

Meridian 64

TCP/UDP IP Internet Connect Alarm Control



XML Installation and Operations Manual

Version 7.0.0

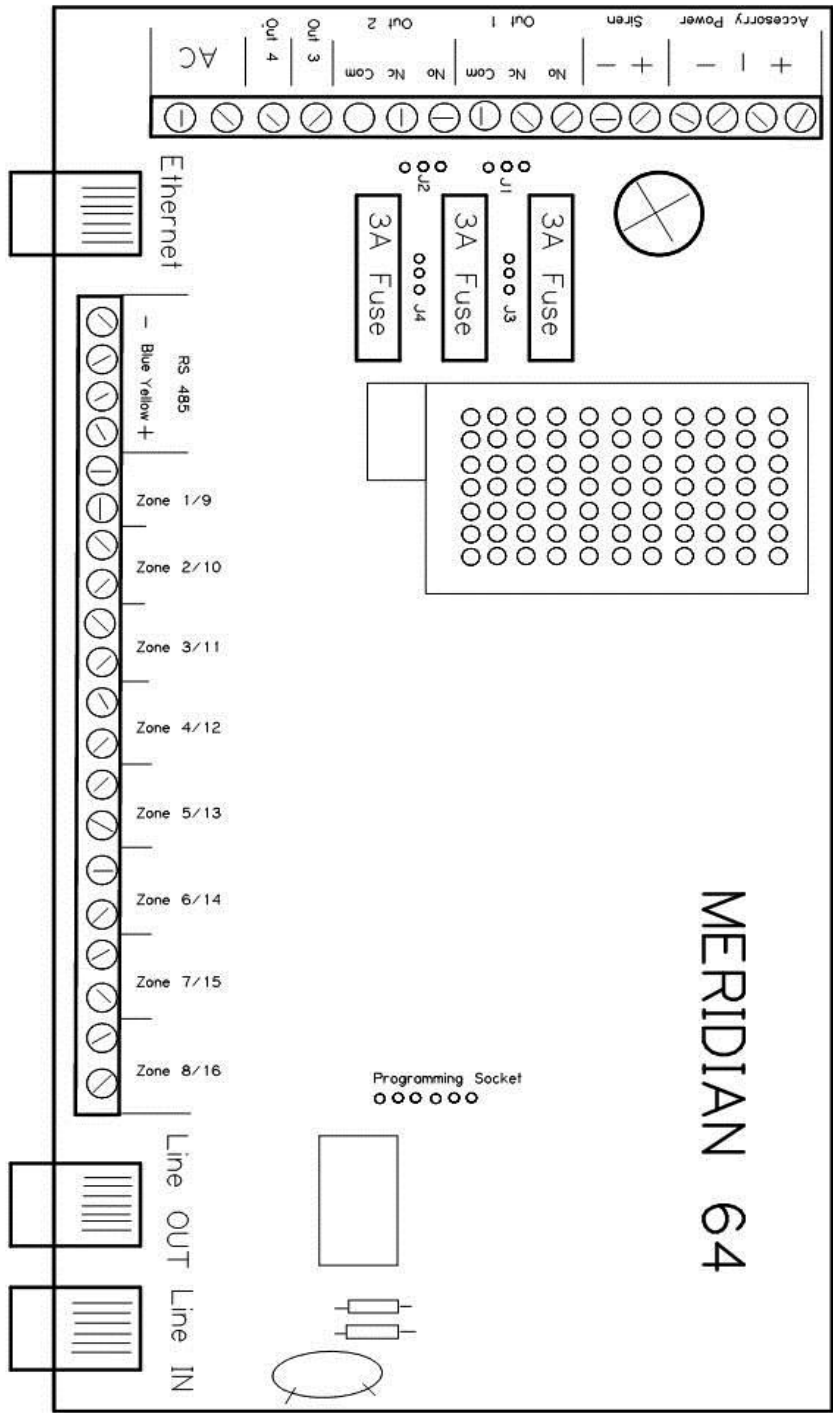
Micron Security Products Ltd

October 2011

Table of Contents

Circuit Board Layout and Wiring Diagram	3
Meridian 64 TCP/UDP IP Alarm Panel	4
Zone and output options	
Meridian Initial Setup	4
Meridian Connection	5
 PROGRAMMING TABS	
 Command Tab	 6
 Partition Tab	 7
Setting up partitions	
How to create a common partition	
Assigning Areas	
Common Zones	
 Zones Tab	 9
Entry and exit delays	
Common zones in the same partition	10
Zone types	
Zone options	
Follow Tab	11
Crossed Tab	12
Codes Tab	13
Auto-Arm Tab	14
Outputs Tab	15
CID Events Tab	17
Path Tab	19
Network Tab	20
 MISCELLANEOUS	
 Meridian Factory Default	 22
Meridian Receiver Self Test Software	23
Download Meridian Firmware Upgrade	23
TXT Files Explained	23
Smart Phone Screen	24
Keypad Command Map	25
Battery Saving Explained	26
Meridian Relay Output Configuration Options	27
Zone Connection Schematic	28
DNS Connection Schematic	29

Circuit Board Layout



Meridian 64 TCP/UDP IP Alarm Panel

The Meridian 64 is a TCP/IP or UDP, internet connected alarm control with an optional backup Telco dialler and eight zones (sixteen zones with double EOL resistors). Each zone may be independently configured as one of five options:

NO/NC (Normal/Alarm) (No resistor needed) (reports 'alarms and restores' only)

1x Resistor (Alarm /Normal/Alarm) (value: 3K3) (short circuit or open contact both generate alarms)

1x Resistor (Short Circuit Protection/Normal/Alarm) (value: 3K3) (short circuit is a tamper, open contact on alarm)

Double Zone (3K3 for zones 1-8 and 6K8 for zones 9-16) (reports 'alarms and restores' only) (Up to 16 zones)

2x Resistors (Tamper/Normal/Alarm/Short Circuit Protection) (3K3 and 6K8) (reports 'alarms' + 'tamper' + 'restores') (open circuit and short circuit generate a tamper condition; open contact generates an alarm)

Zone status can be diagnosed via the XML IP software interface. Zone status is displayed using different colours. For more detailed information see the Command Tab on page 6.

The Meridian 64 has five outputs, three with relays, with one dedicated to an external siren, and two further outputs configured as open collector. Each of the relay outputs may be configured by 'jumper' selection as:

1. NO/COM/NC clean relay contacts
2. Supply +12 Volts when switched
3. Supply Gnd (-ve) when switched

The Meridian alarm transmits **Contact ID CSV format** over the internet. The Meridian 64's **factory IP address** is **192.168.1.28**

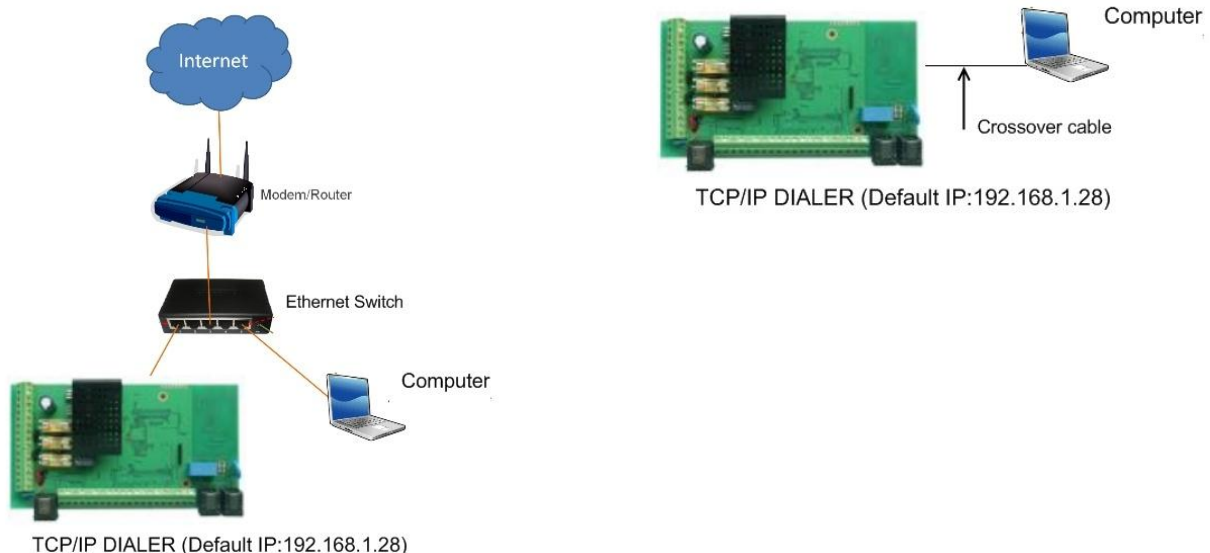
Meridian Initial Setup

Connect the Meridian 64 TCP/IP alarm to your ONT, hub/switch or ADSL router or with a crossover cable directly to a computer.

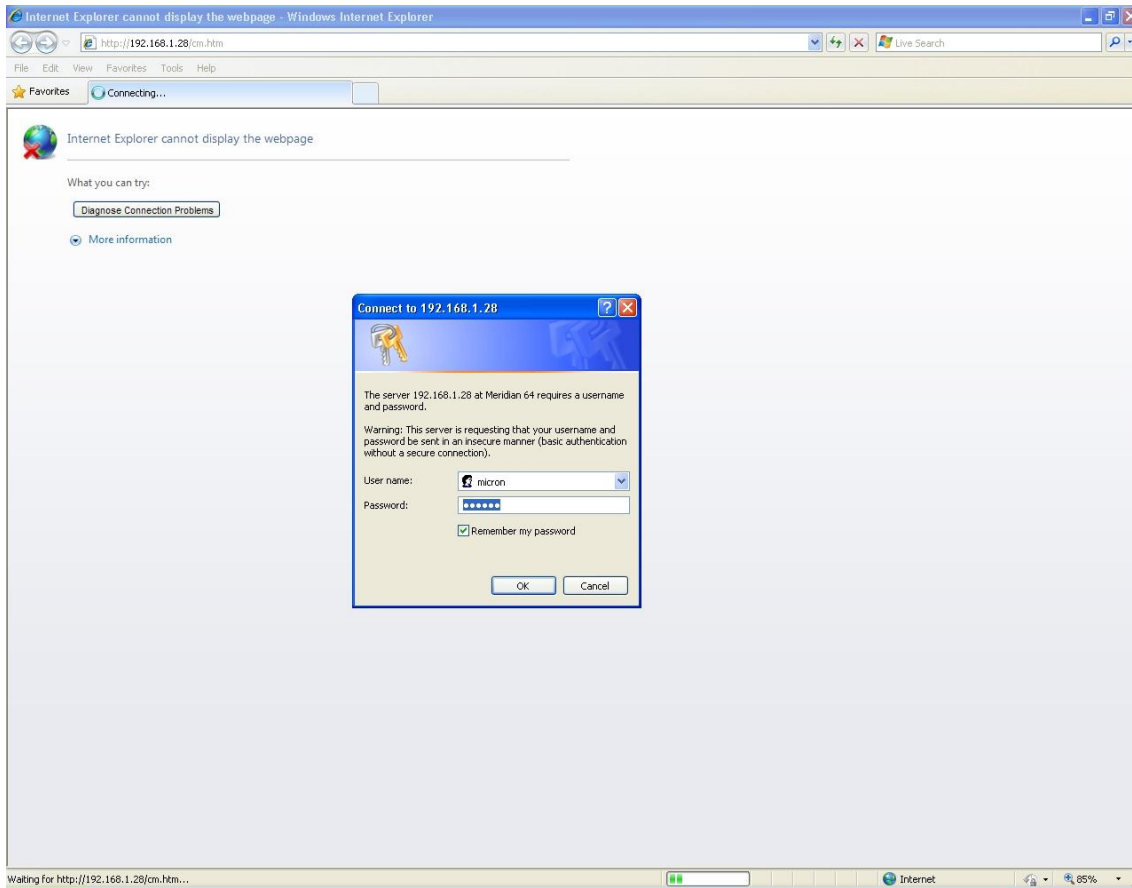
The network or computer connecting to the Meridian 64 must be in the IP address range of 192.168.1.XXX

To enable external remote access to the alarm the customer's router must be "port forwarded". The forwarded port of the router must match the web server port of the Meridian to allow external remote access to the alarm. Refer to the customer's IT specialist if necessary.

