CEM SYSTEMS
From Tyco Security Products

emerald

Quick Start Installation Guide

TSR-UL-0061-1.3

Notice

The information in this manual was correct at the time of publication. Tyco Security Products reserves the right to modify this product. All specifications are subject to change without notice.

© Copyright 2015 Tyco Security Products

Under copyright laws, the contents of this manual may not be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent of Tyco Security Products. All Rights Reserved.

Trademarks

The trademarks, logos, and service marks displayed on this document are registered in the United States (or other countries). Any misuse of the trademarks is strictly prohibited and Tyco Security Products will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco Security Products are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region. Contact your sales representative for more information.

Licence information

Your use of this product is governed by certain terms and conditions.

Support

If you require technical assistance using CEM products, please contact the CEM Support team using the following telephone number:

Telephone:+44(0)2890 456656

Email: cem.support@tycoint.com

• Please provide our support engineers with as much information as possible. This may include:

• Site name

• Product name and model

• CEM software version

• Description of the problem

Publication Date

12th January 2015

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures

Warning

English

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Français

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada.

Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Warning - For FCC Labelled emerald Terminals

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept an interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Installation of this device shall be performed by a qualified person in accordance to all local regulations.

This system must be installed within the protected premise in accordance with the National Electrical Code (NFPA70), and the local authorities having jurisdiction.

Equipment changes or modifications without the approval of the party responsible for compliance could void the user's authority to operate the equipment and could create a hazardous condition.

This page is intentionally blank.

Contents

1 Introduction 1

1.1 Terminal specifications 2

1.1.1 CEM emerald product codes 2

1.1.2 UL-294 grading 2

1.1.3 Terminal dimensions 3

1.1.4 Part ratings 3

1.1.5 emerald terminal key components 4

1.2 Simplified AC2000 Network Topology 5

1.3 Hardware Installation Process 6

2 Mounting the Terminal 7

2.1 Preparing for mounting 7

2.1.1 Recommended tools 7

2.1.2 Opening the terminal 8

2.1.3 Mounting the terminal’s back casing 9

3 Wiring the Terminal 11

3.1 Cabling requirements 11

3.1.1 Ethernet host 11

3.2 The Main Board 12

3.3 The Input/Output Board 13

3.4 Wiring locks 14

3.4.1 Wiring a voltage provided lock (internal power) 14

3.4.2 Wiring a voltage not provided lock (external power) 16

3.4.3 Output power switch 16

3.4.4 Supported third party read heads 16

3.5 Terminal with Request to Exit Switch 17

3.6 Configuration information 18

3.7 Terminal with Third Party Wiegand Read Head 19

3.8 Configuration information 20

3.9 Tamper Detection on Terminal Inputs 21

3.9.1 Wiring the resistor network 21

3.9.2 Re-assembling the terminal. 21

4 Terminal Network Configuration 23

4.1 Checking emerald's Network Status 23

4.2 Accessing the System Configuration Menu 24

4.2.1 Setting the terminal IP address, gateway and subnet mask 24

4.2.2 Network routing - (advanced users) 25

4.2.3 Testing the connection with the AC2000 server 25

5 Using the Terminal 27

5.1 Presenting your card 28

6 Diagnostics and Testing 31

6.1 Navigating the Menus 31

6.2 Accessing the System Configuration Menu 32

6.2.1 System Information menu 33

6.2.2 Tests menu 35

6.3 Maintenance 37

Chapter 1

Introduction

emerald (TS100/200/300) is an intelligent access terminal that is designed to control and monitor access at controlled doors.

Used as part of the AC2000 system, emerald controls access to restricted areas while giving the user a wide choice of information tools and applications at the door. **The AC2000 software suite has not been evaluated by UL**.

Figure 1 Photograph of the emerald terminal

1.1 Terminal specifications

emerald is available in three models; the TS100, TS200 and TS300. For the purposes of UL294, the connection and wiring for the access control function are identical for all three emerald models. **All three models provide the same access control functionality, however the TS200 and TS300 provide additional intercom and remote application functions that are not evaluated by UL and are not for use on UL installations.**

Note

The emerald terminal is for indoor use only.

1.1.1 CEM emerald product codes

Contact CEM sales for further information.

Card technology	TS100	TS200	TS300	FCC ID IC ID
Mifare CSN	TSR/100/105	TSR/200/105	TSR/300/105	QABTSR105V910 12009A- TSR105V910
Picopass	TSR/100/106	TSR/200/106	TSR/300/106	QABTSR608V93E 12009A- TSR608V93E
CEM DESFire	TSR/100/107	TSR/200/107	TSR/300/107	QABTSR608V93E 12009A- TSR608V93E
iClass/iClass SE	TSR/100/108	TSR/200/108	TSR/300/108	QABTSR608V93E 12009A- TSR608V93E
multi smart-card reader	TSR/100/608	TSR/200/608	TSR/300/608	QABTSR608V93E 12009A- TSR608V93E

Table 1: List of CEM emerald product codes

Note

The typical read range for the integrated 13.56MHz read-head is 3 – 5cm (1.2” – 2”)

Supported card technologies

The emerald multi smart-card reader supports the following card technologies:

- CEM DESFire
- MIFARE CSN
- iClass

Important

The appropriate card definitions must be loaded onto the CEM Central Database Computer (CDC).

1.1.2 UL-294 grading

The emerald terminal has been rated according to the UL-294 grading system and is outlined in Table 2:

Feature	Grading
Destructive attack	1
Line security	1
Endurance	4
Standby power	1

Table 2: UL-294 grading

1.1.3 Terminal dimensions

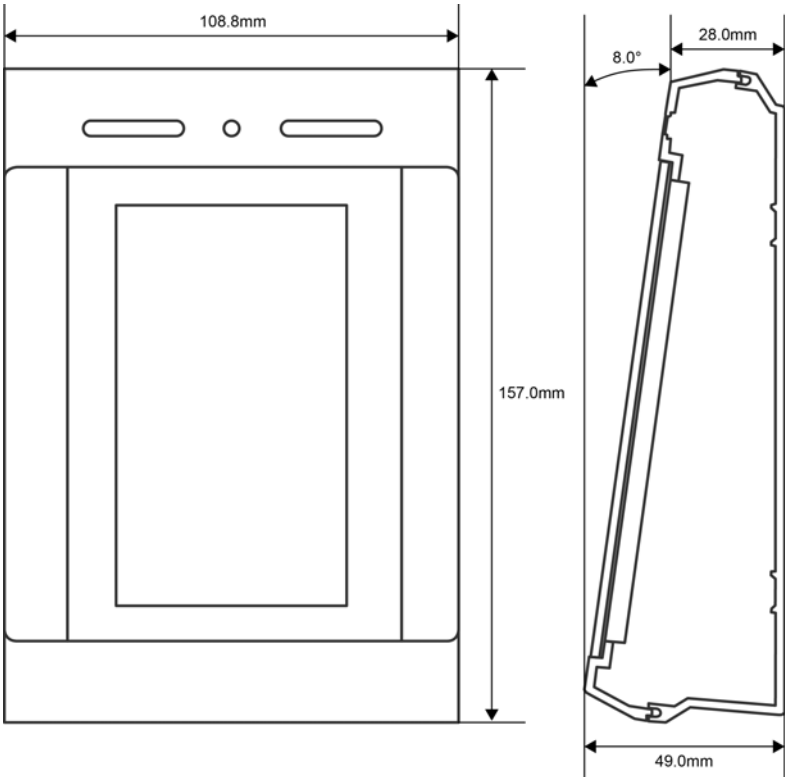


Figure 2 Illustration of emerald including dimensions

Dimensions of the emerald terminal:

Length: 157mm (6.2”)

Width: 109mm (4.3”)

Depth (bottom): 49mm (1.9”)

Depth (top): 28mm (1.1”)

1.1.4 Part ratings

emerald has been tested for operation within the ranges specified in the table below.

Part	Rating
emerald terminal	0º to 49ºC (32º to 120ºF) flame retardant polycarbonate, Humidity 5% to 95% non-condensing
DC power (unit only)	12V nominal (11.75V – 12.25V) @ 500mA peak. Shall be powered by an external UL294 or UL603 listed power-limited power supply with appropriate ratings and external power on indicator.
Inputs	Four supervised analog inputs - voltage supplied
Comms to system host	10/100 Base-T, TCP/IP, CAT5/5e/6, RJ45 connector
Dry contact relay outputs	0 - 30VDC @ 2A each[a]
Wet contact relay outputs	11.3-12VDC @ 1.3A combined between both outputs[b]
Ethernet communications	10/100BaseT Ethernet - RJ-45 connector
Memory	128MB RAM, 256MB NAND Flash supporting up to 250,000 cardholder records and 50,000 transactions off-line)

Table 3: Table of part ratings

a. When powered from an external source, the current per load is limited to 2A by the relay, but the total current drawn is also limited by the capability of the external power supply.
b. If the power to drive the relay loads are sourced from the internal supply, the total current required from the external supply is Relay 1 LOAD + Relay 2 LOAD + 0.5A.

