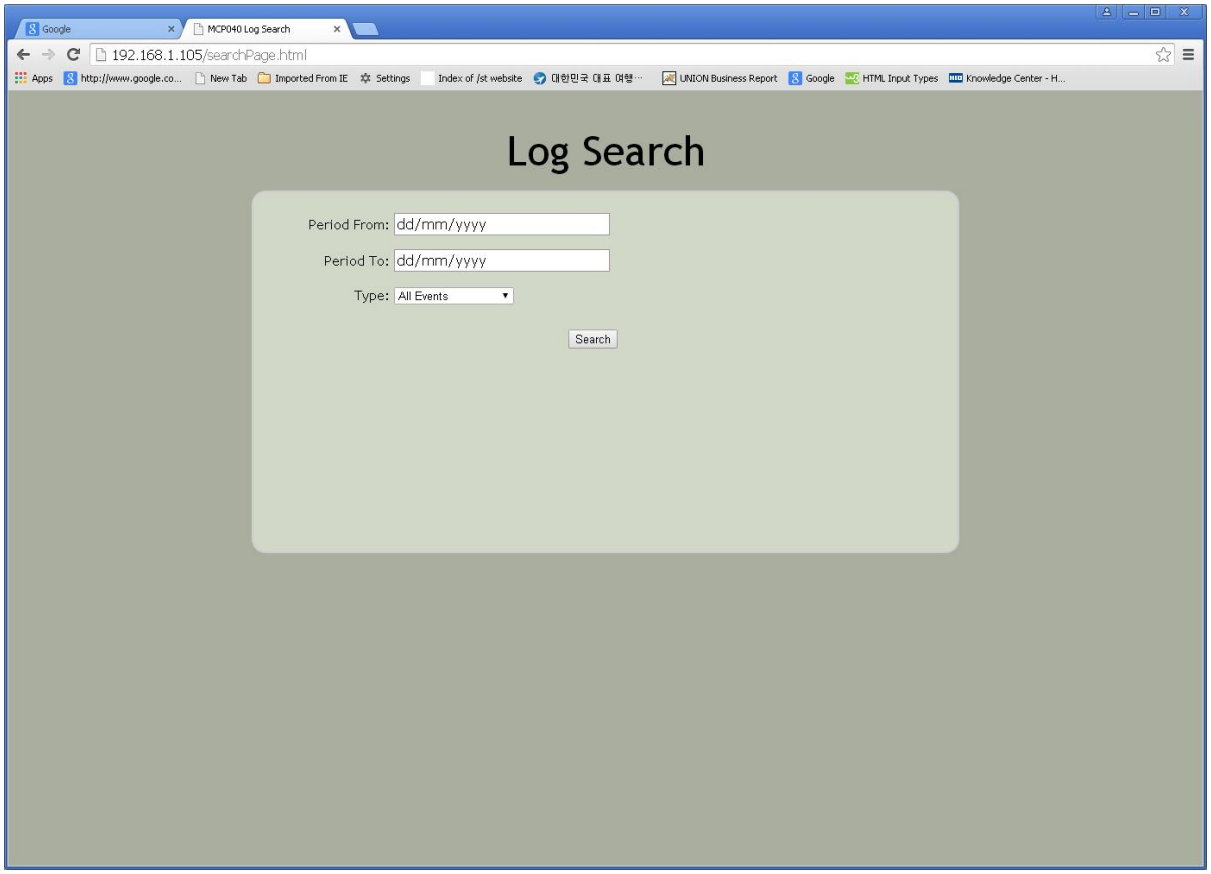
Zone and Lock Status
- Zone Assigned to Lock#, Zone#1-8, Zone Label, Status (Open,Normal,Fault)
- If N/A then zone is not assigned to the lock

Readers
- Readers connected to the MCP040
- ID# (485), type, Version, Status (TAMPER,FAULT),