OR



Meridian Connection

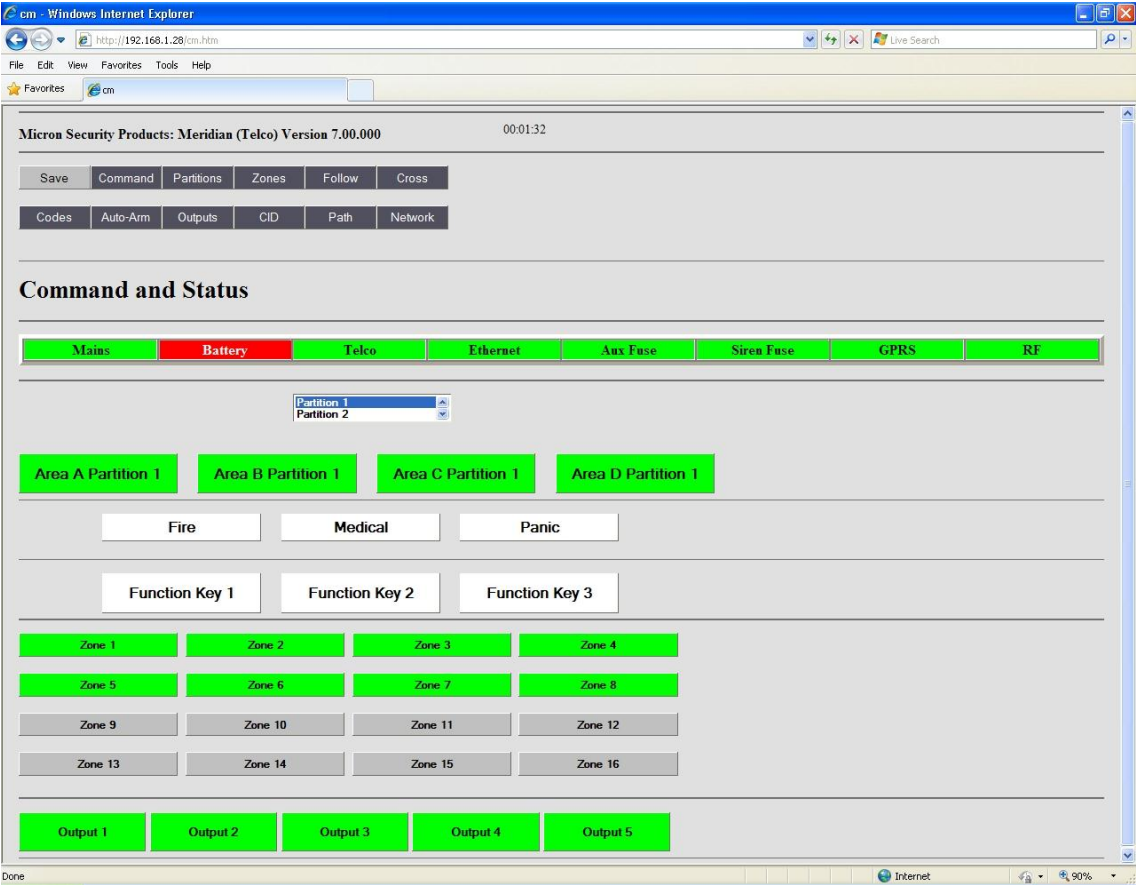


Enter the Meridian's **IP address/cm.htm** (eg: <http://192.168.1.28/cm.htm>) or a valid **DNS address** in any compatible browser (**Internet Explorer, Google Chrome, Firefox or Safari**) on any computer or smart phone with internet connection capability. Enter a **Username** and **Password** in the security login screen of the Meridian alarm, if this is different than the factory default (username: **micron**, password: **micron**).

You may need to refer to your IT specialist or the IP monitoring station to obtain the correct TCP/IP parameters to complete these fields.

Click on **OK** and the Ethernet connection will be established with the Meridian.

Command Tab



This is the first tab to appear when a connection is established. The Command screen displays the Meridian 64’s zones, outputs, system status, version number, time and virtual control buttons for arming and disarming, function key control, output control and zone bypassing. The name of all displayed keys can be changed to match their actual description for your alarm installation. For example “**Zone 1**” could be named “**Kitchen**”, “**Function Key 1**” named “**Garage Door**” and “**Output 1**” named “**Lights**”

System Status

When the **Mains**, **Battery**, **Telco (Phone)**, **Ethernet**, **Auxiliary Fuse**, **Siren Fuse**, **GPRS** or **RF Signal** indicators are green their status is **OK**. When the indicator is red a **FAULT** condition exists. Unavailable functions are grey.

Zone Status

The zone’s colour indicates zone status.

- | | |
|-------------------|--|
| Green indicator: | Contact is normal. |
| Red indicator: | Contact is alarm. |
| Purple Indicator: | Tamper open or shorted |
| Grey Indicator | Zone disabled |
| Black Indicator | Zone bypassed (click on any zone to bypass that zone and arm the system) |

Arm Buttons

A **Partition**, then an **Area** must be selected to activate an arm or disarm cycle. Both end users and installers can arm or disarm the alarm, bypass zones and control outputs from a local or remotely connected personal computer or internet enabled smart phone. Reference the keypad command map on page 25 for further keypad commands.

Panic and Function key buttons

Click one of the **Fire**, **Medical** or **Panic** buttons to initiate an alarm for these services. Or click one of the function keys to trigger a pre-programmed event such as opening a garage door.

Zone Buttons

Click any zone button to manually bypass a zone. This allows the alarm to be armed without the bypassed zone being included.

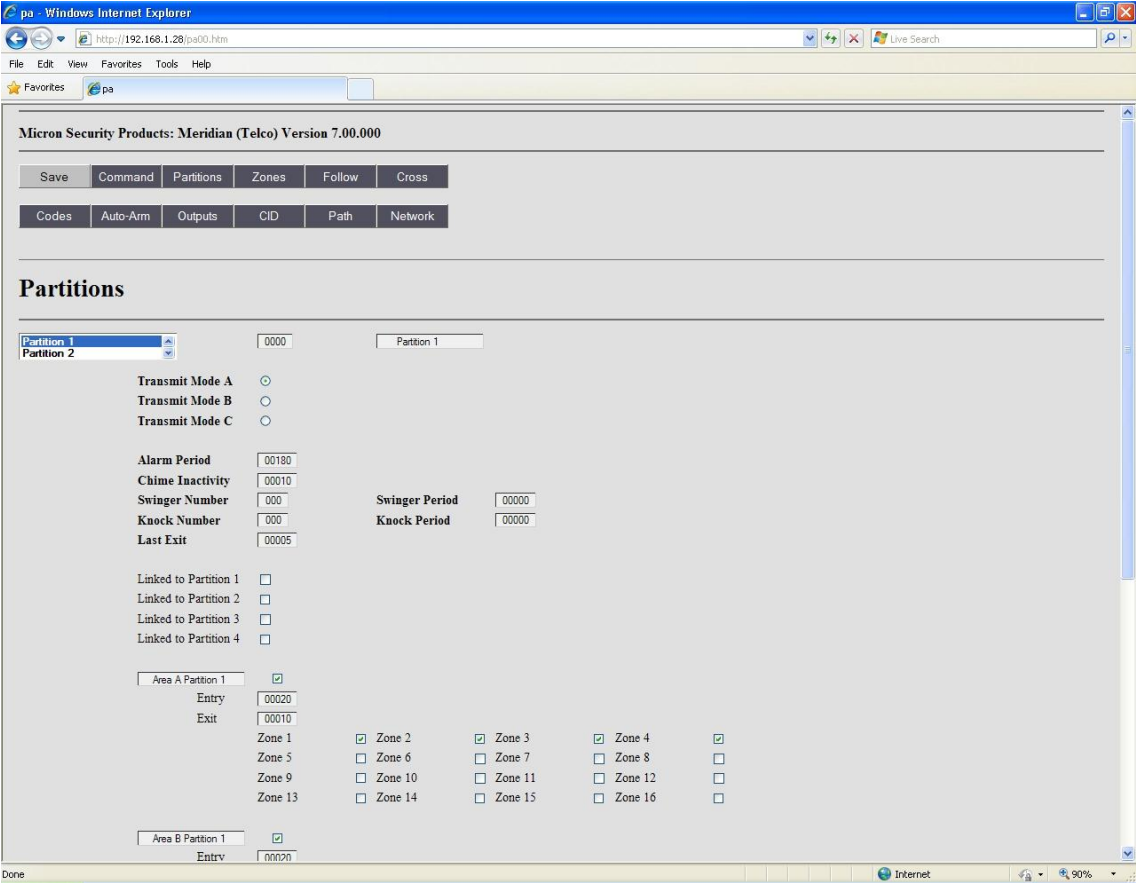
Output Buttons

Click an output button to control an Output.

Output 5 is indicated as a Siren Output on the circuit board. Any Output label may be personalised in the Output Tab.

Partitions Tab

Click on the **Partitions Tab** to setup partitions, areas, zones, set zone delays and account numbers.



Partition and Area labels may be personalised here.