1.1.5 emerald terminal key components

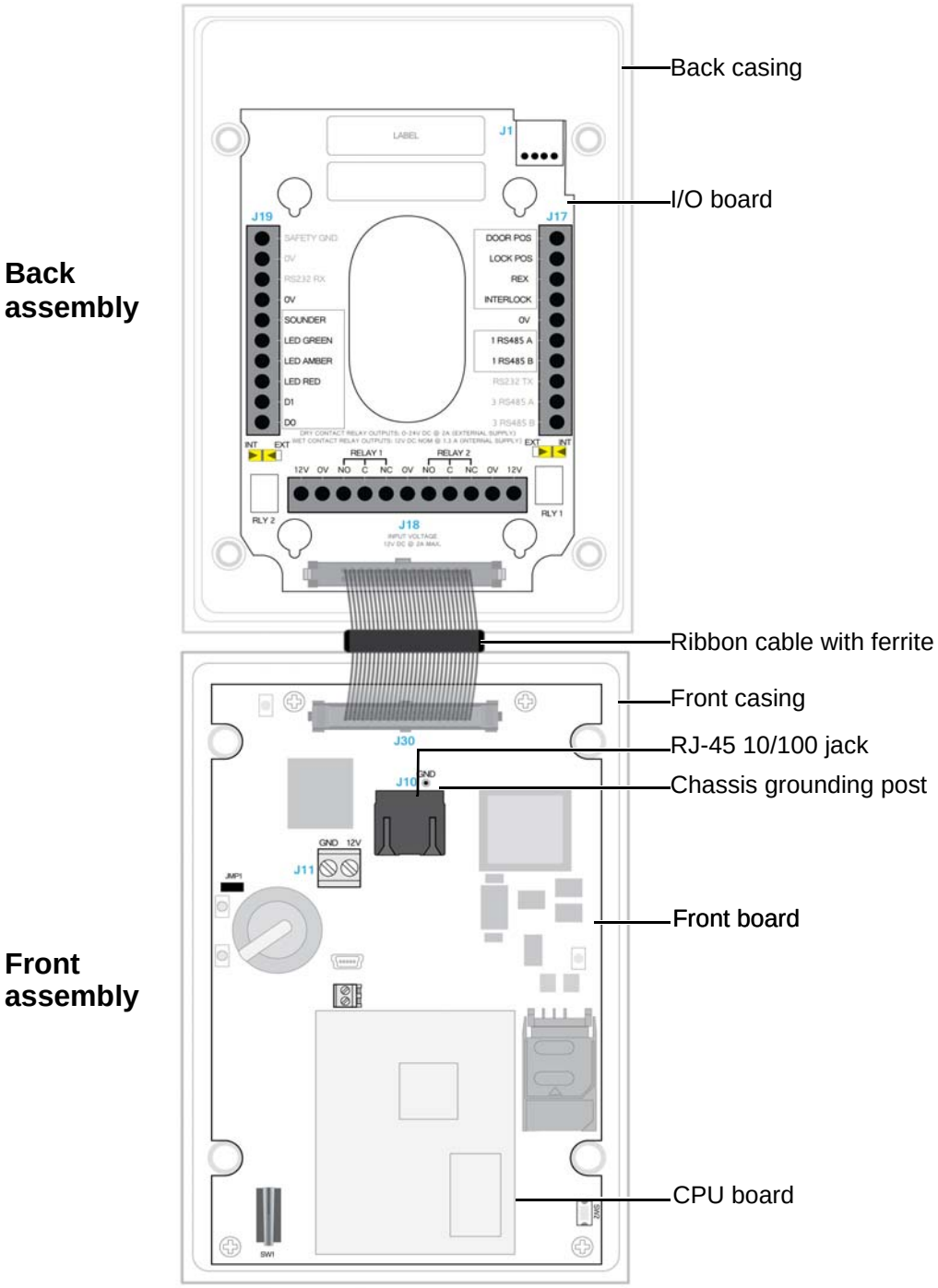


Figure 3 Illustration of the key component parts

Note

All emerald models use the same component parts.

1.2 Simplified AC2000 Network Topology

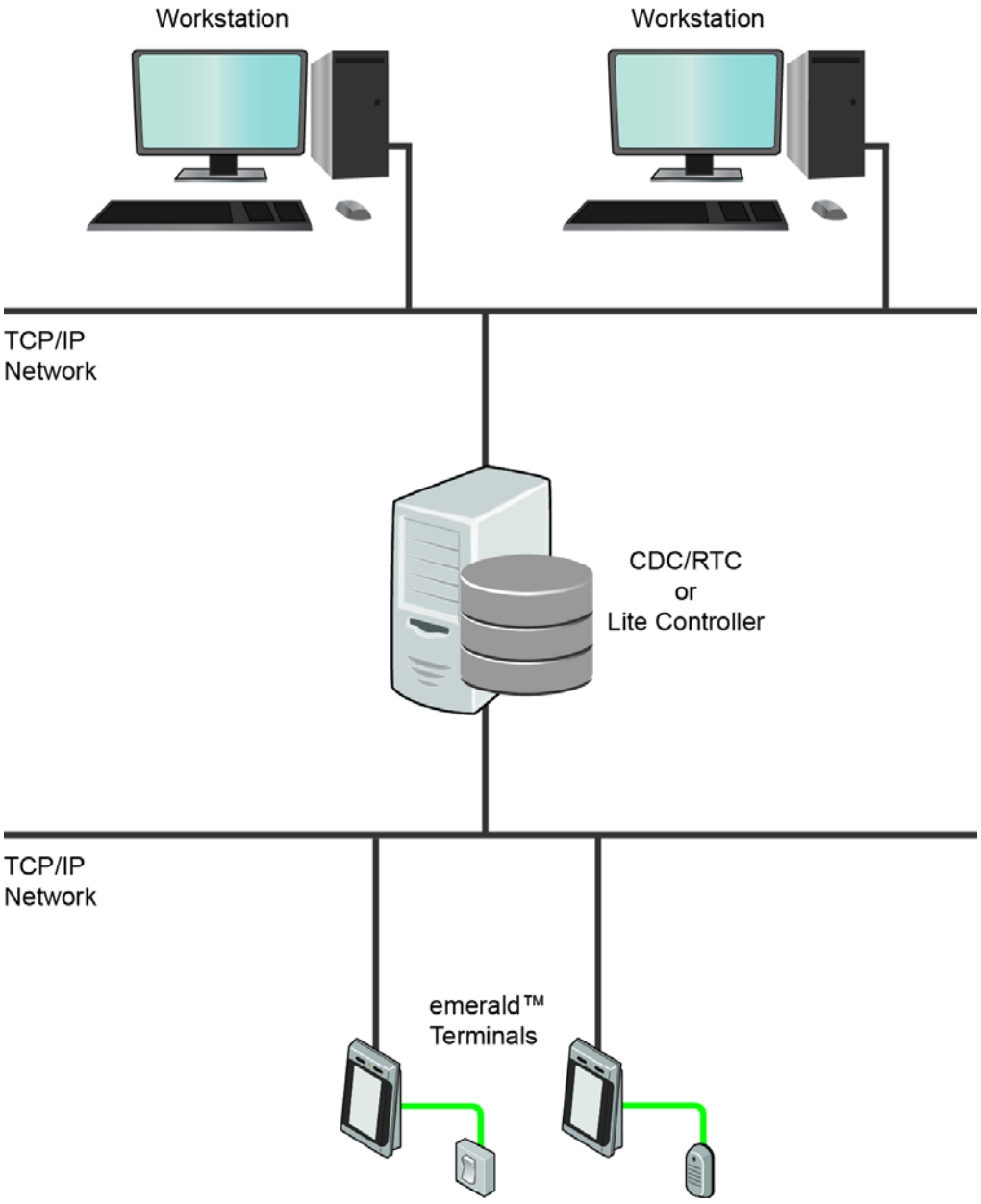


Figure 4 Basic illustration of a typical AC2000 network including emerald configurations

Important

The emerald terminal is only available as an ethernet device.

1.3 Hardware Installation Process

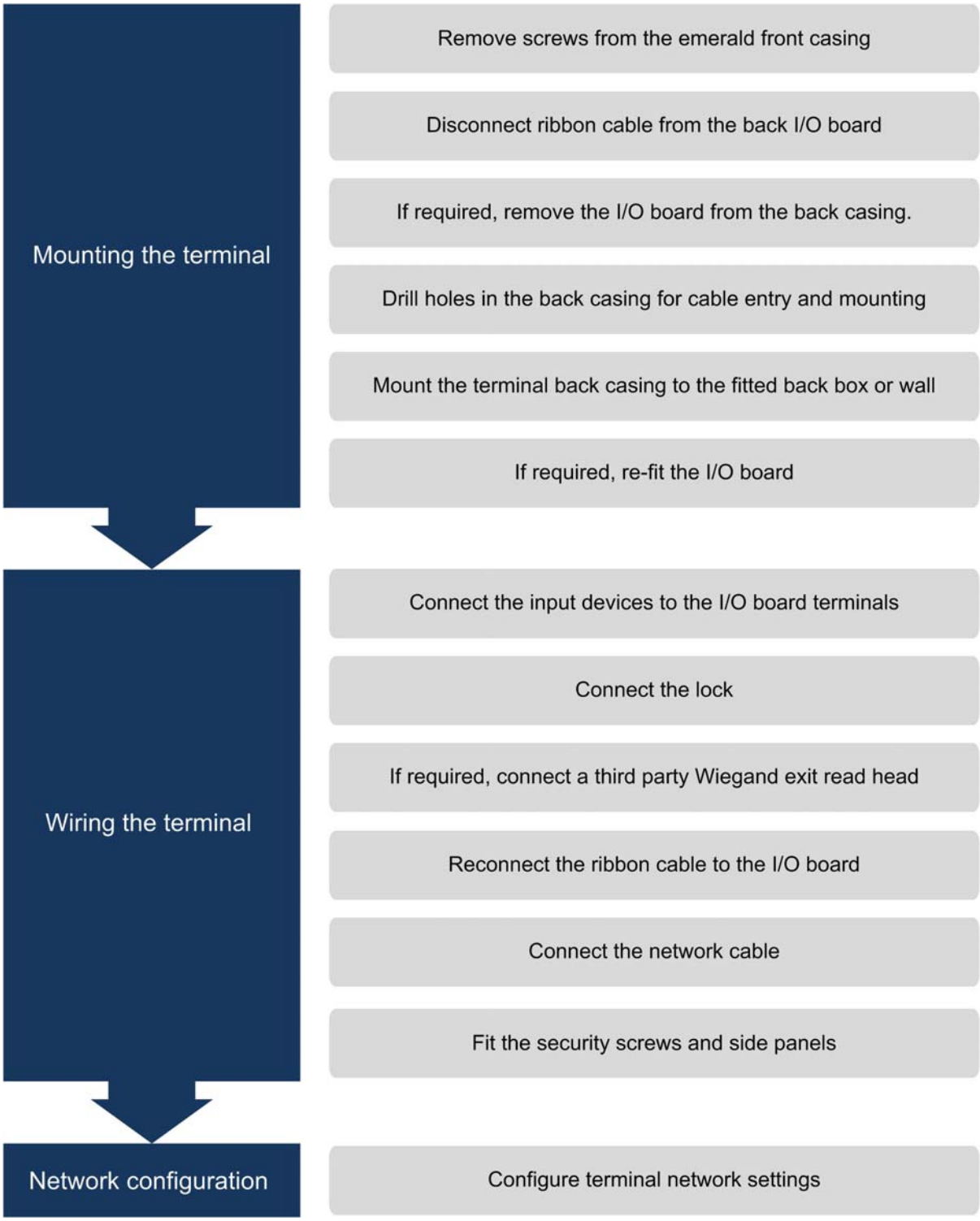


Figure 5 Hardware installation flow chart

Chapter 2

Mounting the Terminal

Important

Care must be taken when working around mains electricity.

