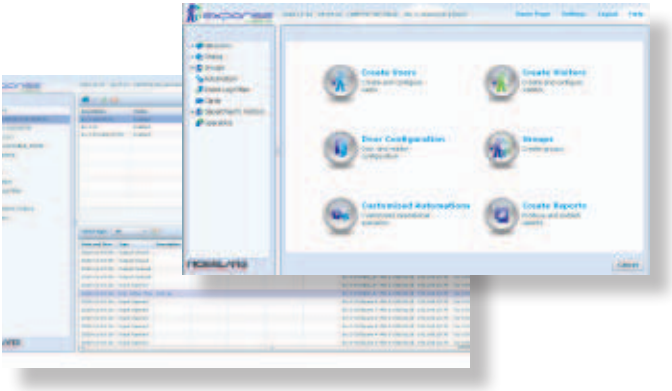
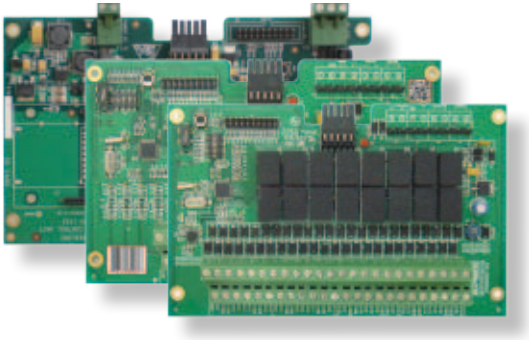
ExpansE

Distributed Access Control System

Installation
& User Manual

June 2011





ROSSLARE
SECURITY PRODUCTS

Table of Contents

1. Introduction

The ExpansE access control system is a state-of-the-art networked access control system with a web based management and control application.

The ExpansE system consists of the following components:

- EXP-1032 – ExpansE Networked Controller with onboard web based application
- EXP-2024 – Dual Reader Door unit
- EXP-2016 – 16 relay Elevator Control unit
- EXP-2088 – 8-Inputs/Outputs Interface Unit

1.1 System Overview

The ExpansE system's control panel does not include any on-board terminals, but instead holds a powerful processing unit as well as high-capacity network communication capabilities, which allows TCP/IP network communication via its on-board TCP/IP interface.

The system components provide all of the necessary door connections such as reader ports, lock outputs and signaling inputs, as well additional inputs and outputs for various access control applications.

Due to the component structure of the system, the various components may be installed in many variations and topologies according to the specific needs of the installation site.

The platform, since not dedicated and limited to enclosed number of doors, can be used for further processing and applications such as security, automation and others.

Targeted for the medium to large installations, this topology brings forth a solution benefiting from:

- Significantly higher capacities.
- Flexible installation.

  Pure processing central units, not limited by physical limitations, such as a maximum number of onboard readers, make it highly flexible for various applications, both

for the initial layout and for future additions, such as door interfaces with various formats, IO interfaces and smart management, security management, elevator control, native support for video interfaces etc.
This type of layout also supports easy future upgrading as only firmware upgrades are required.

- The EXPANSE IP also includes on-board support for communications across a TCP/IP network.

1.2 Features

The ExpansE is a powerful and adaptable access control solution with a wide range of features.

- Up to 2,048 Main Units connected via Ethernet
- Each Main Unit can have up to 32 End Units and up to 32 doors (IN/OUT) or 64 readers.
- Each Main Unit can have up to 256 inputs and 512 outputs
- Panel configuration DIP switch
- 128,000 users per Main Unit
- 100,000 history event log per Main Unit
- 512 multi segmented Time Zones and 128 Holidays dates
- RS-232 and RS-485 serial communication
- Ethernet and USB communication ports

1.3 ExpansE Web Application

The ExpansE system utilizes an embedded web based management and supervision application which controls up to 2048 Main Units, (EXP-1032 ExpansE Networked Controller) referred to as MUs, by creating a Master / Slave configuration of all available MUs within the network, each with their associated secondary units, referred to as End Units (EUs).

Configurable Links

The system's configurable links model makes it possible to trigger any chosen output such as triggering an alarm siren, based on a signal from a selected input. This allows easy

integration with other systems such as intruder alarms and CCTV systems.

ExpansE can also define a selected set of operations (defined in configurable links) when a panel registers a specified user or group of users.