Account Number	Enter the 4 digit customer account number for the chosen partition. (Partition 1 to Partition 4) This is the Contact ID customer number normally supplied by the central station.
	Any alphanumeric characters can be sent when transmitting in TCP/IP or UDP but only B, C, D, E, F alpha characters are permitted when transmitting over PSTN.
Transmission	Select the Transmission Mode: Mode A ALL EVENTS are reported to the Monitoring Station (eg. door contact; Open/Close/Open/Close/Open/ Close; monitoring station will receive 6 messages) Mode B ALL ZONES are reported only ONCE to the monitoring station, irrespective of the number of alarm activations, for the defined Alarm Period. Mode C FIRST ALARM ACTIVATION only will be reported to the monitoring station, irrespective of the number of zones triggered in the Alarm Period.
Alarm Period	Delay before a new activation is reported (this is only available in transmission Modes B and C)
Chime Inactivity	When a chime zone is activated, the programmed output will activate. Chime mode sleeps during the programmed chime inactivity period.
Swinger Number	Enter the number of alarm activations for any zone within a partition before a zone is shut down. Zero (0) value will disable the Swinger shutdown .
Swinger Period	Enter the swinger shutdown time in seconds. When the programmed number of alarm activations has occurred within the Swinger Period , the zone is disabled and can not generate further alarms until the panel is disarmed and re-armed.
Knock Number	Enter the number of zone activations for the same or different zones within a partition before an alarm is generated. Zero (0) value will disable the Knock counting .
Knock Period	Enter the knock count period in seconds

Last Exit Period Any zone may be assigned as a last exit zone. Triggering the last exit zone will cancel the exit period and activate the last exit period.

For example; Zone 8 is the last exit door contact for the premises. If the **exit period** is set for 180 seconds and the **last exit period** for 10 seconds, once the Meridian is armed the 180 second exit period will begin to count down. When the exit door contact is opened and closed the exit period is cleared and the 10 second last exit period begins.

How to create a Common Partition (Link to Partition)

Linked to Partition 1

☐

Linked to Partition 2

☐

Linked to Partition 3

☐

Linked to Partition 4

☐

For example; Building A (Partition 1) and Building B (Partition 2) share a corridor (Partition3)

Select Partition 1, tick ‘Linked to Partition 3’
Select Partition 2, tick ‘Linked to Partition 3’

Partition 3 is defined as a common partition. Partition 3 will be automatically armed **only** if Partition 1 **and** Partition 2 are **armed** (even partially). Partition 3 will be automatically disarmed if either Partition 1 or 2 is **disarmed**.

Assigning Areas:

Tick the area for the appropriate partition and then assign the zones to that area.

Area A Partition 1

☒

Entry

00020

Exit

00010

Zone 1

☒

Zone 2

☒

Zone 3

☒

Zone 4

☒

Zone 5

☐

Zone 6

☐

Zone 7

☐

Zone 8

☐

Zone 9

☐

Zone 10

☐

Zone 11

☐

Zone 12

☐

Zone 13

☐

Zone 14

☐

Zone 15

☐

Zone 16

☐

Entry Period An entry zone is defined as a zone which allows a programmable time delay to elapse before generating an alarm status. This “entry period” is independently programmable for each area. Enter the entry time period in seconds.

Exit Period Enter the exit period time in seconds.

Common zones in two different Areas of the same Partition

For example; Zone 5 is in Partition 1, Area A and in Partition 1, Area B.

Zone 5 will only be activated if Area A **and** Area B are armed.

If either of these two areas is disarmed, Zone 5 is not activated

Now click on the **Save** button to save this data.

Zones Tab

Click on the **Zones Tab** to set Meridian 64 zone attributes.

Micron Security Products: Meridian (Telco) Version 7.00.000

Save Command Partitions **Zones** Follow Cross

Codes Auto-Arm Outputs CID Path Network

Zones

Zone 1 Zone 2 Zone 3 Zone 4

Zone 1 Selected ☒

Debounce 00010

NO/NC ☐ Alarm 1 ☒
Single Type 1 ☒ Alarm 2 ☒
Single Type 2 ☐ Tamper 1 ☒
Balanced ☐ Tamper 2 ☒
Double ☐ 24 Hour 1 ☒
24 Hour 2 ☒

Status Only ☐
24 Hour ☐ Service Mode ☐ Delay 00900
Entry Zone ☒ Entry Follow ☐ Follow Group 0
Exit Zone ☒ Last Exit ☐
Key Switch ☐ Momentary ☐
Sensor ☐

Tamper 24 Hour ☐
Bypassable ☒
Inverted ☐
Forced Arming ☐
Chime ☐

Knock Count ☐
Swinger ☒
Crossed ☐ Cross Group 0

Select a zone from the list to setup

Tick the **Selected** button to enable the zone

Un-tick the **Selected** button to disable the zone

Debounce

Select each zone's sensitivity in multiples of 10 milliseconds. Minimum sensitivity is 10 milliseconds. Maximum sensitivity (trigger delay) is 10 minutes.

Example: Enter 100 = 100 x 10 m/s = 1000 m/s = 1 second.

Zone Wiring

To select how the zone is to be physically wired

NO/NC (Normal/Alarm): no resistor needed

Single Type 1: 1x Resistor (Alarm /Normal/Alarm): **value, 3K3**

Single Type 2: 1x Resistor (Short Circuit Protection/Normal/Alarm): **value, 3K3**

Balanced: 2x Resistors (Tamper/Normal/Alarm/Short Circuit Protection): **3K3 and 6K8**
(open circuit and short circuit generate a tamper condition; open contact generates an alarm)

Double Zone: **3K3** for **zones 1-8** and **6K8** for **zones 9-16**, tick **Double Zone** tick box

Zone to Output

Any zone may be assigned to two alarm outputs; any 24 hour zone may be assigned to two 24 hour outputs; and any tamper may be assigned to two tamper outputs.

Alarm1

Alarm2

Tamper 1

Tamper 2

24 Hour 1

24 Hour 2

Zone Type

Any zone which is not ticked with one of the following options will act as an instant zone.

Status Only

Any change in the input status generates automatic Contact ID (CID) events.

The zone status is only reported. The zone has no output control. Please refer to the below table.

Resistor Connection	OPEN CIRCUIT	R1//R2	R1	R2	R1+R2	CLOSE CIRCUIT
Resistor Value	0	2K2	3K3	6K8	10K1	∞
CID Event	133 (New Event)	131 (New Event)	132 (New Event)	134 (New Event)	135 (New Event)	130 (Restore)

24 Hour

Tick to select the zone as a 24 hour zone (eg Tamper)

Service Mode

Tick if you want this zone to be a service zone. The router reset function will be bypassed until the zone is closed. This function is only available when the system is disarmed.

Enter the **Delay** in seconds the router reset will be bypassed in Service Mode.

Entry Zone

Tick if you want this zone as an entry zone

The entry delay is defined in the **Settings Tab** (one delay per Area)

Entry Follow

At least one zone must be defined as an entry zone to enable entry follow mode. Setup the follow group in the **Follow Tab**. (See examples in the **Follow Tab** section)

Exit Zone

Tick if you want this zone as an exit zone (no alarm during exit period)

The exit delay is defined in the **Settings Tab** (one delay per Area)

Last Exit

Tick if you want the last exit to clear a longer exit period.

When the final door is opened and closed the exit delay will be cleared.

The last exit delay is defined in the **Settings Tab** (one delay for the panel)

Key Switch

Tick to use this zone as a key switch zone to arm and disarm the alarm panel.

If selected, the zone will arm the **Area and Partition** to which the zone is assigned.

Momentary

Tick to set the key switch to momentary operation

Sensor

If the alarm is **armed**, triggering this zone will activate an output without an alarm condition.

For example; activating an external light

Zone Options

Tamper 24 Hour

Tick if tamper is to trigger a 24 hour zone activation

Bypassable

Tick if you want this zone to be bypass able, by either a user or by swinger shutdown

Inverted

The '**Inverted**' check box, when selected, will switch the selected zone from **NC = Normal** and **NO = Alarm** to **NC = Alarm** and **NO = Normal**.

Force Arming

Select this option to enable the alarm to arm even if zones are open. If zones are restored they are re-instated as active zones if the system is armed

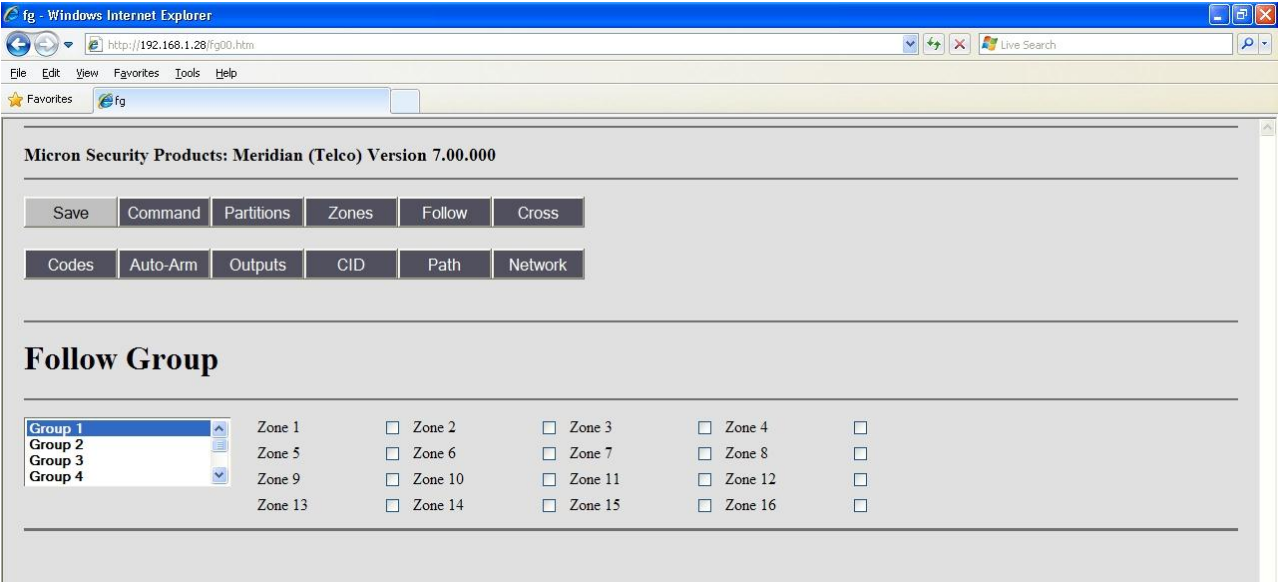
Chime

Select chime mode for this zone. Enter the period the chime is inactive after being triggered in the **Partition Tab** (one period per partition)

Now click on the **Save** button to save this data.

Follow Tab

Click on the **Follow Tab** to setup follow zones.



Example 1 Zone 5 is an entry zone
 Zone 2 should follow Zone 5
 Zone 3 should follow Zone 2

You need to define a **Follow** group (8 possible) (say group 7), then in group 7 select only Zone 5
You need to define another **Follow** group (say group 6), then in group 6 select only Zone 2

Then go to the **Zones Tab** and
For Zone 2 select Follow group 7
For Zone 3 select Follow group 6

There will be no alarm activation if you enter zone 5, then go to zone 2 and then zone 3.
Any other order will trigger an alarm.