The emerald terminal can be mounted on a variety of standard electrical back boxes:

- UK single back box
- US single gang electrical junction box
- UK double back box mounted vertically
- 75mm (3”) VESA mount

2.1 Preparing for mounting

Care must be taken with the internal components when disassembling the terminal.

2.1.1 Recommended tools

- 3 mm (0.1”) slot screwdriver for input/output connections and DC supply
- Wire cutters and strippers
- Security hex socket screwdriver

Product	CEM Product Code
Security screwdriver handle	HTO/000/001
Security screwdriver bit	HTO/000/000

Table 4: Security screwdriver product codes

2.1.2 Opening the terminal

Important

Take care not to strain the ribbon cable connecting the two halves of the terminal.

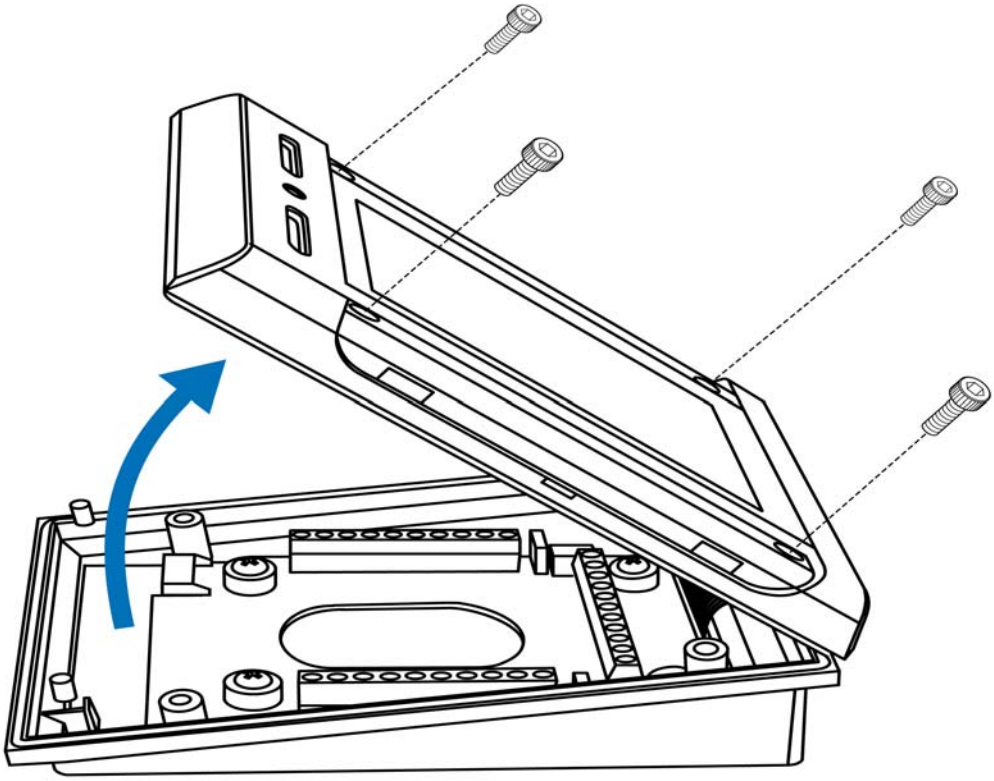


Figure 6 Opening the terminal

1. If the terminal is being retro-fitted after installation the side panels must be removed. To do this, position a 5 mm (0.2”) flat head screwdriver under the panel and slide it along the length to release it.

Note

A factory shipped terminal does not have the panels fitted.

2. Set the terminal on a stable, level surface to reduce the risk of the front of the terminal falling when it is disconnected.
3. Remove the four screws using a security hex screwdriver.
4. Carefully lift the top casing away from the back of the terminal, pivoting as shown.
5. Disconnect the ribbon cable from the I/O board before commencing wiring.

2.1.3 Mounting the terminal's back casing

Important

The emerald terminal must be fitted on the secure side of the door.

To access the full range of mounting screw positions of the terminal the Input/Output board must first be removed from the back box.

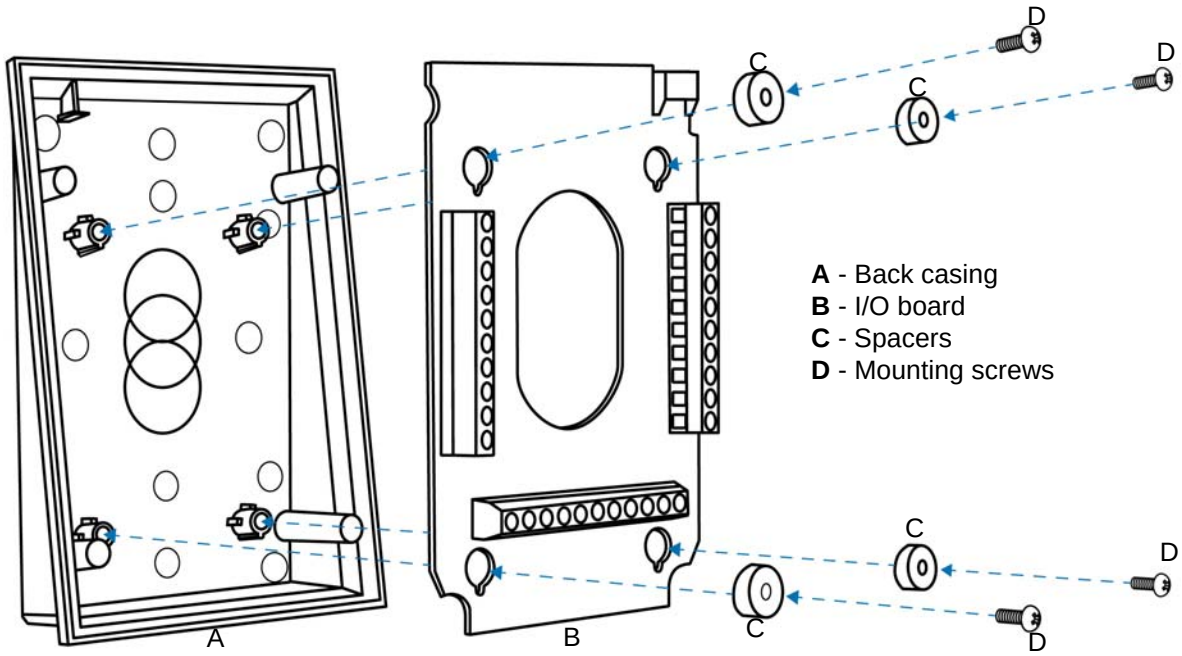


Figure 7 Exploded view illustration of the back casing and I/O board

1. Remove the four screws and spacers using a Phillips star head screwdriver.
2. Lift the I/O board away from the mountings.
3. Drill the back outer casing as required for cable access and back box mounting. (see Figure 8)

Note

To maintain the IP65 rating, waterproof glands must be fitted to the drilled holes.

4. Fit the back casing to the electrical junction box.
5. Re-attach the input/output PCB to the back casing ensuring to replace the spacers in the correct orientation.

Drilling the back casing

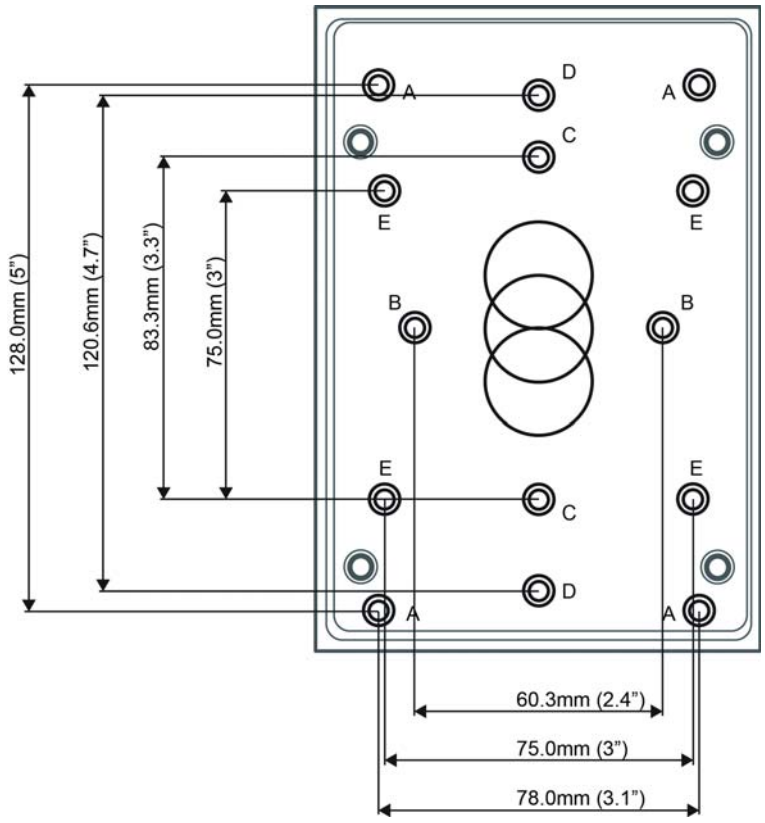


Figure 8 emerald™ back casing drill hole dimensions

Mounting hole	Description
A	Generic positions for wall mounting. These holes are accessible when the I/O board is in place.
B	UK single back box.
C	US Single back gang electrical junction box.
D	UK double back box mounted vertically.
E	75mm (3") VESA mount.

Table 5: emerald mounting descriptions

Chapter 3

Wiring the Terminal

3.1 Cabling requirements

Table 6 outlines recommended cabling requirements for each connector on the emerald.