1.4 ExClouds Reports Production Software

The ExClouds is a custom designed reports production software that manages all the reports available in the system. See chapter 11, Reports Wizard, on page 135.

In addition the ExClouds has extensive backup abilities. See chapter 10, ExClouds PC Set-Up, on page 128.

ExClouds Structure

ExClouds PC software operates through a dedicated computer, which communicates with the ExpansE MU.

2. Technical Specifications

2.1 EXP-1032 Networked Controller

Electrical Characteristics

Operating Voltage	12-16VDC 1.5A from external DC input connector
Maximum Input Current	Standby: 150mA @ 12V Maximum: 1200mA @ 12V (Not including attached devices)
Visual Indicators	Power LED TCP/IP Speed LED TCP/IP Link LED TCP/IP Duplex LED
Real-time Clock Battery	CR1225 3V Lithium Battery

Communication Characteristics

RS-485	Full-duplex data communication
USB	One USB host
Ethernet	One RJ-45 Ethernet connector
Tamper	Two inputs

2.2 EXP-2024 Dual Reader Door Unit

Electrical Characteristics

Operating Voltage	12-16VDC @ 1.0A
Maximum Input Current	Standby: 150mA @ 12V Maximum: 1000mA @ 12V
General Inputs	4 Supervised high impedance inputs and 1 tamper input Maximum voltage: 5VDC
Relay Outputs	4 Relay outputs 5A Relay (N.O. or N.C.)
Reader Ports	2 Reader ports Output voltage: 12VDC Max. output current: 300mA LED control output D0/D1, tamper input

Communication Characteristics	
Tamper switches	Front and Back
Visual Indicators	Power LED
Audio	Sounder Output (with BL-D40)
Communication	RS-485
Baud Rate	115200 bps
Unit configuration	8 DIP Switches RS-485 serial address (1-32) Tamper options

2.3 EXP-2016 16 Relay Elevator Control Unit

Electrical Characteristics	
Operating Voltage	12-16VDC @ 1.0A
Maximum Input Current	Standby: 100mA @ 12V Maximum: 800mA @ 12V
General Inputs	1 Tamper input Maximum voltage: 5VDC
Relay Outputs	16 Relay outputs. 5A Relay (N.O. or N.C.)

Communication Characteristics	
Tamper switches	Front and Back
Visual Indicators	Power LED
Communication	RS-485
Baud Rate	115200 bps
Unit configuration	8 DIP Switches RS-485 serial address (1-32) Tamper options

2.4 EXP-2088 – 8-Inputs/Outputs Interface

Electrical Characteristics	
Operating Voltage	12-16VDC @ 0.5A
Maximum Input Current	Standby: 100mA @ 12V Maximum: 500mA @ 12V

Electrical Characteristics	
General Inputs	8 Supervised high impedance inputs and1 tamper input Maximum voltage: 5VDC
Relay Outputs	8 Relay outputs 5A Relay (N.O. or N.C.)

Communication Characteristics	
Tamper switches	Front and Back
Visual Indicators	Power LED
Communication	RS-485
Baud Rate	115200 bps
Unit configuration	8 DIP Switches RS-485 serial address (1-32) Tamper options

2.5 System Environmental Characteristics

- **Operating Temp. Range:** 32°F - 120°F (0°C - 49°C)
- **Operating Humidity:** 0 - 90% (Non-condensing)

3. ExpansE Architecture

This chapter comes to explain the difference between the various access control topologies with an emphasis on the benefits of the ExpansE topology as well as detailed explanation on the various ExpansE components and enclosures

3.1 Central versus Distributed Topology

Central access control systems typically duplicate the hardware many times in order to cover large applications, and are often expensive, since they involve complicated and costly installation, configuration, networking, and cabling. Furthermore, since multiple controllers must be synchronized, it limits their performance and system capacity.

In a distributed system, the main networked controller unit (EXP-1032) is physically separated from the secondary units that manage the various door elements (such as readers, locks, REX buttons, switches and other I/Os) — substantially reducing cabling work and simplifying the installation process.

Distributed architecture allows systems to expand from a single door to thousands of doors in multiple sites, without unnecessary redundancy, and offers easy integration with external systems such as DVRs, Alarms, and more .