Example 2 Zone 5 is an entry zone
 Zone 2 should follow Zone 5
 Zone 3 should follow Zone 5

You need to define a Follow group (8 possible) (say group 7) then in group 7 select Zone 5

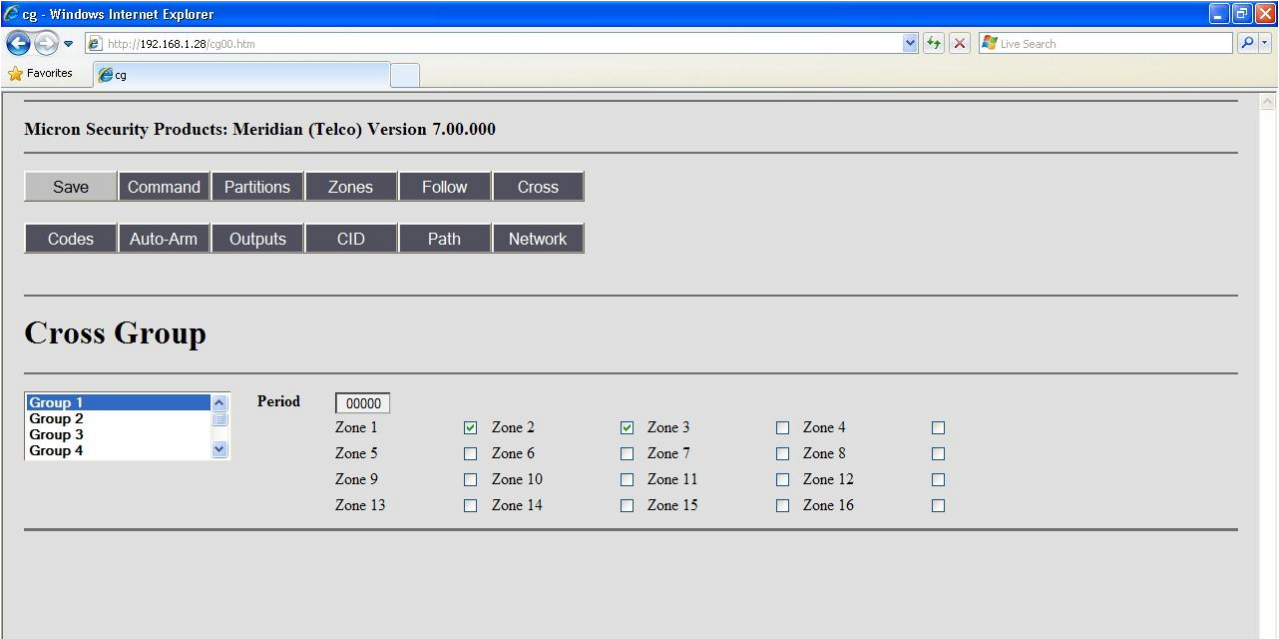
Then go to the **Zones Tab** and
For Zone 2 select Follow group 7
For Zone 3 select Follow group 7

There will be no alarm activation if you enter zone 5 then go to zone 2 and/or then zone 3

Now click on the **Save** button to save this data.

Cross Tab

Click on the **Cross Tab** to setup the cross zones



Cross Group Selected zones must be triggered within a defined period to generate an alarm condition

In this example both zone 1 and zone 2 must be triggered within 30 seconds to generate an alarm condition.

Note: If you are using double zones (low zones 1-8 and high zones 9-16) do not cross high zones with low zones.

Now click on the **Save** button to save this data.

Codes Tab

Click on the **Codes Tab** to setup the user codes.

User Code Setup

- If **Master**, **Codes** and **Save** are selected then this user can see and **change** all user codes and passwords.
- If **Master** and **Codes** are selected then this user can see but **not change** all user codes and passwords.
- If **Codes** and **Save** are selected then this user can only see and **change** their own user code and password.
- If **Codes** is selected then this user can only see but **not change** their user code and password.

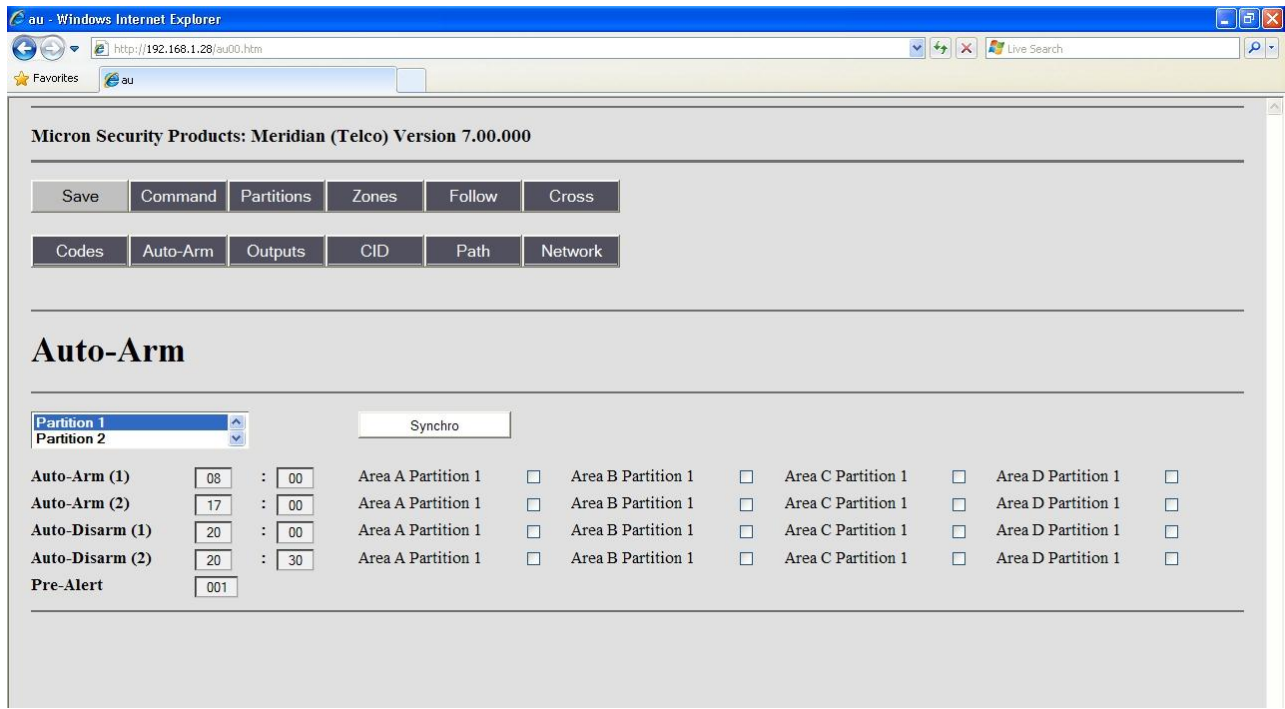
Enter the **User Code** for each user (from 2 to 32)
Enter the **Username** and **Password** for each user to allow the user to log on to the panel.
Select the **Partition** and **Area** for which this code is valid
Then select the attributes for each user code **Arm**, **Disarm** and **System Access** options.

- Installer User Name:** Installer’s login name for connecting to the Meridian 64. No commas or spaces allowed
- Installer Password:** Installer’s password for connecting to the Meridian 64. No commas or spaces allowed

Now click on the **Save** button to save this data.

Auto Arm Tab

Click on the **Auto Arm Tab** to setup the auto arm parameters.



Auto Arming Select **Partitions** and **Areas** to auto arm or disarm then enter the time in 24 hour format. If a **Pre-Alert** time is entered the keypad will generate an audible alert before the panel auto arms. Two different auto arm and disarm times may be programmed per partition.

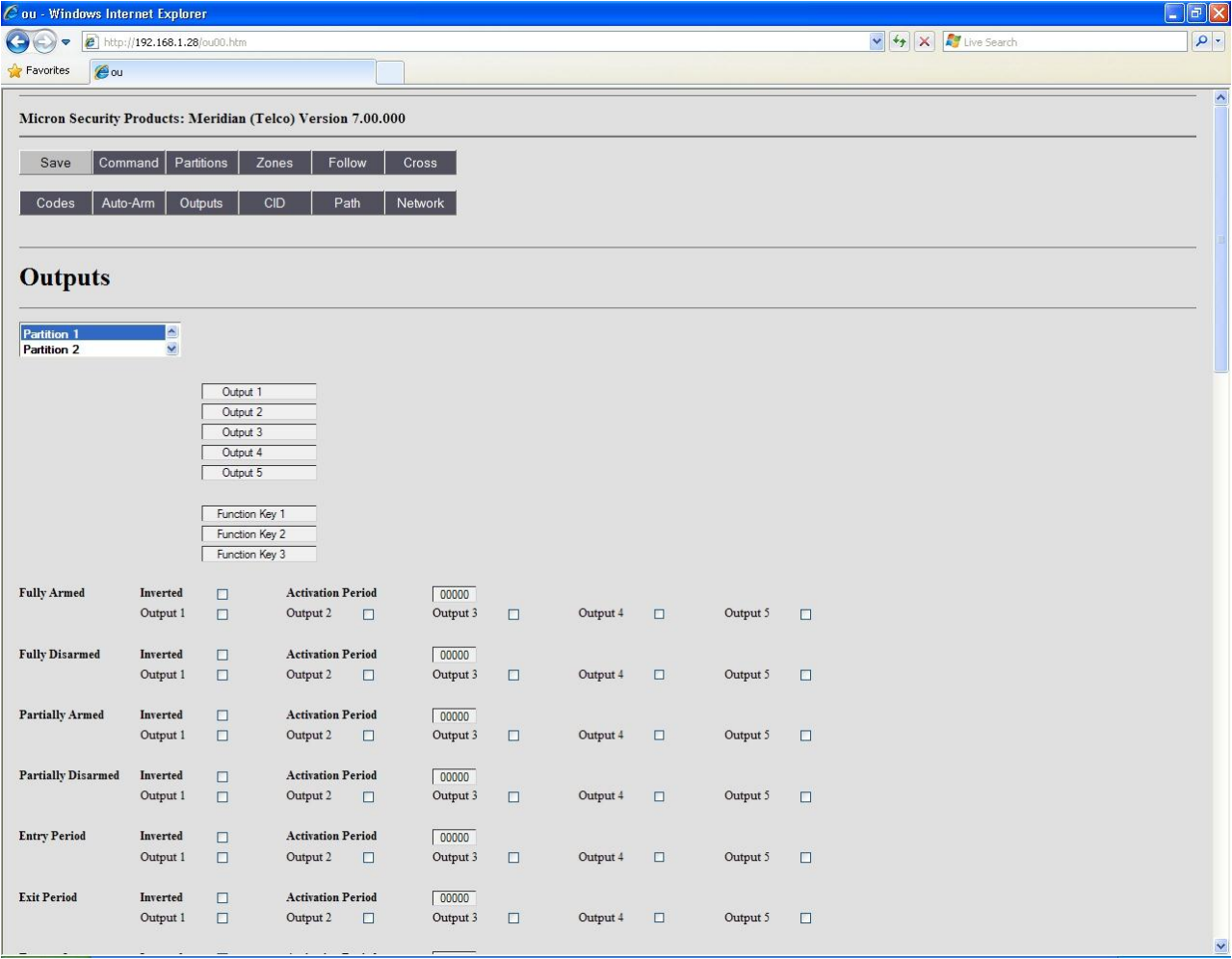
Meridian 64 Time and Date Setup:

Click the **Synchro** button to synchronize the Meridian 64’s date and time with the computer time.