Purpose	Recommended Cable	Connector	Max Length
External 12V supply	Belden 8760 18AWG two conductor cable or equivalent	14AWG Screw Terminal	30m (98.4')
Inputs	Belden 95XX or equivalent (XX = the number of pairs from 01 - 50)	14AWG Screw Terminal	3m (9.8')
Outputs	Belden 9462 or equivalent	14AWG Screw Terminal	Variable[a]
Wiegand	Belden 9514 (7 x 22AWG), Alpha 1229C(9 x 22AWG) or equivalent	14AWG Screw Terminal	30m (98.4')

Table 6: Terminal installation cabling requirements

a. As a guideline, a typical maglock from 650mA up to 1500mA @ 12V would use AWG18 cable, located no more than 7.6m (25') from the emerald™ terminal. Cables should not exceed 30m (98.4') in length.

Note

22AWG is the smallest acceptable cabling for a UL-294 installation, cable

3.1.1 Ethernet host

Ethernet communications should be cabled & terminated for 100Base-T operation according to IN ANSI/TIA/EIA-568-A / TIA/EIA-568-B. In order to comply with FCC requirements, a snap-on ferrite (Wurth Electronics 74272722 or equivalent) should be used around the Ethernet cable.

Type	Recommended Cable	Connector	Max Length
Host	CAT5/CAT5e/CAT6	RJ-45 Socket	100m (328')

Table 7: Ethernet host

Due to limited space, additional care should be taken when using CAT6 connectors or CAT5 connectors with a strain relief boot at the terminal. There should be enough spare cable left within the enclosure/back box to allow a service engineer to open the terminal case without straining the RJ45 connector. Where the cable is subject to movement or vibration, stranded Ethernet cable (and appropriate connectors) should be used.

3.2 The Main Board

The front PCB contains the main electronic components of the terminal; it is also where the Ethernet cable must be connected. **Any connections not labelled are not evaluated by UL and are not to be used in UL installations**.

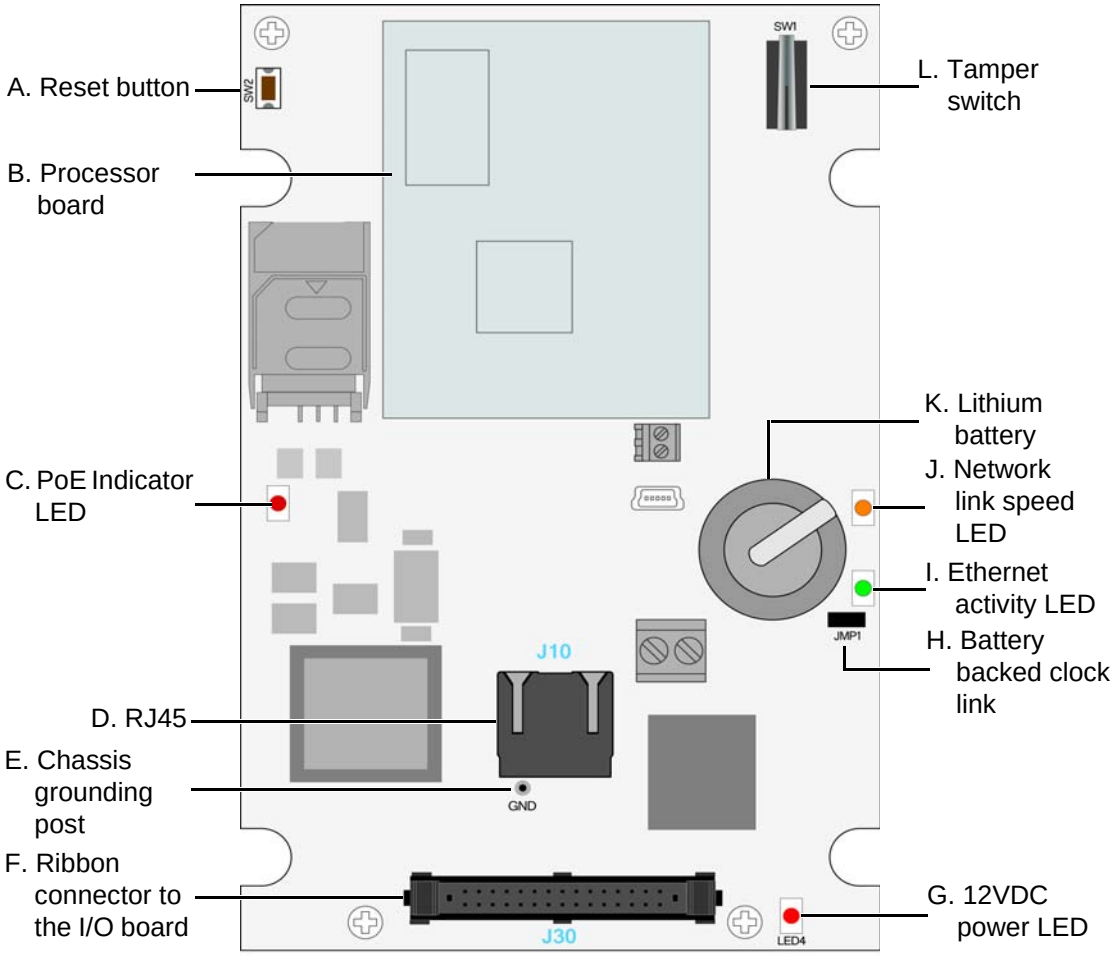


Figure 9 Illustration of the front board

Component	Description
A. Reset button	Used to hard reboot the terminal.
B. Processor board	The terminal processor board.
C. PoE Indicator LED	PoE has not been evaluated by UL.
D. RJ-45 connector	Used for ethernet communications and also for Power over Ethernet when being used.
E. Chassis grounding post	Chassis ground, to be tied to earth ground when testing the terminal.
F. Ribbon connector	Links the front PCB to the I/O PCB.
G. 12V power LED	Red indicates 12VDC power is being supplied to the board
H. Battery backed clock link	This link is fitted at the factory. If it is removed, the terminal will not store the current time & date; card transactions may fail due to a time/date mismatch.
I. Ethernet activity LED	Flashing green indicates ethernet activity
J. Network link LED	Orange indicates 100baseT connection speed. Unlit indicates 10baseT connection speed.
K. Lithium battery	Real time clock battery. The battery is not a serviceable part.
L. Tamper switch	Used to trigger an alarm when the case is opened.

Table 8: Description of front board components

3.3 The Input/Output Board

The input/output board provides connections points for terminal power, inputs, outputs, and third party Wiegand read heads.

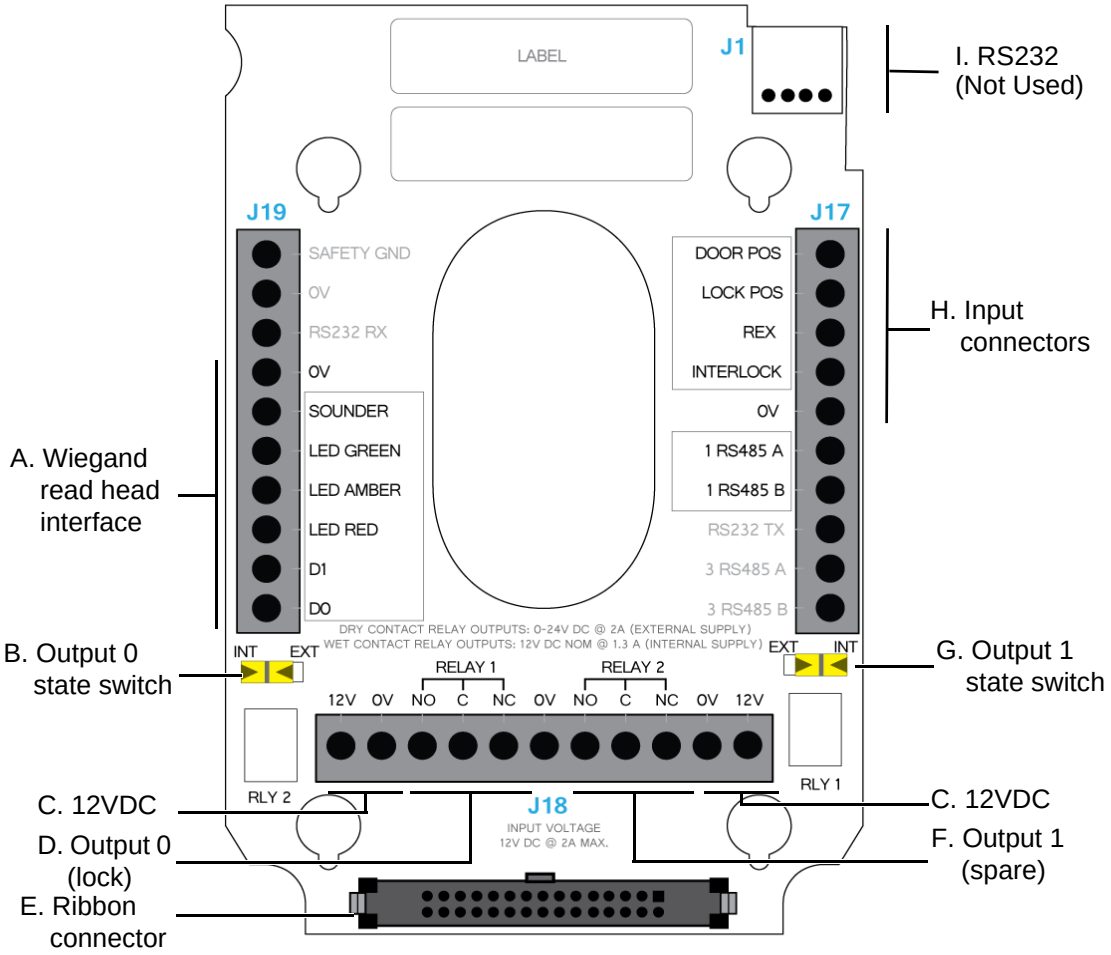


Figure 10 Illustration of the Input/Output board

Component	Description
A. Wiegand interface	Interface for third party exit read-heads using Wiegand protocol.
B. Output 0 state switch	Switches output 0 relay common ‘C’ between internal 12V or an external 12/24V UL294 or UL603 listed power supply.
C.12V and 0VDC	12V power from an appropriate UL294 or UL603 listed power source is supplied to the terminal. 12V can also be drawn from this circuitry to power attached door furniture.
D. Output 0	Lock output, either 12V provided by the terminal or 12/24V provided externally via the relay and a UL294 or UL603 listed power supply.
E. Ribbon connector	Links the I/O PCB to the front PCB.
F. Output 1	Spare output.
G. Output 1 state switch	Switches output 1 relay common ‘C’ between internal 12V or an external 12/24V UL294 or UL603 listed power supply.
H. Input connectors	Connection points for monitored inputs.
I. RS232	J1 has no functional impact/use on this product version and is not supported for use on UL installations.