Partition
- Partition Label, Status (Disarm/Armed), Alarm status

Database
- Number of Users
- Number of Cards
- Number of Logs

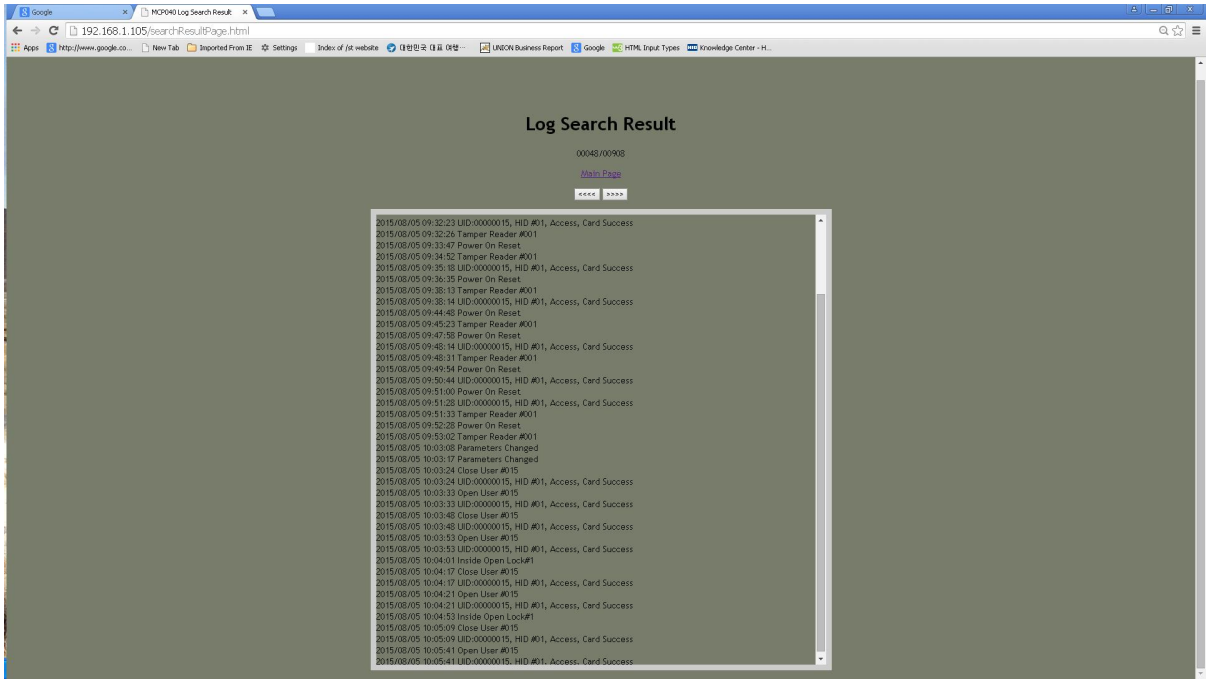
After selecting ‘Log View’ link you may choice a date period for searching, if using Chrome, you can select the date with the calendar by clicking the right side of the date field. Other browsers (IE, Safari, Fire Fox) require you to enter the date manually YYYY-MM-DD



Type:

All Events (Access + System Events)
Access (Access events only)
Successful Access (Only success access events)
Failed Access (Only failed access events)
System (System events only include partition, troubles, alarms)
Alarm Events (System events only alarms – burglar, alarm, etc)
Trouble Events (System events only troubles)

Search results will display a maximum of 48 events per page, click the right '>>>>' button to view more or left '<<<<' to go back.



5. Operational Information

5.1. Factory Initialization

In cases where you need to reset all parameters to factory default values you can use a hardware default method. This may be needed if you lost your network settings and you do not know your MCP040 IP or Terminal ID. You can always refer to section 3.1.1.4 'UDP Setup' for finding terminal information. See Installation Guide for details how to factory initialize.

5.2. Warning/Alarm Notifications

Reader LED or beeper will be activated under certain conditions. See the table below for details.
Also, the bell output will be activated normally under an alarm condition. See the table below for details.

Reader Notifications	
Type	Reason/Comment
Double beep sound every 30 seconds	485 communication trouble. The reader cannot receive any information from the MCP040
Double beep every 2 seconds	Reader tamper is unsecured on back of case.
Continuous beep every 1 second	Door left open warning. Door left open after access granted.
Beep every 2 seconds. Red LED Flashing	Reader partition exit delay in progress, after arming this will occur until exit delay expires.
Red LED flashing every 1 second	Reader partition is in armed state.
3/2 Beeps from reader when door is open	Partition chime function enabled.
Red, Blue, White LED flashing continuously	MCP040 auto-enroll period (one minute during power up)
Continuously 3 Beeps	Alarm, Force Alarm
Bell Output Notifications	
Bell output on steady (always on)	Door is forced opened with no authorization. Bell will turn off when door is closed and no other alarms or at the end of the Siren Time.
Bell output on steady (always on)	Alarm condition. If a zone is opened during an armed state or a 24-hour zone is opened. Bell will turn off if partition is disarmed or the Siren Time expires
Bell output pulsing 1 second on, 1 second off	Fire Alarm condition. If a fire zone or INPUT event for fire is generated. Bell will turn off if partition is disarmed or the Siren Time expires

5.3. Technical Support

If there are any problems with setup, configuration or operation please contact

'support@virditech.com'

It is important you include the following information before contacting technical support.

- Current MCP040 firmware version – See UNIS Terminal status
- Current UNIS Software version – UNIS-> Help - > About
- Your system configuration settings
    - Include a system layout diagram (readers, locks, I/O etc)
    - Include wire type/distance etc
    - System configuration (setup by UNIS) – lock, reader, input/output settings, etc.