Now click on the **Save** button to save this data.

Outputs Tab

Click on the **Output Tab** to setup outputs.



Output 5 is indicated as a Siren Output on the circuit board. Any Output label may be personalised in the Output Tab.

Output Options:

Inverted	Inverts output polarity from NO to NC
Activation Period	Must be set for all selected outputs (value in seconds); if zero then output is latched.
Fully Armed	When system armed the selected output will activate.
Fully Disarmed	When system disarmed the selected output will activate.
Partially Armed	When system partially armed the selected output will activate.
Partially Disarmed	When system partially disarmed the selected output will activate.
Entry Period	Output follows entry period
Exit Period	Output follows exit period
Tamper 1	A tamper event will activate the selected output (eg siren)
Tamper 2	A tamper event will activate the selected output (eg siren)
Alarm 1	An alarm event will activate the selected output (eg siren).
Alarm 2	An alarm event will activate the selected output (eg siren).
24 Hour 1	A 24 hour event will activate the selected output (eg siren).
24 Hour 2	A 24 hour event will activate the selected output (eg siren).
Walk Test	Output can be used for walk test.
Sensor	Output can be used for sensor output.
Chime	Output can be used for chime mode.
Panic	A panic alarm will activate the selected output (eg siren). Pressing and holding 7 on the keypad for 2 seconds generates a panic alarm.

Medical	A medical alarm will activate the selected output (eg siren). Pressing and holding 8 on the keypad for 2 seconds generates a medical alarm.
Fire	A fire alarm will activate the selected output (eg siren). Pressing and holding 9 on the keypad for 2 seconds generates a fire alarm.
Duress	A duress event will activate the selected output (eg siren).
F1	Output can be used for function key 1 on the keypad.
F2	Output can be used for function key 2 on the keypad.
F3	Output can be used for function key 3 on the keypad.
Remote Locked**	Remote software access will activate the selected output.
Low Battery**	Low battery condition will activate the selected output.
Mains Failed**	Mains failure will activate the selected output.
Bus Failed**	Output can be used for RS485 communication failure.
Gateway1 Failed**	Network communication failure of Gateway 1 will activate the selected output. Output can be used to reset the router after a communication fail event. Output delay time allows the router time to synchronise after a communication fail reset.
Gateway2 Failed**	Network communication failure of Gateway 2 will activate the selected output. Output can be used to reset the router after a communication fail event. Output delay time allows the router time to synchronise after a communication fail reset.
Telco Failed**	Output can be assigned for Telco communication failure.
GPRS Failed**	Output can be assigned for GPRS communication failure.
SMS Failed**	Output can be assigned for SMS communication failure.
Transmit Gateway 1**	Output turns on for the duration of the selected activation time during internet transmission.
Transmit Gateway 2**	Output turns on for the duration of the selected activation time during internet transmission.
Transmit Telco**	Output turns on for the duration of the selected activation time during telephone transmission.
Transmit GPRS**	Output turns on for the duration of the selected activation time during GPRS transmission.
Transmit SMS**	Output turns on for the duration of the selected activation time during SMS transmission.

These functions are only valid for **Partition 1 as these are internal functions

Now click on the **Save** button to save this data.

CID Tab

Click on the **CID Tab** to setup Meridian 64’s Contact ID parameters.

ci - Windows Internet Explorer

http://192.168.1.28/ci.htm

Live Search

ci

Micron Security Products: Meridian (Telco) Version 7.00.000

SaveCommandPartitionsZonesFollowCross

CodesAuto-ArmOutputsCIDPathNetwork

CID Events

		Gateway 1	Gateway 2	Telco	GPRS	SMS	
Reset	305	1	0	0	0	0	
Arm/Disarm (Full)	400	1	0	0	0	0	
Arm/Disarm (Partial)	402	1	0	0	0	0	
Fire	700	1	0	0	0	0	SGD 0 Multi-Drop ☐
Medical	100	1	0	0	0	0	
Panic	120	0	0	0	0	0	
Duress	121	1	0	0	0	0	
Tamper	137	1	0	0	0	0	
Alarm	130	1	0	0	1	1	
Communication Failed	354	1	0	0	0	0	
Battery	302	1	0	0	0	0	Delay before Event 01800
Mains	301	1	0	0	0	0	Delay before Event 01800
Bypassed	570	1	0	0	0	0	
Remote	412	1	0	0	0	0	
Periodic Test (1)	602	1	0	0	0	0	Test Period 00000060
Periodic Test (2)	603	1	0	0	0	0	Test Period 00000060

For each event enter the CID event code to transmit to a monitoring station.

Establish the CID event reporting priority by entering numbers **1** to **5** in the Gateway 1, Gateway 2, Telco, GPRS and SMS columns. A **1** establishes first priority, **2** a secondary priority, **3** a third priority, **4** a fourth priority and **5** a fifth priority. If **zero** (0) is selected there will be no transmission of this event via this pathway.

If an event has **1** entered in the Gateway 1 column and **2** in the GPRS column, for example, then this event will be communicated via the Gateway 1 internet router. If this communication fails the GPRS alternate pathway will be attempted.

If an event has **1** entered in the Gateway 1 column and **1** in the SMS column then this event will be communicated via both pathways simultaneously.

If an event has **1, 2, 3, 4, 5** entered, in any order, then this event will be communicated via pathways in this order of priority until a successful acknowledgement has been received from the central monitoring station. If a successful acknowledgement is received from the first pathway (**1**) then no further communications are attempted. An SMS transmission is not acknowledged.

Reset

Sent to the central station each time the Meridian 64 is powered on.
This event transmits the firmware version of the panel as Area 01 and the zone as the main firmware version eg 7.

Event 305 (Reset Event)

Area Zone

01 7 (firmware version)

Arm/Disarm (Full)

Sent to the central station each time the Meridian 64 is armed or disarmed.
(Optional if KeySwitch option selected)

Arm/Disarm (Partial)

Sent to the central station each time the Meridian 64 is armed or disarmed.

Fire

Sent to the central station if a fire alarm is generated from a keypad (pressing and holding 9).

Medical	Sent to the central station if a medical alarm is generated from a keypad (Pressing and holding 8).																					
Panic	Sent to the central station if a panic alarm is generated from a keypad (pressing and holding 7).																					
Duress	Sent to the central station if an arm or disarm under duress is generated from a keypad																					
Tamper	Sent to the central station if a tamper is triggered.																					
Alarm	Sent to the central station when an alarm is generated.																					
Communication Failed	Sent to the central station when a communication fail event has occurred. This event transmits the communication failures of the panel as an Area and a zone, defined as follows: Event 354 (Communication Failed) <table><tr><th>Area</th><th>Zone</th><th></th></tr><tr><td>01</td><td>16</td><td>Ethernet Cable</td></tr><tr><td>01</td><td>01</td><td>G1 IP1/IP2 Failed</td></tr><tr><td>02</td><td>02</td><td>G2 IP3/IP4 Failed</td></tr><tr><td>03</td><td>01</td><td>Telco Failed</td></tr><tr><td>04</td><td>01</td><td>GPRS Failed</td></tr><tr><td>05</td><td>02</td><td>SMS Failed</td></tr></table>	Area	Zone		01	16	Ethernet Cable	01	01	G1 IP1/IP2 Failed	02	02	G2 IP3/IP4 Failed	03	01	Telco Failed	04	01	GPRS Failed	05	02	SMS Failed
Area	Zone																					
01	16	Ethernet Cable																				
01	01	G1 IP1/IP2 Failed																				
02	02	G2 IP3/IP4 Failed																				
03	01	Telco Failed																				
04	01	GPRS Failed																				
05	02	SMS Failed																				
Battery	Sent to the central station if the low battery condition exceeds the Low Battery Delay time																					
Delay before Low Battery Event	Delay before sending Low Battery to the central receiving station in seconds																					
Mains	Sent to the central station when mains failure exceeds the Mains Delay time																					
Delay before Mains Failed Event	Delay before sending Mains Fail to the central receiving station in seconds																					
Bypassed	Sent to the central station when a zone is bypassed.																					
Periodic Test 1	Sent to the central station when a periodic system test occurs for the selected path(s)																					
Periodic Test 2	Sent to the central station when a periodic system test occurs for the selected path(s)																					
Test Period	Enter the monitoring station test signal period in seconds																					
Test Period	Enter the monitoring station test signal period in seconds																					

Now click on the **Save** button to save this data.

Path Tab

Click on the **Path Tab** to set phone numbers and Meridian 64 communication options.

te - Windows Internet Explorer

http://192.168.1.28/te.htm

Live Search

te

Micron Security Products: Meridian (Telco) Version 7.00.000

SaveCommandPartitionsZonesFollowCross

CodesAuto-ArmOutputsCIDPathNetwork

Telco

Phone Number 13608619

Phone Number 23608619

Modem StringATS16=50S17=50S18=5S19=7S1A=3S1B=1SE1=0SF5=24SF6=24SF

GPRS

IP Destination 1219088071179

IP Destination 2219088071179

Destination Port 100012

Destination Port 200012

Time Out010

SMS

Message Service Center+6421600600

Phone Number0211234567

GSM / PDU Mode☐

Telco

Phone numbers 1 and 2 are the monitoring station phone numbers for transmitting CID reporting

Modem String International String to set up the internal Modem

GPRS

IP Destination 1 IP address of the central station receiver or DNS address**

IP Destination 2 IP address of the central station receiver or DNS address**

Destination Port IP1 Port identifier of the central station receiver application**

Destination Port IP2 Port identifier of the central station receiver application**

Time Out Maximum TCP/IP propagation delay before attempting the next IP address

**** This data is supplied by the central monitoring station**

SMS

Phone and Message Service Personal mobile phone number and message service centre number.
Contact the mobile network operator for their service centre number.

GSM / PDU Mode If the GSM/PDU mode is ticked, the phone number format to send SMS messages must be in the international format but without the + symbol eg. 6427123456.

Now click on the **Save** button to save this data.

Network Tab

Click on the **Network Tab** to setup the TCP/IP parameters.