Table 9: Description of I/O board components

Important

RS232 and RS485 connections have not been evaluated by UL and are not for connection in UL Installations.

3.4 Wiring locks

The terminal supports lock types rated 12-24V at 1.5A max current if using an external power supply. It is recommended that the lock is powered by an external power supply as this provides the most flexibility. However if required, internal power to a lock can be provided at 12V, 1.3A max current combined across both relays.

Important

The output state switch must be configured for the correct type of supply, as described in this section.

3.4.1 Wiring a voltage provided lock (internal power)

Only 12V locks can be wired to be powered internally by the terminal. When internal power is utilised it is possible to connect locks in a fail safe or fail secure configuration.

Note

The maximum current that can be supplied is 1.5A using an external power supply or 1.3A from the internal supply.

Fail safe lock

The fail safe configuration means that in the event of a power loss to the terminal the lock will open allowing free access. A lock that is constantly powered such as a maglock must be used.

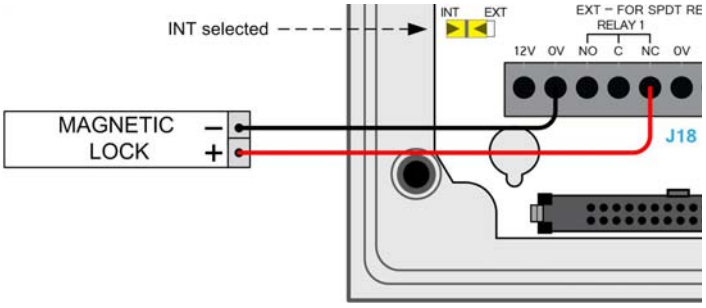


Figure 11 Illustration of wiring for a fail safe lock

Fail secure lock

The fail secure configuration means that in the event of a power loss to the terminal the lock will remain secure. A lock that requires power to open such as a shear lock must be used.

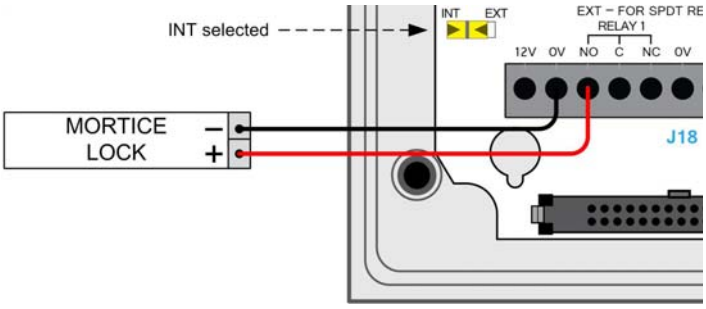


Figure 12 Illustration of wiring for a fail secure lock

3.4.2 Wiring a voltage not provided lock (external power)

The emerald relays can be used to control a lock using a 12-24V DC, UL294 or UL603 listed power supply.

Important

When using 24V power for a lock, it is imperative that the switch position is set to **EXT**. Setting the switch to **INT** will result in 24V being supplied to the terminal which may cause irreversible damage.

This is the recommended wiring configuration when locks require 24V.

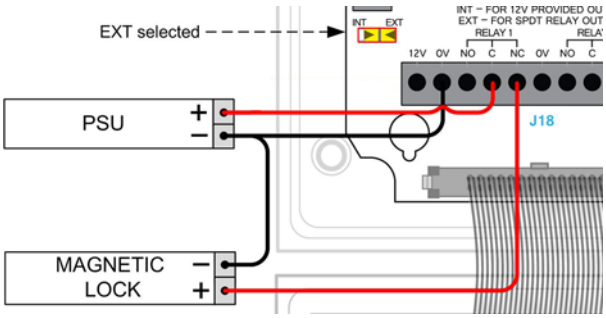


Figure 13 Illustration of wiring for lock with external power provided

3.4.3 Output power switch

Each of the two outputs has a switch that allows power to be provided to the output from the terminal's internal power circuit or by an external power source.

External power

When the switch is set to **EXT** a separate 12 - 24V DC, UL294 or UL603 listed power supply must be used to provide power for any locks or other door furniture attached to the output.

Internal power

When the switch is set to **INT**, the lock or other load is powered by the terminal's internal supply. In this case the total load must not exceed 1.3A @ 12V.

Important

The terminal's 12V connectors all link to the same circuit, powering the terminal and any outputs set to **INT**. It is imperative that before attaching 24V to power an output checks should be made that the relevant output switch is set to **EXT**. Applying 24V to an output with the switch set to **INT** will result in 24V being supplied to the common power circuitry, potentially damaging the terminal.

3.4.4 Supported third party read heads

UL approved emerald installations must only use listed read heads.

Read head	Manufacturer product code
HID iClass SE R10 Smart Card Reader	6100/6108
HID iClass SE R30 Smart Card Reader	6110/6118

Table 10: Supported third party read heads

3.5 Terminal with Request to Exit Switch

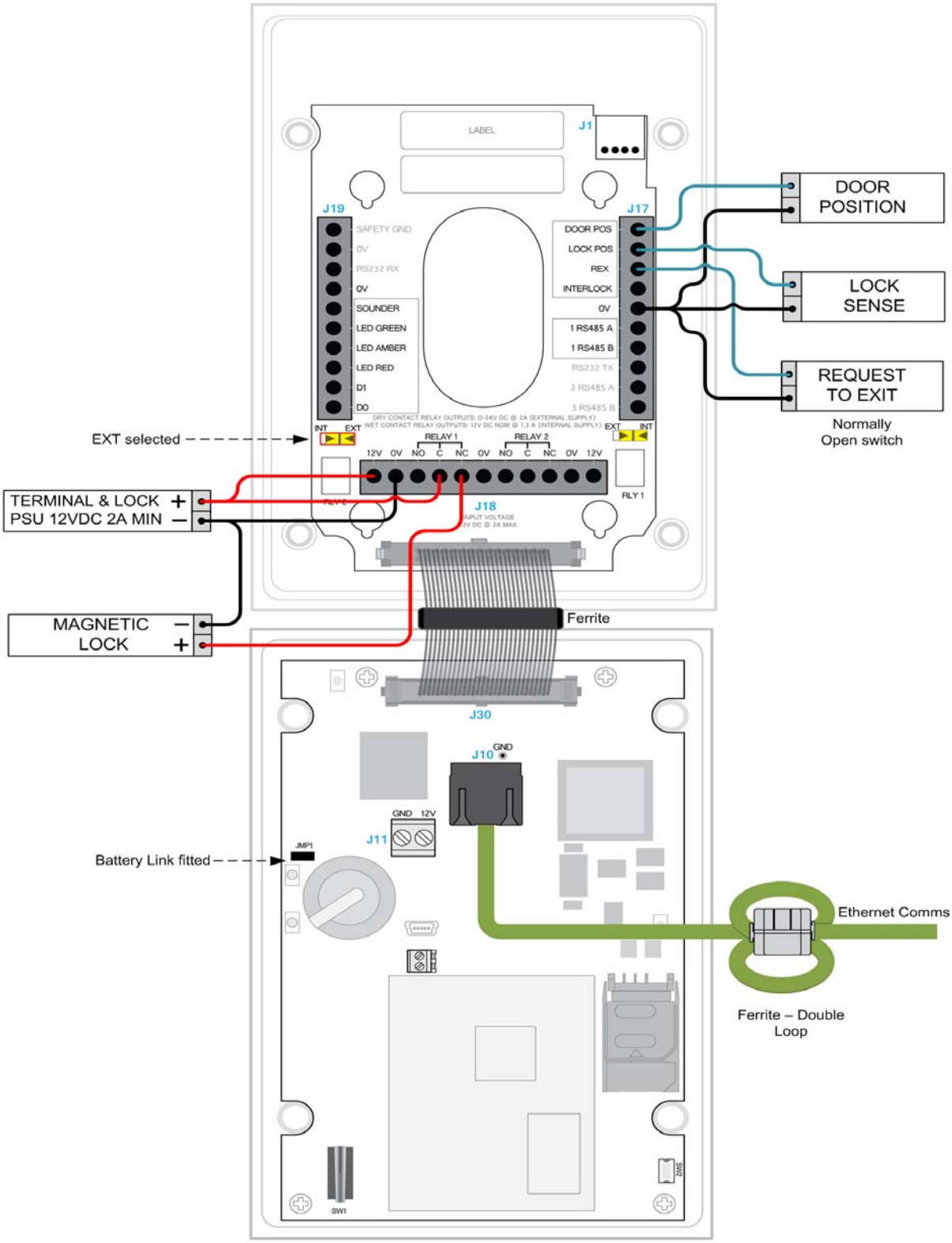


Figure 14 emerald master terminal with REX wiring diagram

Note

Terminals J1 and J11 have no functional impact/use on this product version and are not supported for use on UL installations.

3.6 Configuration information

Wiring an emerald terminal with a Request to Exit switch is the most basic wiring configuration. It is not recommended for high security installations as the emerald is installed on the unsecure side of the door.

Power connections

The 12V power connections on J18 connect to the same common circuitry and are used to provide power to the emerald terminal, as well as to output power to door furniture.

Input configuration

The table below illustrates the configuration and operation of the inputs on the terminal when configured with a Request to Exit switch.