See Figure 1, below for an explanatory comparison between Rosslare's AC-225 networked access control system as a central architecture and that of Rosslare's new ExpansE distributed architecture.

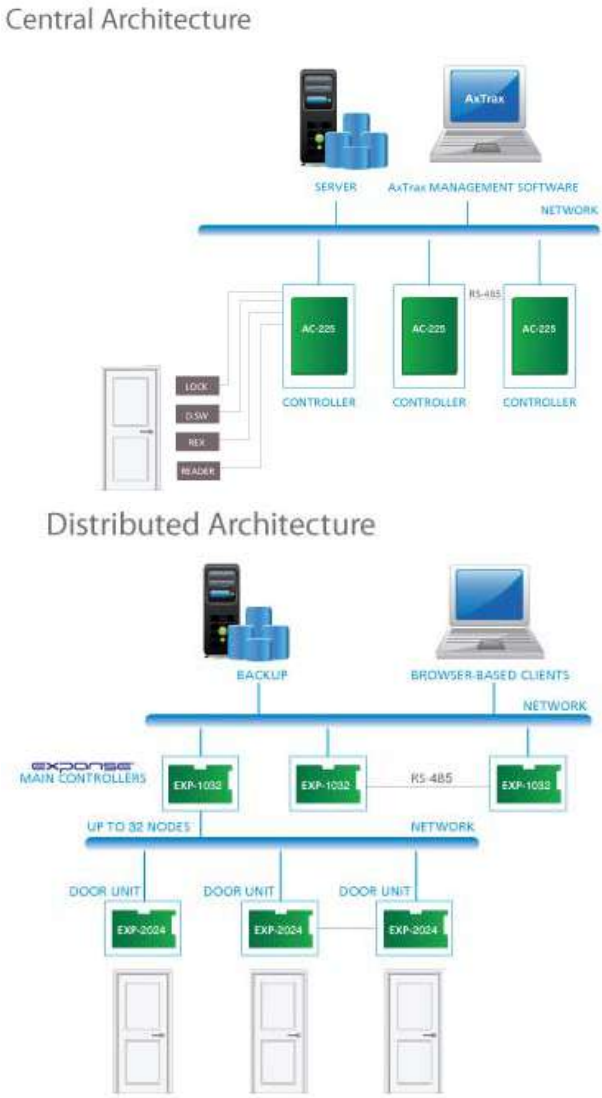


Figure 1: Central versus Distributed Architectures

3.2 ExpansE Distributed Access Control

The ExpansE system supports up to 2,048 Networked controllers (MUs), one designated as the master and the rest as slaves

connected over an Ethernet network, each of these MUs are then connected to various EUs via RS-485 connection.

The ExpansE system offers various EUs including dual reader door unit, an 8- I/O interface, dedicated 16 relay elevator control unit and many more.

Based on distributed architecture, each one of the ExpansE's EUs (e.g., a door or I/O) is physically separated from the MU, which controls up to 32 EUs. Each of the MUs can manage up to 256 inputs, 512 outputs or 32 doors. The panels are controlled by a web based application embedded into the controller and also has an optional server based software.

The ExpansE system also offers several mounting options to best respond to each specific need, be it a small singular box for individual units, a specially designed box which includes an integrated power supply and backup battery, or a rack mount which can hold several MUs , EUs or a combination of both. Figure 2 below, shows an example set-up for a distributed network of the ExpansE access control system.