The screenshot shows the 'Network' tab of the Meridian (Telco) Version 7.00.000 configuration utility. The interface includes a top menu bar with 'Save', 'Command', 'Partitions', 'Zones', 'Follow', and 'Cross'. Below this is a sub-menu with 'Codes', 'Auto-Arm', 'Outputs', 'CID', 'Path', and 'Network'. The 'Network' section contains the following fields:

- MAC Address:** 00 01 02 03 04 67
- IP Address:** 192 168 001 028
- Subnet:** 255 255 255 000
- DNS Server:** 008 008 008 008
- Local Port:** 01098
- Gateway(1):** 192 168 001 001
- IP Destination 1:** 192 168 001 011
- DNS Address 1:** [Empty]
- Destination Port 1:** 00012
- IP Destination 2:** 192 168 001 011
- DNS Address 2:** [Empty]
- Destination Port 2:** 00013
- Gateway(2):** 192 168 001 001
- IP Destination 3:** 192 168 001 011
- DNS Address 3:** [Empty]
- Destination Port 3:** 00012
- IP Destination 4:** 192 168 001 011
- DNS Address 4:** [Empty]
- Destination Port 4:** 00013
- Remote Port:** 00080
- Gateway 1 Sync:** 00060
- Max Resets:** 005 within 00001
- Gateway 2 Sync:** 00060
- Max Resets:** 005 within 00001
- Time Out:** 002
- DHCP:** ☐
- Auto-Increment:** ☐
- Battery Saving:** ☐
- CID CheckSum:** ☐
- Encryption:** ☐
- UDP:** ☐
- IP1 First:** ☒
- LOCKED:** ☐
- Tx Identification:** TX_IDT yo_from_micron
- Buttons:** Reboot, Backup, Browse..., Restore

The date 'Tuesday, 11 October 2011' is displayed at the bottom right.

- Mac Address

The MAC address is the unique identifier assigned to the EC-2. (Enter hexadecimal data).
No action required (change only when a network MAC address conflict occurs)
- IP Address

The network administrator must assign a fixed IP address. This is the logical IP address of the EC-2 in the local network. If DHCP is ticked this section is disabled.
- Local Port

No action required
- Gateway 1

Only available when DHCP is not ticked. The network administrator must assign a gateway address if DHCP is not ticked. A gateway is a network point that acts as an entry to the internet, usually the local router address.
- Gateway 2

Only available when DHCP is not ticked. The network administrator must assign a gateway address if DHCP is not ticked. A secondary gateway is a network point that acts as a secondary entry to the internet, usually an alternate local router address.

If Gateway 2 is established in your network then this will be used in the event that communications on Gateway 1 fail.
- Subnet

Only appears when DHCP is not ticked. The network administrator must assign a subnet mask address if DHCP is not ticked.
- DNS Server

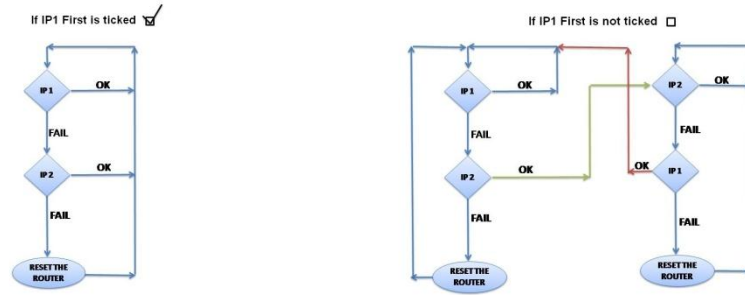
This address is obtained from the customer’s IT specialist or the IP monitoring station. **
A DNS server is a server that stores the DNS records
- IP Destination 1 or DNS Address 1

IP address of the central station receiver or DNS address**

The **Internet Protocol** (IP) address is a numerical label that is assigned to devices participating in a network utilizing the Internet Protocol for communication between its nodes.
Domain Name System (DNS) serves as the phone book for the Internet by translating computer host names into IP addresses. For example, www.centralstation.com translates to 203.114.129.9

Destination Port IP1	Port identifier of the central station receiver application** A number assigned to EC-2 sessions and central station receiver applications in an IP network.
IP Destination 2 or DNS Address 2	IP address of a 2 nd central station receiver or DNS address **
Destination Port IP2	Port identifier of the 2nd central station receiver application**
Remote Port	Web server port. This must match the forwarding port of the router to allow remote access to the EC-2.
Gateway 1 Sync	In the event an internet router communication fails within the parameters defined and the internet router is connected to the EC-2's communication fail relay (see page 12) then after EC-2 resets the router this is the time in seconds to allow the router to fully synchronise, " adsl.isp... " before the EC-2 makes further transmission attempts. Typically an ADSL router will require 60 - 120 seconds to synchronise.
Max Resets....Within	This is the number of router resets allowed 'within' this period in seconds. After the number of resets within the period has been reached, the EC-2 will continue to try to communicate but without further attempting to reset the router.
Gateway 2 Sync	In the event an internet router communication fails within the parameters defined and the internet router is connected to the EC-2's communication fail relay (see page 12) then after EC-2 resets the router this is the time in seconds to allow the router to fully synchronise, " adsl.isp... " before the EC-2 makes further transmission attempts. Typically an ADSL router will require 60 - 120 seconds to synchronise.
Max Resets....Within	This is the number of router resets allowed 'within' this period in seconds. After the number of resets within the period has been reached, the EC-2 will continue to try to communicate but without further attempting to reset the router.
TimeOut	Maximum TCP/IP propagation delay before attempting the next IP address
DHCP	If the network router is set to DHCP then this must be ticked. The IP address will be automatically allocated by the router. If the network router is not set to DHCP then a unique IP address must be entered for the EC-2. ** DHCP is a protocol used to dynamically distribute the IP address to the EC-2. ** This data is supplied by the central monitoring station
Auto-Increment	Default is ticked. The local port identifier is incremented with each transmission. If not ticked then the Local Port count is not incremented.
Battery Saving	In the event of a power failure the EC-2 will power down the router and only power it up for the time required for an alarm transmission.
CID Checksum	Contact ID Checksum will be transmitted in the CSV format to the central station with each transmission if ticked. Default is ticked.
Encryption	If ticked the EC-2 sends encrypted data to the monitoring station.
UDP	If UDP is ticked, the system will transmit UDP over Internet Protocol instead of TCP/IP.
IP1 First	If IP1 First is ticked, the system will transmit the signal to destination IP1. If the transmission is successful, IP1 will be used for subsequent transmissions. If the IP1 transmission fails, IP2 will be used to send the transmission. Subsequent transmissions will revert back to IP1. Should this transmission fail again, the router will be reset and IP1 retried.

If **IP1 First** is not ticked, the system will transmit the signal to destination IP1. If the transmission is successful, IP1 will be used for all subsequent transmissions. If the IP1 transmission fails, IP2 will be used to send the transmission. Subsequent transmissions will continue on IP2 until a failed transmission occurs. Transmission will then revert to IP1 and remain on IP1. If transmission attempts to both IP1 and IP2 fail, the router will be reset and the system will return to the last communication cycle.



LOCKED

If ticked, no users or installers will be able to access the **Network Tab**.

If **LOCKED** is ticked and the Master User Name and Password are lost the Meridian 64 will need to be returned to the micron factory to be unlocked.

Tx Identification

Message identification for the central station**

Reboot

Reset the system.

Backup

Backup the latest changes on the EC-2 in XML format to your computer storage.

Restore

Restore a previously backed up XML file to the EC-2.
First click on the browse button to locate the saved XML file then click on Restore.

**** This data is supplied by the central monitoring station.**

Now click on the **Save** button to save this data.

Meridian Factory Default

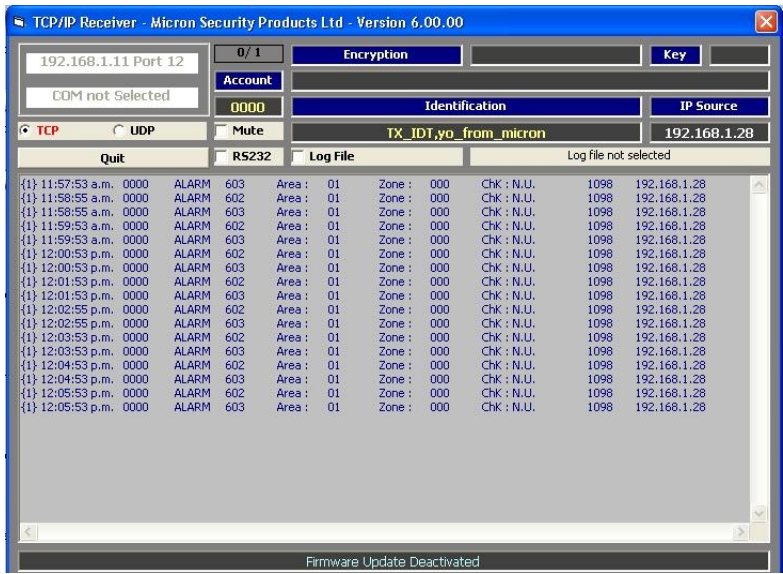
Power down the system, shunt the reset pin on the panel, re-apply the power, wait for 20 seconds, remove the reset pin and then reset the board again.

Important: When ANY changes to ANY location are made in the **Network Tab** you **MUST** reset the board.

Meridian 64 Receiver Self Test Software

This software displays EC-2 communications on a local or remote personal computer when the EC-2 has been connected and setup on your network. Ensure that the computer running the Receiver Software is set to the IP address (192.168.1.7) that has been set as the destination address in the EC-2. The receiver is listening on Port 12 by default.

Start the **Receiver V6-00-00.exe** software in the **Receiver V6-00-00.zip** file and the following screen will appear.



Trigger zones to view communications

RS232	Every message is forwarded in Ademco 685 format when selected.
-------	--

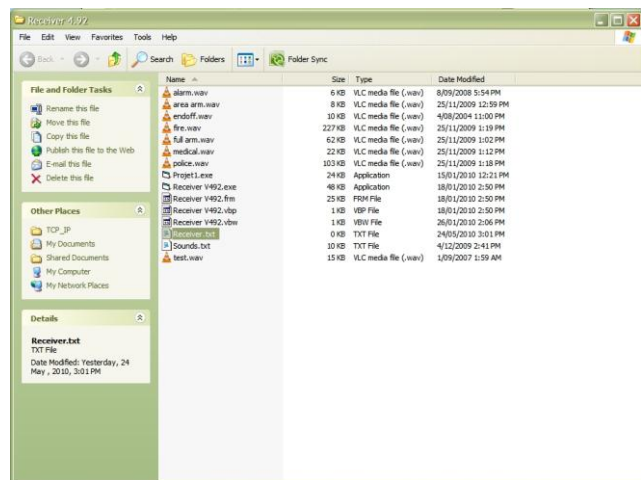
Log File A receiver log file is saved as a text file to the computer hard drive for future reference. Files are saved in this date and time format: **2011317120 Receiver History.log**

Download Firmware Upgrade

Firmware upgrades can be downloaded to the Meridian 64 using this receiver software.