Input number	Input function	Default input trigger state change
0	Door position	short => open
1	Lock position	short => open
2	Request to exit	switch open => momentary short => open
3	Spare/Interlock	short => open

Table 11: emerald and request to exit switch input configuration

Note

Inputs are not for use as part of a burglar alarm system.

Inputs not in use

The door position input 0 must be shorted out between the IP0 and GND pins with wire when not in use, to prevent alarms being generated on the system.

Ethernet cable ferrite

The ferrite must be attached to the Ethernet cable close to the exit point from the emerald terminal. The cable should be looped through the ferrite once.

3.7 Terminal with Third Party Wiegand Read Head

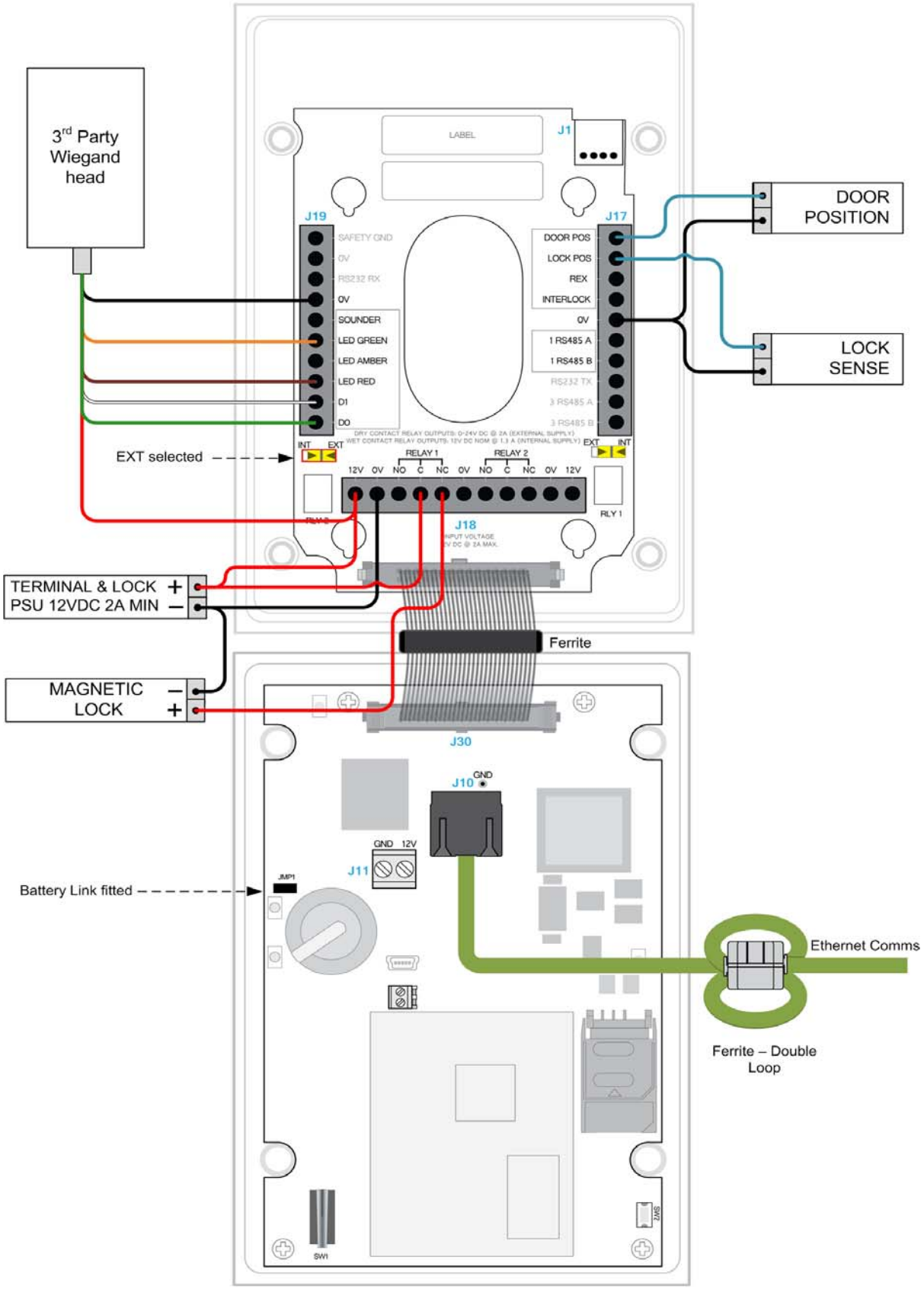


Figure 15 emerald master terminal with Wiegand read head wiring

3.8 Configuration information

The emerald terminal facilitates the use of a third party exit Wiegand head with three LEDs.

Power connections

The 12V power connections on J18 connect to the same common circuitry and are used to provide power to the emerald terminal, as well as to output power to door furniture.

Typical Wiegand read head wiring

For specific read head wiring consult the third party manufacturer's documentation.

I/O board connection	Typical HID colour
0V	Black
Sounder	**Not Supported**
LED Green	Orange
LED Amber	Not fitted
LED Red	Brown
D1	White
D0	Green
Head 12V	Red

Table 12: Typical Wiegand head wiring

Important

For proper regulatory compliance, the drain wire should be disconnected at the power supplied end of the cable.

Input configuration

The table below illustrates the configuration and operation of the terminal inputs when configured with a third party Wiegand read head.

Input number	Input function	Default input trigger state change
0	Door position	short => open
1	Lock position	short => open
2	Request to exit	switch open => momentary short => open
3	Spare / Interlock	short => open

Table 13: emerald and third party read head input configuration

Note

Inputs are not for use as part of a burglar alarm system.

Inputs not in use

The door position input 0 must be shorted out between the IP0 and GND pins with wire when not in use, to prevent alarms being generated on the system.

Ethernet cable ferrite

The ferrite must be attached to the Ethernet cable close to the exit point from the emerald terminal. The cable should be looped through the ferrite once.

3.9 Tamper Detection on Terminal Inputs

Terminal inputs can be monitored for four state tampering: open, close, tamper short and tamper cut. If an input is tampered with, an alarm will be triggered in the AC2000 software. The alarm is a universal tamper alarm and does not distinguish between the four different states. In order to monitor inputs for tamper short and tamper cut, a resistor network must be installed on the input sensor wiring as show in Figure 16 B), and the AC2000 software configured to monitor the input.

3.9.1 Wiring the resistor network

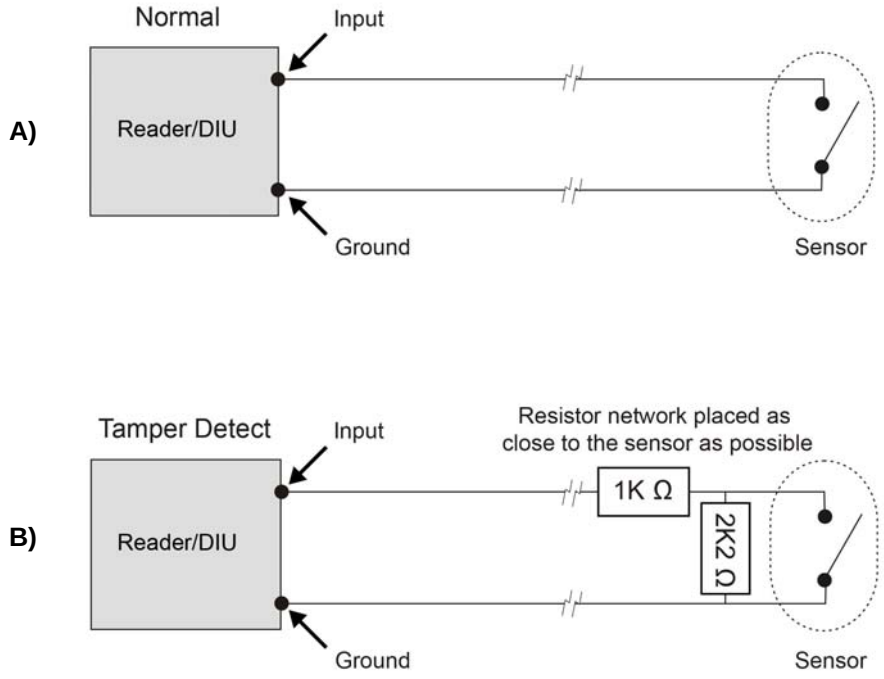


Figure 16 Illustration of the resistor network for four state tamper detection on inputs

Important

It is imperative that the tamper resistor network is wired as close to the sensor as possible.

3.9.2 Re-assembling the terminal

1. Ensure that there is adequate cable length available to reach the connectors comfortably for each of the following:

   – 12VDC

   – Cat5e/6 cable for communications

   – Output wiring for lock

   – Wiring for inputs e.g. door position sensor, lock sense

Important

To maintain the terminal's IP65 rating, the cable access hole should be adequately sealed before completing the installation process.

2. Attach the front panel of the terminal via the ribbon connector.

3. Attach the front of the terminal to the back casing and fix in places with the screws.
4. Attach the side panels to the terminal.

Note

If the terminal needs to be open after installation, the side panels can be removed by inserting a 5 mm (0.2”) flat head screwdriver into the slot under the centre of the panel and sliding along the length of the panel.

Chapter 4

Terminal Network Configuration

The network settings are accessed via the installer configuration menu on the terminal.

4.1 Checking emerald's Network Status

1. Tap the **Reader Address** icon. The **network status indicator** is displayed on screen for eight seconds.

Figure 17 Checking the network status

Each section of the status indicator represents a different aspect of the network connectivity. The presence or absence of a block indicates whether or not the connection is good.

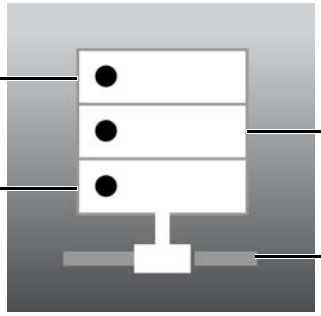


Figure 18 The network status indicator

4.2 Accessing the System Configuration Menu

1. Slowly swipe a finger across the date/time from left to right.
2. When prompted to enter passcode type 67679999.

Figure 19 Accessing the configuration menu

Note

Once the terminal has received a configuration from the server this passcode will be changed to 67670000. The final four digits of this PIN are configurable using the AC2000 software.