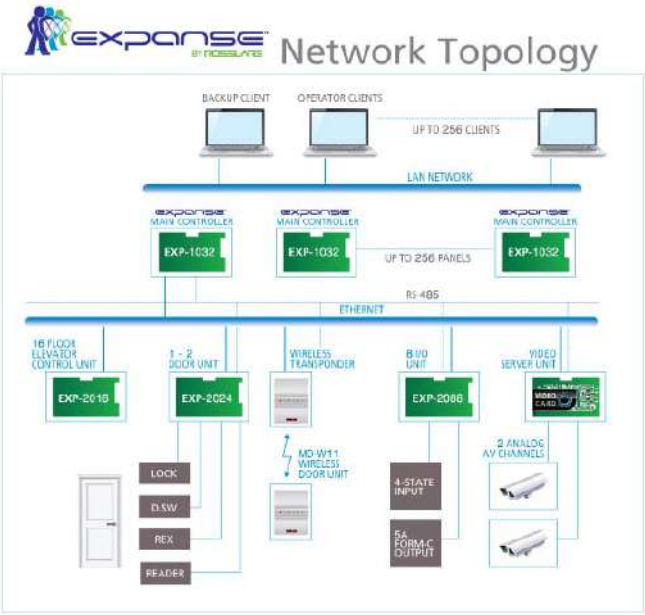


Figure 2: Sample of EXPANSE Configuration

3.3 ExpansE Mounting Options

The ExpansE units come in various mounting options be it as a MU or EU board, or a board mounted in one of several box types as described below.

ME-01 Single Board Self Powered Metal Enclosure

This sturdy, lockable, metal case has room for a single board along with a power supply and backup battery, see Figure 3 below.

Figure 3: ME-01 Single Board Self Powered Metal Enclosure

ME-12 Single Board Self Powered Plastic Enclosure

The ME-12 plastic enclosure holds a single board along with a power supply and backup battery. The wiring ducts and holders secure both the various components and the wiring within the enclosure. The enclosure's lockable door is designed to be easily removed when opened for better access during installation, yet cannot be removed when the door is closed in normal use. See Figure 4 below.

Figure 4: ME-12 Single Board Self Powered Plastic Enclosure

ME-14 Compact Single Board Self Powered Enclosure

The ME-14 is a simple plastic enclosure suited for a singular board. See Figure 5 below.

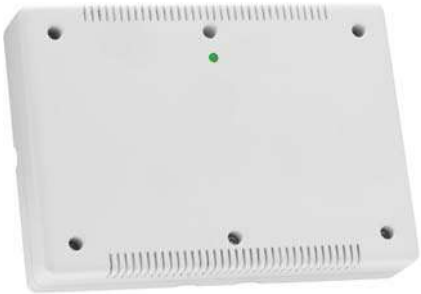


Figure 5: ME-14 Compact Single Board Self Powered Enclosure

ME-00 9 Boards Tray Cabinet Housing

The ME-00 offers a rack which can hold several MUs, EUs or a combination of both. The rack holds one 14 Ah backup battery as well as a power supply which powers all the connected units. See Figure 6 below.

Figure 6: ME-00 9 Boards Tray Cabinet Housing

3.4 ExpansE Hardware Units

The ExpansE system is comprised of several hardware units, the MU, EXP-1032 ExpansE Networked Controller, and several EUs such as the EXP-2024 Dual Reader Door Unit, EXP-2016 16 relay Elevator Control Unit, and the EXP-2088 – 8-Inputs/Outputs Interface.

EXP-1032 ExpansE Networked Controller

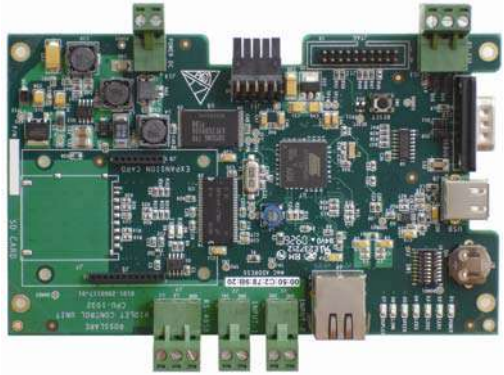


Figure 7: EXP-1032 ExpansE Networked Controller

- Supports 32 EUs, which can include up to 32 doors / 64 readers, up to 256 inputs and 512 outputs, as well as up to 128,000 users per controller
- 100,000 history event log size
- On-board Ethernet, RS-485 and USB (host) 2.0 ports

EXP-2024 Dual Reader Door Unit

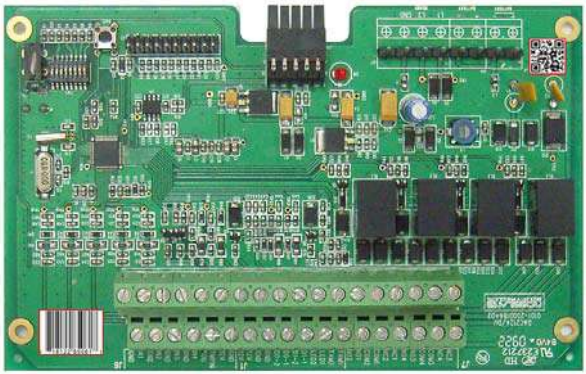


Figure 8: EXP-2024 Dual Reader Door Unit

- 2 reader ports - supports Wiegand 26 bits and other standard and non-standard formats
- 4 four-state inputs, 4 form-C relay outputs, and a sounder output
- RS-485 communication ports