Download the Firmware Upgrade Guide from micron's secure website.

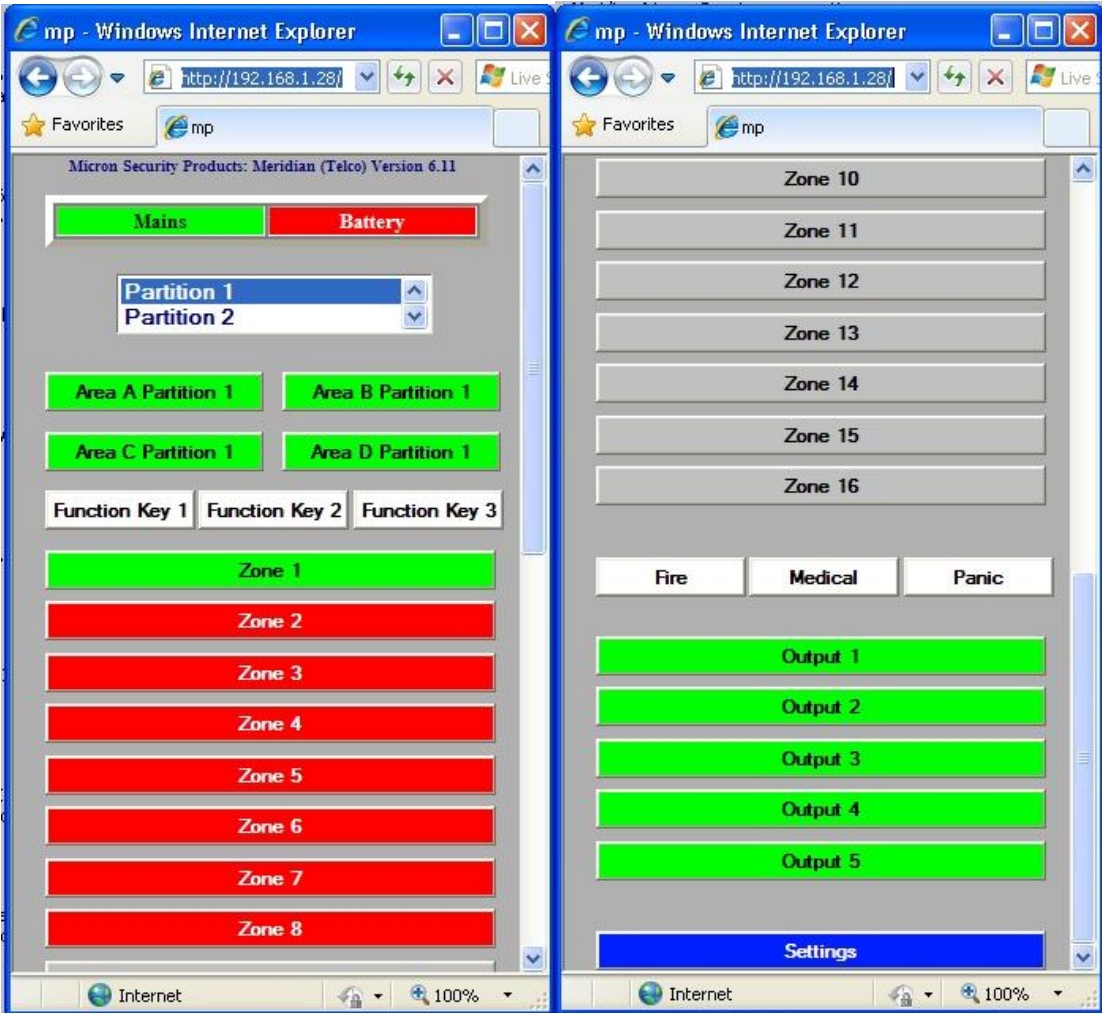
Explanation of .txt files



Sounds.txt Each Contact ID event sound can be changed in this text file. Save the **.wav** file in the same folder as the receiver software (for example **panic.wav**) and align it with the corresponding Contact ID code to trigger the sound. When an event is triggered the appropriate sound is played by the computer attached to the Meridian.

Param.txt This file details the settings of the receiver software. The screen labels can be customised in this file.

Smart Phone Screen



See the explanation for all smart phone keypad functions in the Command Tab section.

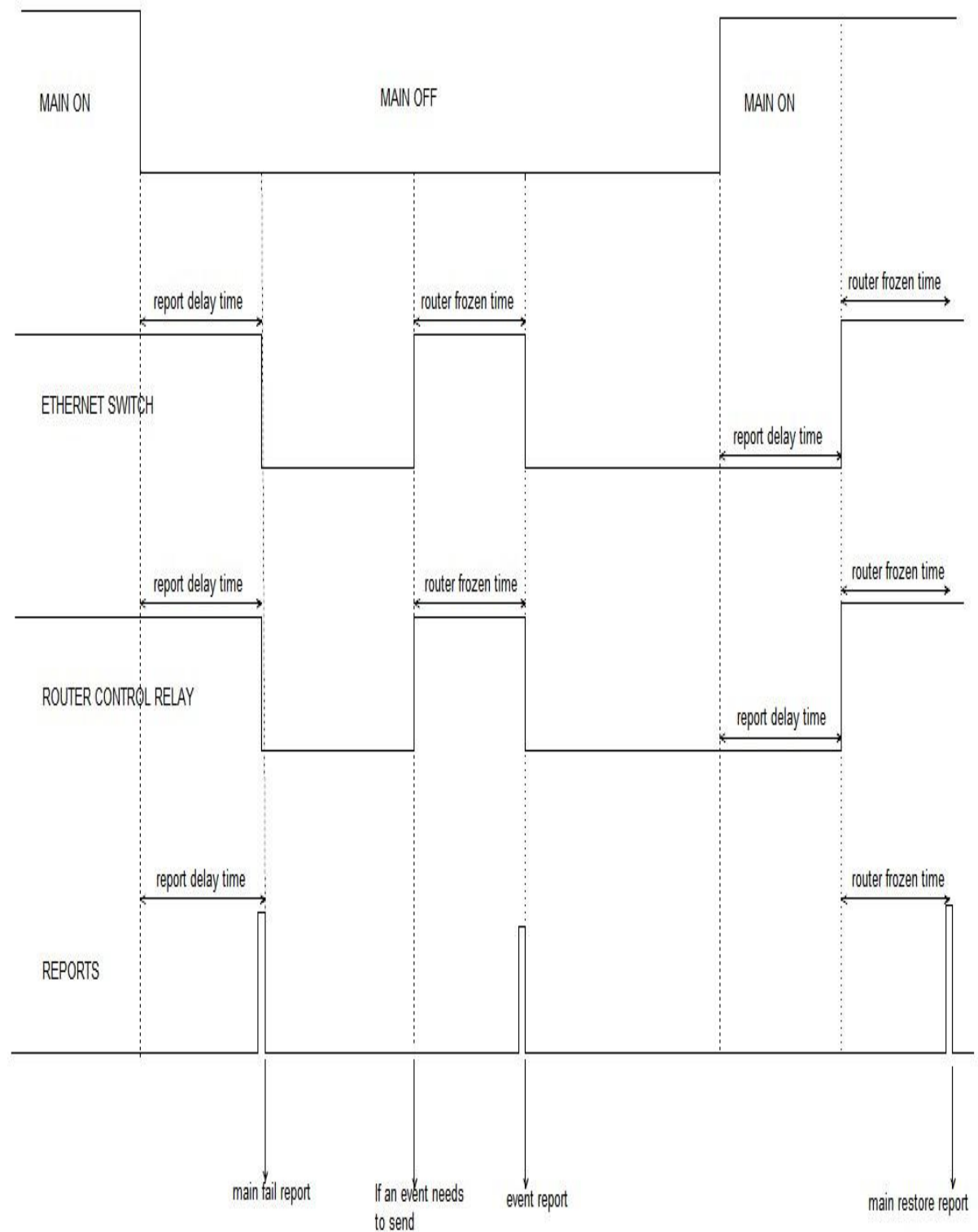
If the user that has logged on to the above screen has the appropriate security settings assigned to their username then by clicking the **Settings** button they are able to access assigned panel settings in the **Command**, **Codes** and **Auto Arm** tabs.

It is recommended that the installer block user access to the **Partitions**, **Zones**, **Follow**, **Cross**, **Outputs**, **CID**, **Path** and **Network Tabs** as these are specialist installer programming sections.

Keypad Command Map

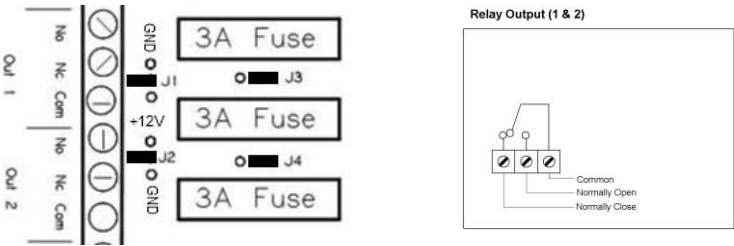
Quick arm all	0	#							
Quick arm A	1	#							
Quick arm B	2	#							
Quick arm C	3	#							
Quick arm D	4	#							
Arm All	<n>	<n>	<n>	<n>	#				
Disarm All	<n>	<n>	<n>	<n>	*				
Arm A	1	*	<n>	<n>	<n>	<n>	#		
Arm B	2	*	<n>	<n>	<n>	<n>	#		
Arm C	3	*	<n>	<n>	<n>	<n>	#		
Arm D	4	*	<n>	<n>	<n>	<n>	#		
Disarm A	1	*	<n>	<n>	<n>	<n>	*		
Disarm B	2	*	<n>	<n>	<n>	<n>	*		
Disarm C	3	*	<n>	<n>	<n>	<n>	*		
Disarm D	4	*	<n>	<n>	<n>	<n>	*		
Arm A (duress)	1	*	<n1>	<n2>	<n3>	<n4>	<n3>	<n4>	#
Arm B (duress)	2	*	<n1>	<n2>	<n3>	<n4>	<n3>	<n4>	#
Arm C (duress)	3	*	<n1>	<n2>	<n3>	<n4>	<n3>	<n4>	#
Arm D (duress)	4	*	<n1>	<n2>	<n3>	<n4>	<n3>	<n4>	#
Disarm A (duress)	1	*	<n1>	<n2>	<n3>	<n4>	<n3>	<n4>	*
Disarm B (duress)	2	*	<n1>	<n2>	<n3>	<n4>	<n3>	<n4>	*
Disarm C (duress)	3	*	<n1>	<n2>	<n3>	<n4>	<n3>	<n4>	*
Disarm D (duress)	4	*	<n1>	<n2>	<n3>	<n4>	<n3>	<n4>	*
Start Walk Test	5	#							
Zone Bypass	9	<z>	#						
or	9	<z>	<z>	#					
Assign Keypad to Partition	1 (hold)	<p>	#						
		<0>	#	Access any partitions					
Assign Keypad to Areas	2 (hold)	<a>	#						
or	2 (hold)	<a>	<a>	#					
Program Slave/Master	3 (hold)	<0>	#	master					
		<1>	#	slave					
Send Key 7	7 (hold)	Panic							
Send Key 8	8 (hold)	Medical							
Send Key 9	9 (hold)	Fire							
Send Key F1	F1								
Send Key F2	F2								
Send Key F3	F3								
Cancel Auto Arm	0 (hold)								
	Hold = 2 secs								
Display Control Status	*								
1	Mains	Off=OK	On=Fault						
2	Battery	Off=OK	On=Fault						
3	Telco	Off=OK	On=Fault						
4	Ethernet	Off=OK	On=Fault						
5	Siren Output	Off=OK	On=Fault						
6	Auxiliary Fuse	Off=OK	On=Fault						
7	RF	Off=OK	On=Fault						
Press any key to cancel system status fault attention beep									