4.2.1 Setting the terminal IP address, gateway and subnet mask

1. From the **Config Menu** press **Device settings | Network**.

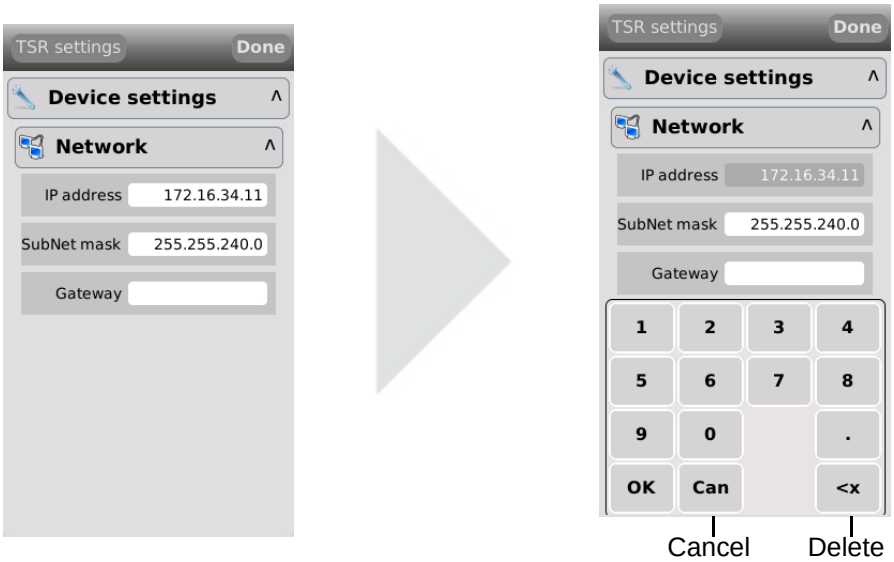


Figure 20 Configuring the terminal network settings

2. Press the **IP address** field, type the address and press **OK**.
3. Press the **SubNet mask** field, type the address and press **OK**.
4. Press the **Gateway** field, type the address and press **OK**.
5. Press **Done** to close the **Network** menu.

4.2.2 Network routing - (advanced users)

The emerald terminal needs to be able to communicate with the Central Database Computer (CDC) and the Real Time Computer (RTC). If a network is fragmented, and the terminal, CDC and RTC are on different parts of the network it may be necessary to route communications to the RTC. In this situation contact the site network administrator.

Figure 21 The routing menu

1. From the **Configuration Menu** press **Device Settings | Routing**.
2. Press the **Network** field, type the network IP address and touch **OK**.
3. Press the **SubNet mask** field, type the address and touch **OK**.
4. Press the **Gateway** field, type the address and press **OK**.
5. Touch **Done** to close the menu.

4.2.3 Testing the connection with the AC2000 server

The terminal can be used to test the connectivity with the AC2000 server via a PING utility.

1. From the **Configuration Menu** press **Tests | Network tests**
2. Press the **Ping address** field below **Ping any**.

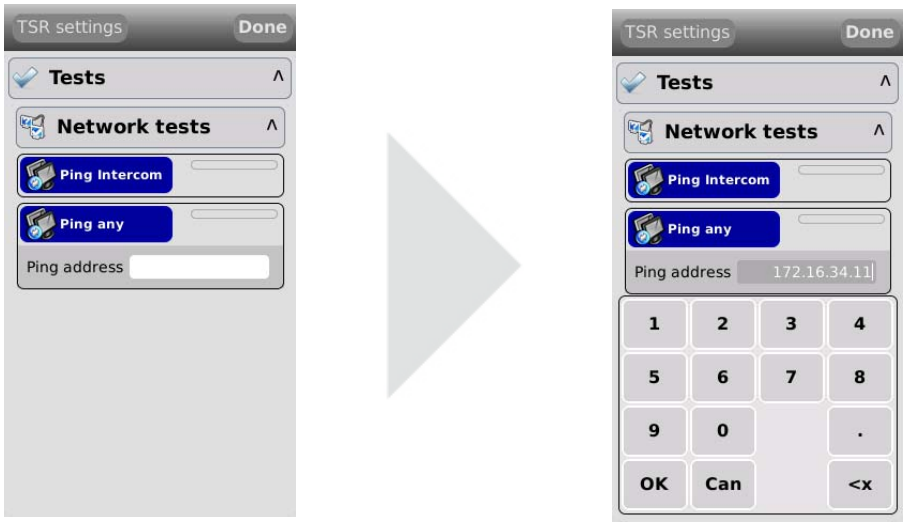


Figure 22 Testing the connection with the AC2000 server

3. Type the IP address of the AC2000 server (CDC/RTC) and press **OK**.
4. Press **Ping any**.
   i. If a response is received from the pinged address the **Ping any** button will turn green.
   ii. If no response is received from the address the **Ping any** button will turn red.
5. The PING utility can be used to check connectivity to any device on the network.

This page is intentionally blank.

Chapter 5

Using the Terminal

emerald is always in one of three modes: Door mode, Free access mode or Locked down mode. Each mode defines the terminal's function and behaviour at the door.

You can see which mode the terminal is in by the Home screen display.

Door mode

Free access mode

Locked down mode

Door mode
The door enables access to all valid cardholders after their card is swiped.

Free access mode
In Free access mode, no card swipe is necessary as the door is unlocked.

Locked down mode
In Locked down mode the door is locked and no access is allowed.

5.1 Presenting your card

To open a door pass your access card approximately three centimetres in front of the terminal. The emerald terminal's LED status indicator changes colour and the appropriate response screen is displayed.

The response screens are described in Table 3 below.

Screen	Message	Description
	Access granted LED: Green	Access is granted
	Not in System LED: Red	Access is not granted as card is not registered on the system

Table 14: Response screens

Screen	Message	Description
	Expiring Card LED: Flashes green	Access is granted. The flashing green LED indicates that your card will expire in less than 14 days.
	Expired Card LED: Red	Access is not granted as your card has expired
	Lost / Stolen Card LED: Flashing red	Access is not granted as your card has been reported as lost or stolen
	Wrong Time LED: Red	Access is not granted as you are attempting to gain access outside the permitted time for your card
	Wrong Door LED: Amber	Access is not granted as you do not have permission to enter this door

Table 14: Response screens

This page is intentionally blank.

Chapter 6

Diagnostics and Testing

emerald utilises an intuitive Graphical User Interface to access diagnostic and testing functionality.

6.1 Navigating the Menus

Sub-menus on the emerald terminal are accessed by touching the menu option to expand.

- Menus are expanded and closed by pressing the menu name or the arrow.

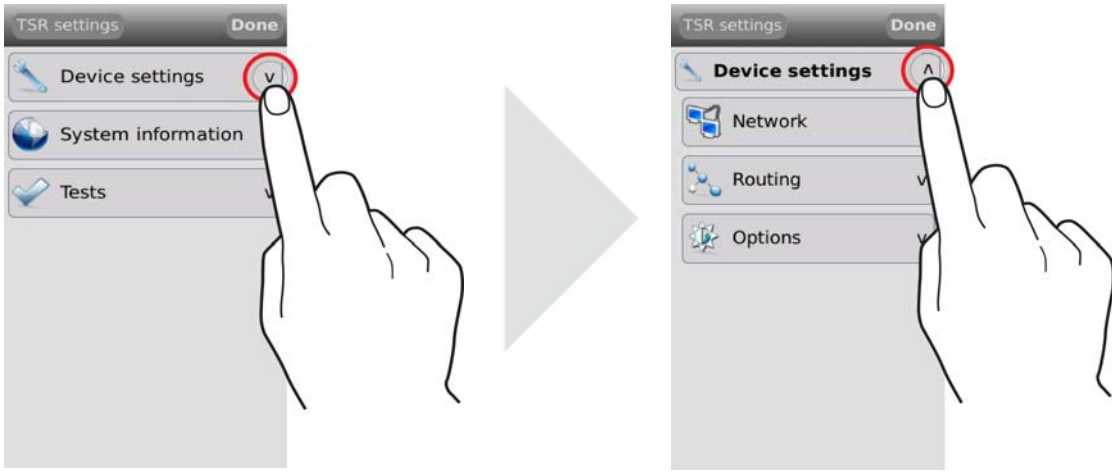


Figure 23 Expanding and closing terminal menus

6.2 Accessing the System Configuration Menu

The diagnostic and testing functionality is accessed via the configuration menu.

1. Slowly swipe a finger across the date/time from left to right.
2. When prompted to enter passcode type 6767000.

Note

See Accessing the System Configuration Menu on page 24 for more details on passcodes..

Figure 24 Accessing the configuration menu

The system configuration menu has three sub-menus, each of which contains specific terminal maintenance functions. The **System information** and **Tests** menus are used for the purposes of testing and fault finding.

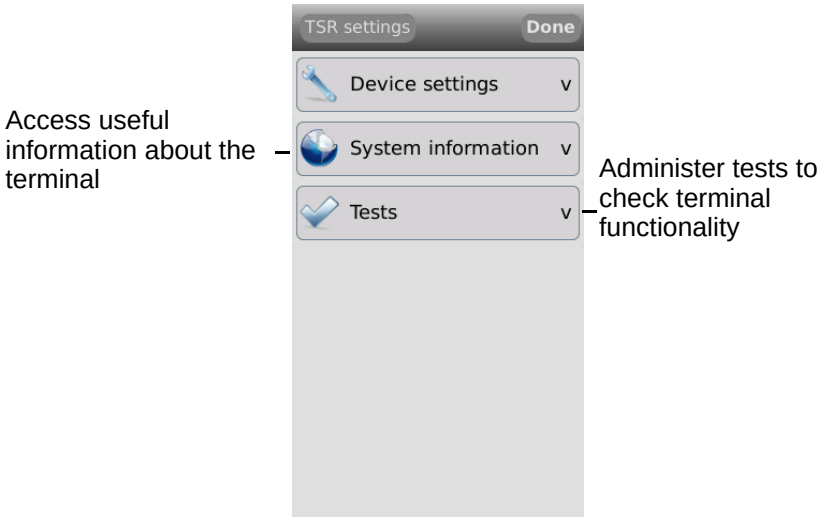


Figure 25 The system configuration menu

6.2.1 System Information menu

This menu provides access to five sub-menus which display useful device data about the network, firmware, database, configuration and unit information.