EXP-2016 16 Relay Elevator Control Unit

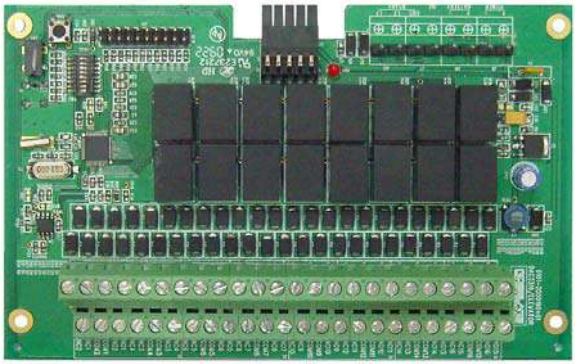


Figure 9: EXP-2016 16 Relay Elevator Control Unit

- 16 Form-C relay outputs, ideal for elevator control applications
- RS-485 communication ports

EXP-2088 – 8-Inputs/Outputs Interface Unit

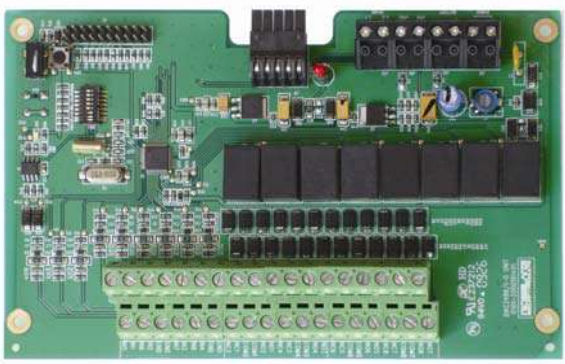


Figure 10: EXP-2088 – 8-Inputs/Outputs Interface Unit

- 8 four-state inputs and 8 form-C relay outputs
- RS-485 communication ports

3.5 Reports Production and Backup Software

The ExpansE system is complemented with the ExClouds software; see ExClouds PC Set-Up, on page 128 as well as the ExClouds Software manual.

3.6 Card Readers and Keypads

Each Door Unit can be connected to a maximum of two readers. There are four types of readers supported:

- Biometric Readers
- Card readers
- Keypads
- Dual keypad & card readers

A keypad is required for any reader mode that requires PIN code entries, such as "Card or PIN", "PIN Only" or "Card and PIN (Secured mode)".

4. Hardware Installation

Each MU needs to be wired and defined in the web based application along with its associated EUs separately.

4.1 Wiring Instructions

The wiring chapter is divided per units showing the various connections unique to each board, followed by general instructions applicable to several units.

EXP-1032 ExpansE Networked Controller

The EXP-1032 MU board and its components as well as general connections from the MU are shown in Figure 11, below.

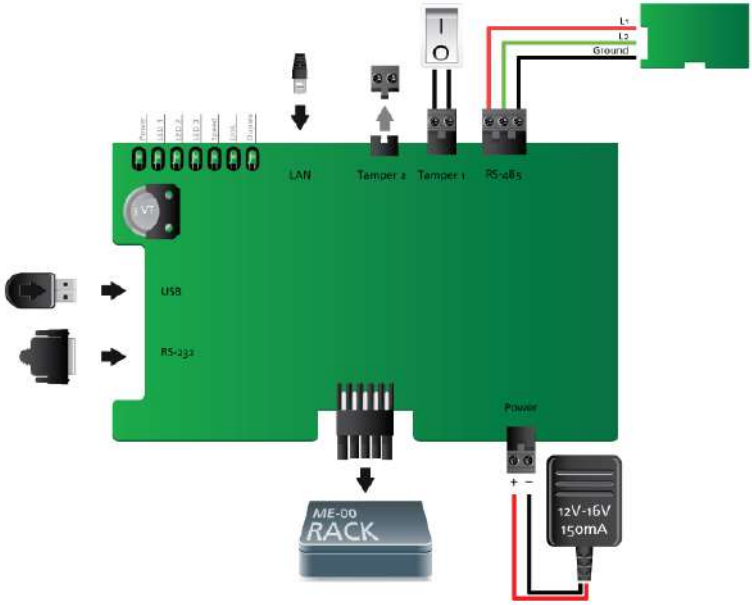


Figure 11: EXP-1032 ExpansE Networked Controller Wiring

To wire the EXP-1032 ExpansE networked controller:

1. Connect a 12-16VDC 1500mA transformer to the power terminal block see Power Supply wiring section on page 30.

2. Connect the EUs to the MU using daisy chain methodology, using the RS-485 terminal block. See RS-485 Daisy Chain, on page 30 for detailed instructions.
3. When placing the MU into the ME-00 rack mount, remove the Power terminal block and slide the controller into the slot, making sure the ME-00 Molex connector is secured.

Note:
When using the ME-00 rack mount, the power and RS-485 communication connection are received from the rack itself and do not require direct wiring.

4. Connect a tamper switch to the tamper input terminal block. See General Purpose Inputs, on page 36.
5. Connect the RJ-45 cable to the LAN socket in the wall and the other end to the LAN socket on the MU board.

EXP-2024 Dual Reader Door Unit

The EXP-2024 unit and its components are shown in Figure 12 on page 23, detailed wiring instructions are explained below and shown in Figure 13, on page 25.

When connecting a reader, the following should be defined:

Single door controller:	Door 1 – Reader 1 IN
	Door 1 – Reader 2 OUT
Double door controller:	Door 1 – Reader 1 IN
	Door 2 – Reader 2 IN

Use the ExpansE web application to set the readers for single or dual door operation as well as IN or OUT usage. Additionally set the data transmission format for each reader. See Setting a Door controller EU on page 66, and Configuring the Reader on page 69.

The reader's tamper output connects to the access control panel's Reader-Tamper input. If the reader is interfered with, an alarm can be generated.

The panel's Reader G.LED output activates the reader's green LED input when operating in "Card and PIN" secure mode.

While this mode is activated, users must enter a PIN on the keypad immediately after presenting the card.

The controller activates the LED control for 2 seconds when an access granted event occurs.

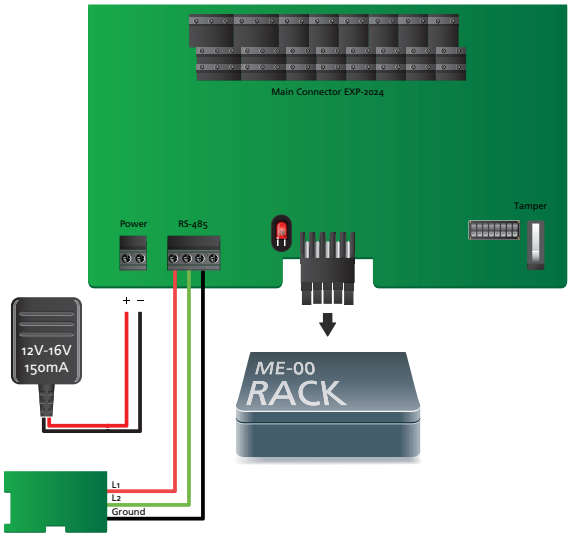


Figure 12: EXP-2024 Dual Reader Door Wiring

To wire the EXP-2024 Dual Reader Door Unit:

1. Connect a 12-16VDC 1500mA transformer to the power terminal block see Power Supply wiring section on page 30.
2. Connect the RS-485 communication terminal block to the controller using daisy chain methodology. See RS-485 Daisy Chain, on page 30 for detailed instructions.
3. When placing the EXP-2024 into the ME-00 rack mount, remove the Power terminal block and slide the controller into the slot, making sure the ME-00 Molex connector is secured.

Note:
When using the ME-00 rack mount, the power and RS-485 communication connection are received from the rack itself and do not require direct wiring.

4. Connect the reader(s) to the EXP-2024 using the table below as reference.

   If the tamper output is being utilized, connect the purple wire to the tamper input on the EXP-2024.