BATTERY SAVING EXPLAINED

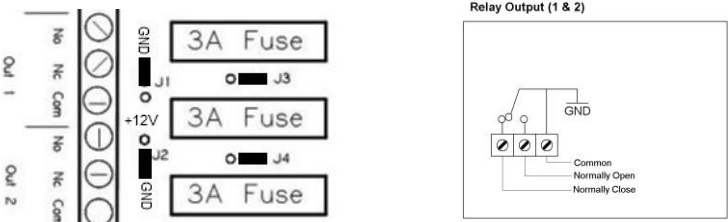


Meridian 64 Relay Output Configuration Options

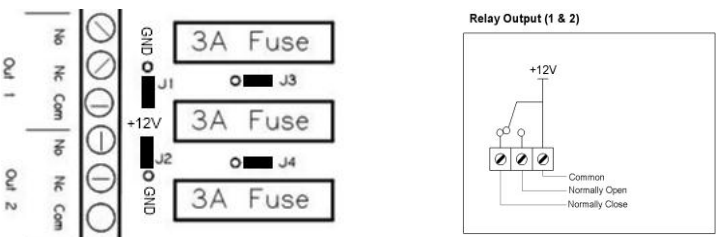
Out1 and Out2 as a switch



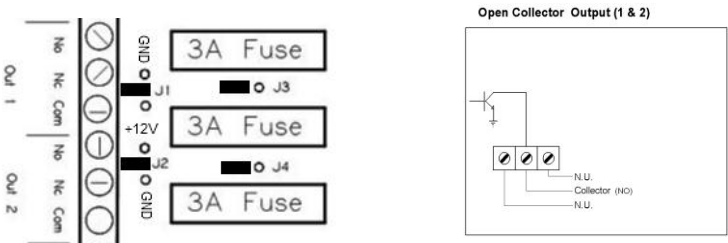
Out1 and Out2 common is ground



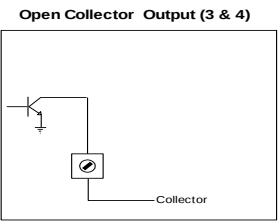
Out1 and Out2 common is +12V



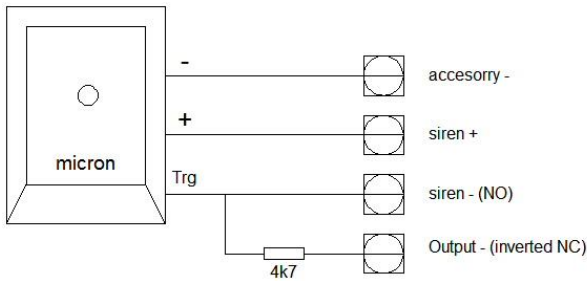
Setup Out1 and Out2 as an open collector



Output 3 and 4 are open collector outputs



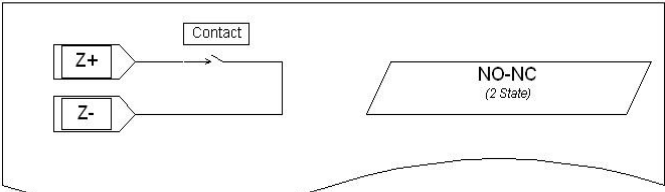
Siren output schematic



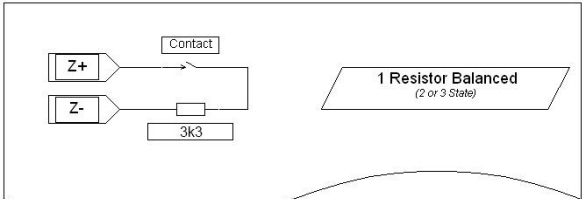
Example of a micron external siren connection

Zone Connection Schematic

If Normally Open contacts are used, zones need to be inverted from the setup software.

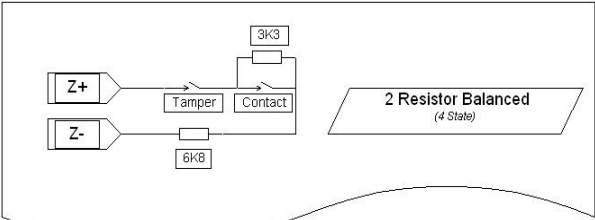


NO/NC (Normal/Alarm)

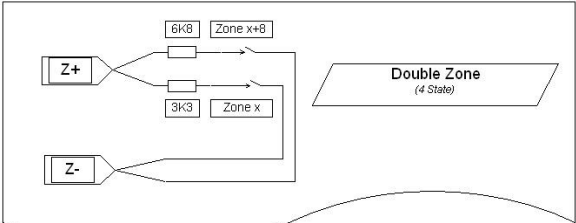


1x Resistor (Alarm /Normal/Alarm)
(Short Circuit or open contact both generates alarm)

1x Resistor (Short Circuit Protection/Normal/Alarm)
(Short Circuit generates tamper. Open contact generates alarm)

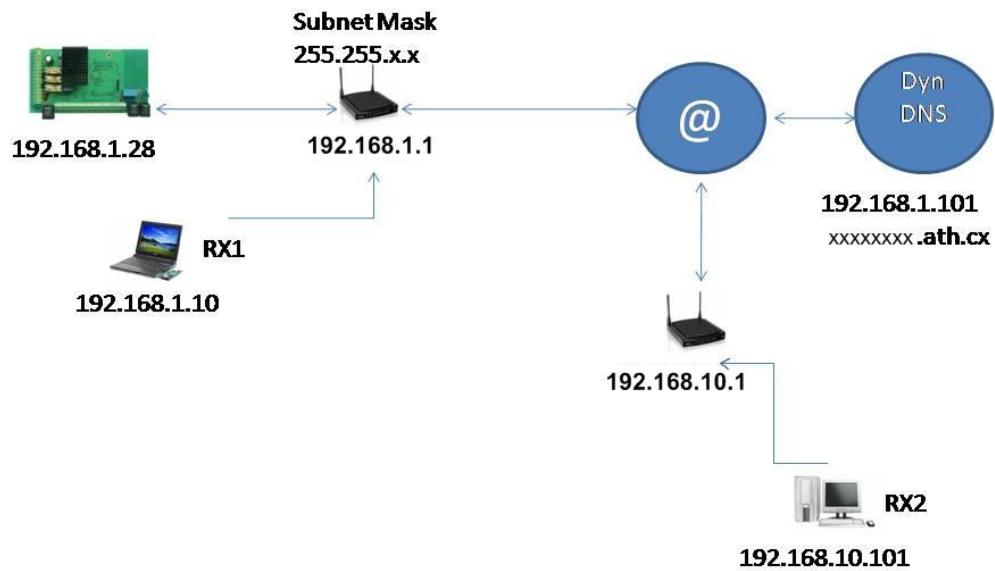


2x Resistor (Tamper/Normal/Alarm/Short Circuit Protection)
(Tamper and Short circuit generate tamper. Open contact generates alarm)

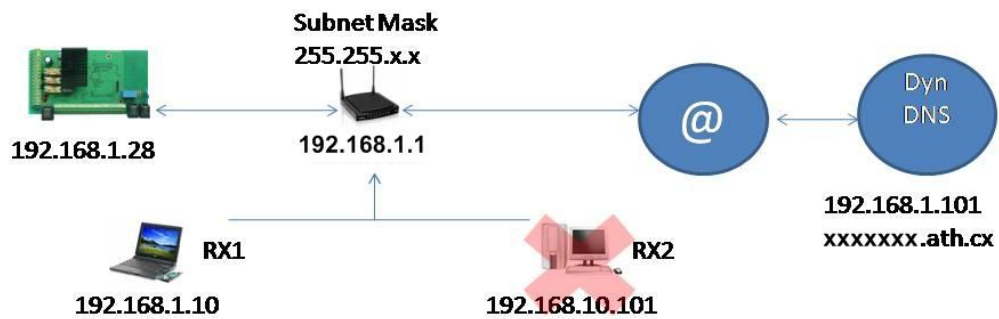


Double Input, (3K3 for low inputs and 6K8 for high inputs)

Correct DynDNS Connection



Wrong DynDNS Connection



WARRANTY

1. Subject to clause 2 below, micron warrants this product against defects in materials and workmanship for a period of 24 months from the date of delivery to the purchaser as follows:
 - (a) Micron will repair or replace free of charge any goods or part thereof found to be defective by reason of faulty material or workmanship.
 - (b) The purchaser must give micron notice of the alleged defect within 14 days of it becoming apparent and must return the defective goods or part thereof to micron.
2. This guarantee does not apply or extend to:
 - (a) Any product altered or repaired by any person other than micron so as in Micron's sole judgement to adversely affect the product.
 - (b) Damage, malfunction or failure arising from accident, misuse or misapplication, neglect, modifications, use of unauthorised replacement parts or accessories, exceeding the specific ratings, improper voltage or connection of any wire to any part of the circuit board other than the terminal block.
 - (c) Any product where the rating label or serial number is removed or altered.
 - (d) Any consequential or indirect loss.

Notice of Liability

While every effort has been made to ensure the accuracy of this document, neither Micron Security Products Ltd nor any of its official representatives shall have any liability to any person or entity with respect to any liability, loss or damage caused or alleged to be caused directly or indirectly by the information contained in this manual. Should any error or inconsistency be found, please notify us.

Micron Security Products Ltd reserves the right to make changes to features and specifications at any time, without notification, in the interest of ongoing product development and improvement. Most up to date versions of this manual can be downloaded from micron's secure web site.

Designed and manufactured in New Zealand by

micron
security products

Micron Security Products Ltd
30-32 Crummer Road
PO Box 78-006 Grey Lynn
Auckland New Zealand
Phone: 64 9 378 6098
Facsimile: 64 9 378 6454
Email: info@micronsecurity.com
www.micronsecurity.com