Important

When contacting CEM support with any issues, this information may be asked for.

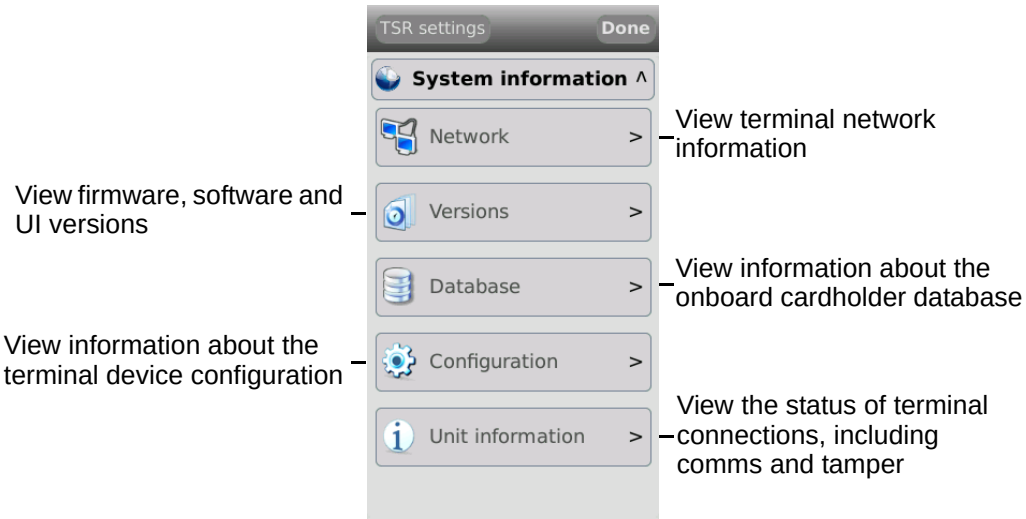


Figure 26 The System information menu

Network

The **Network** information section details all of the terminal network settings.

Info	Description
CEM address	The CEM reader address of the terminal.
IP address	The IP address of the terminal.
Subnet mask	The subnet mask of the network hosting the terminal.
Default gateway	The IP address of the gateway server.
MAC address	The MAC address of the terminal.
RTC address	The IP address of the RTC controlling the terminal.
VOIP server	The IP address of the VOIP server for intercom functionality.
VOIP help station	Intercom station number. This number is used to allow an intercom workstation to communicate with the terminal.

Table 15: Terminal network information descriptions

Versions

The **Versions** information section details all hardware and software versions of the terminal.

Info	Description
TSR Version	Firmware version
UI Version	User interface version
S/W Date	Date of last firmware update
S/W Time	Time of last firmware update on the S/W Date
H/W Version	Version of the terminal hardware
H/W s/n	Serial number of the terminal
Linux	Linux kernel version, including date and time.
Qt	Version of Qt library used by the UI.

Table 16: Terminal versions information descriptions

Database

The **Database** information section details the information about the onboard card database.

Info	Description
CEM address	The CEM reader address of the terminal.
Coldstart count	Record of the number of times the terminal has been coldstarted.
Last coldstarted	Date and time of the terminal's last coldstart.
Card count	Number of active cards held on the terminal.
Last updated	Date and time of the last database update from the server.
Trans all count	Displays the number of buffered transactions and alarm events (in offline mode). This is cleared when the terminal next goes online.
Trans card count	Displays the number of buffered transactions only (in offline mode). This is cleared when the terminal next goes online.
Last configured	Displays the date and time that the terminal last received configuration data from the server.

Table 17: Terminal database information descriptions

Configuration

The **Configuration** menu provides information about terminal door modes. The additional door modes are not evaluated by UL.

Unit information

The **Unit information** section provides information regarding the status of the terminal.

Info	Description
Tamper sensor	Describes the status of the internal tamper switch.
Run time	Information about the running time and load of the terminal.
Main comms	Indicates the status of the main comms.
Database engine	Indicates the status of the database engine.

Table 18: Terminal unit information descriptions

Info	Description
Local inputs	Indicates the status of the local inputs such as door position, lock sense etc.
Main reader	Indicates the status of the emerald™ master terminal.
Door interface	Indicates whether a door interface unit is currently connected to the emerald™ terminal. The emerald™ is not UL evaluated with a Door Interface Unit.
2nd reader	Indicates whether an exit reader is currently connected to the terminal.

Table 18: Terminal unit information descriptions

6.2.2 Tests menu

The emerald terminal has built in tests that can be performed to check specific functionality.

Important

When contacting CEM support with any issues, these tests may be requested.

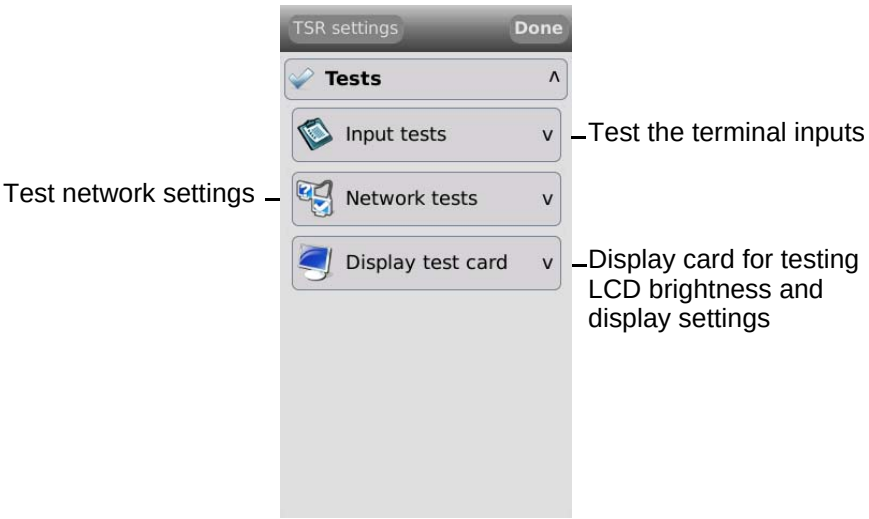
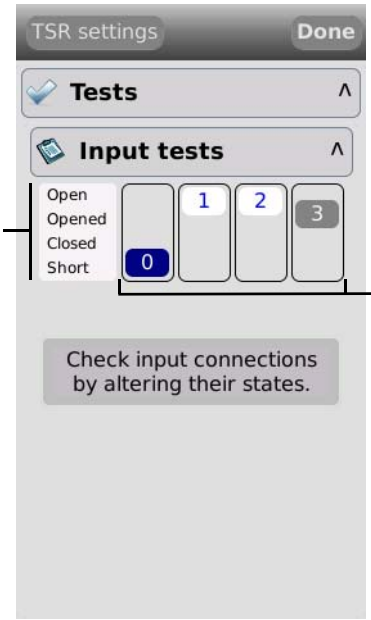


Figure 27 The tests menu

Input tests

The default **Input tests** screen displays the status of each of the four inputs.



Input state. To test the inputs, change the state of the input e.g. open and close the door to test if the terminal is registering the state change.

Inputs. Each number correlates with a terminal input number as detailed in chapter 3. e.g input 0 is door position.

The vertical position of each highlighted number indicates the input state as defined on the left of the screen.

Figure 28 The input tests screen

Two state input test

When an input has been wired in a 2 state open and closed configuration only the **Open** and **Short** tests can be administered.

Open - The input is opened.

Short - The input is closed.

Four state input test

When an input has been wired in a 4 state configuration as described in section 3.9.1 on page 21, all four input state tests can be administered.

Open - Indicates a tamper cut fault condition.

Opened - The input is open.

Closed - The input is closed.

Short - Indicates a tamper short fault condition.

Network tests

The **Network tests** screen provides PING tests to check connectivity with the intercom server and with any other provided IP address.

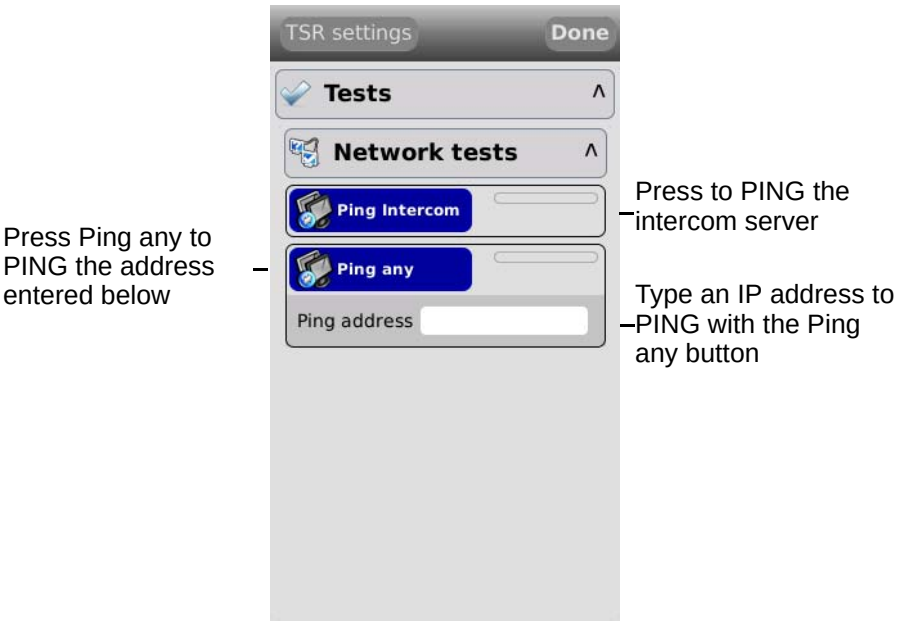


Figure 29 Terminal network tests

There are two possible responses for the ping utilities:

Red:	No response received
Green:	Response received

6.3 Maintenance

There are no required maintenance guidelines.

CEM Systems
195 Airport Road West
Belfast
BT3 9ED
United Kingdom
Tel: +44(0)2890 456767