Color	Wiegand Output
Red	+DC Input
Black	Ground
White	Data 1 / Clock
Green	Data 0 / Data
Brown	LED/Buzzer Control
Purple	Tamper

5. Connect a tamper switch to the tamper input terminal block see General Purpose Inputs, on page 36. There are 4 inputs on the EXP-2024, see Inputs and outputs, on page 31 for detailed wiring instructions and uses.
6. There are 4 outputs on the EXP-2024 board that can be used for various applications, see Output Description, on page 36 for detailed wiring instructions and uses.
7. You have the option of connecting Rosslare's BLD-40 sounder see the BLD-40 manual for wiring instructions.

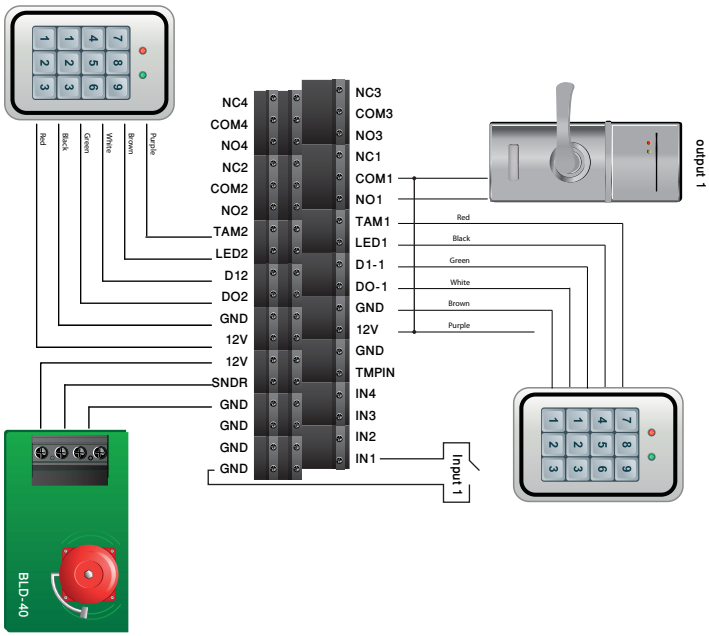


Figure 13: EXP- 2024 Dual Reader Door Unit Wiring Details

EXP-2016 16 Relay Elevator Control Unit

The EXP-2016 board and its components are shown in Figure 14 on page 26, detailed wiring instructions are explained below and shown in Figure 15, on page 27.

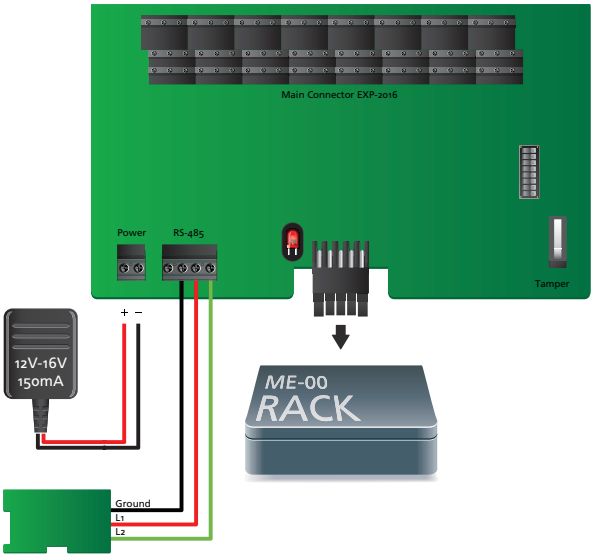


Figure 14: EXP-2016 16 Relay Elevator Control Unit Wiring

To wire the EXP-2016 16 Relay Elevator Control Unit:

1. Connect a 12-16VDC 1500mA transformer to the power terminal block, see Power Supply wiring section on page 30.
2. Connect the RS-485 communication terminal block to the EXP-2016 using daisy chain methodology. See RS-485 Daisy Chain, on page 30 for detailed instructions.
3. When placing the EXP-2016 into the ME-00 rack mount, remove the Power terminal block and slide the controller into the slot, making sure the ME-00 Molex connector is secured.

Note:
When using the ME-00 rack mount, the power and RS-485 communication connection are received from the rack itself and do not require direct wiring.

4. There are 16 outputs on the EXP-2016 board that can be used for various applications, see Output Description, on page 36 for detailed wiring instructions and uses.

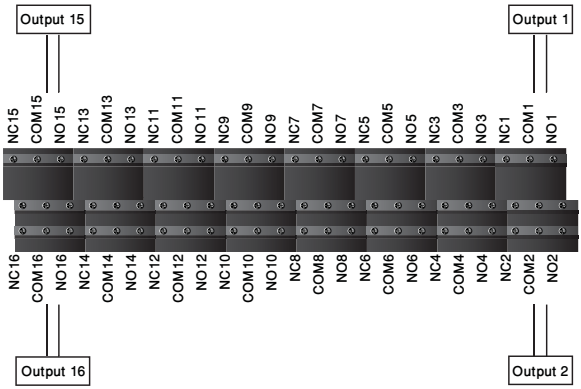


Figure 15: EXP-2016 16 Relay Outputs Elevator Control Unit Wiring

EXP-2088 – 8-Inputs/Outputs Interface

The EXP-2088 and its components are shown in Figure 16 below, detailed wiring instructions are explained below and shown in Figure 17, on page 28.

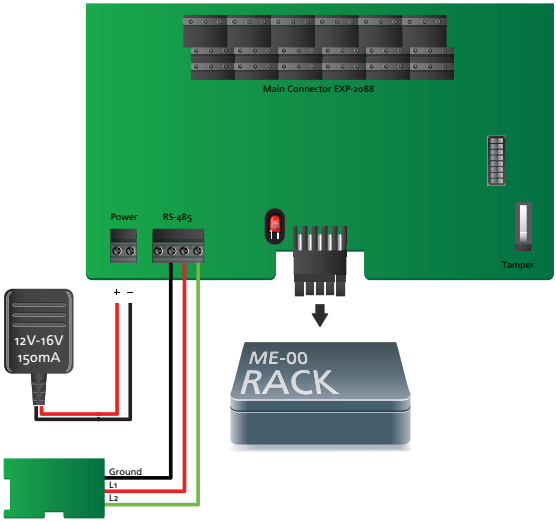


Figure 16: EXP-2088 – 8-Inputs/Outputs Interface Wiring

To wire the EXP-2088 8-Inputs/Outputs Interface Unit:

1. Connect a 12-16VDC 1500mA transformer to the power terminal block see Power Supply wiring section on page 30.

2. Connect the RS-485 communication terminal block to the EXP-2088 board using daisy chain methodology. See RS-485 Daisy Chain, on page 30 for detailed instructions.
3. When placing the EXP-2088 into the ME-00 rack mount, remove the Power terminal block and slide the EXP-2088 into the slot, making sure the ME-00 Molex connector is secured.

Note:
When using the ME-00 rack mount, the power and RS-485 communication connection are received from the rack itself and do not require direct wiring.

4. Connect a tamper switch to the tamper input terminal block, see General Purpose Inputs, on page 36. There are 8 inputs on the EXP-2088 board, see Inputs and outputs, on page 31 for detailed wiring instructions and uses.
5. There are 8 outputs on the EXP-2088 board that can be used for various applications, see Output Description, on page 36 for detailed wiring instructions and uses.

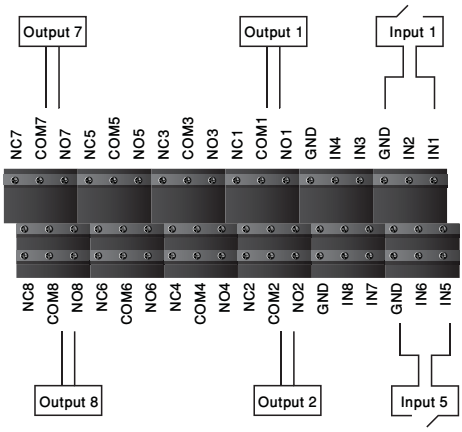


Figure 17: EXP-2088 – 8-Inputs/Outputs Interface Detailed Wiring

4.2 ME-00 9 Boards Tray Cabinet Housing Wiring

The ME-00 9 Boards Tray Cabinet Housing can be used to store several MUs and/or EUs. The Cabinet provides internal RS-485

communication between the units as well as power to each of the connected units.

See the detailed wiring instructions below on wiring the cabinet itself as well as Figure 18, below.

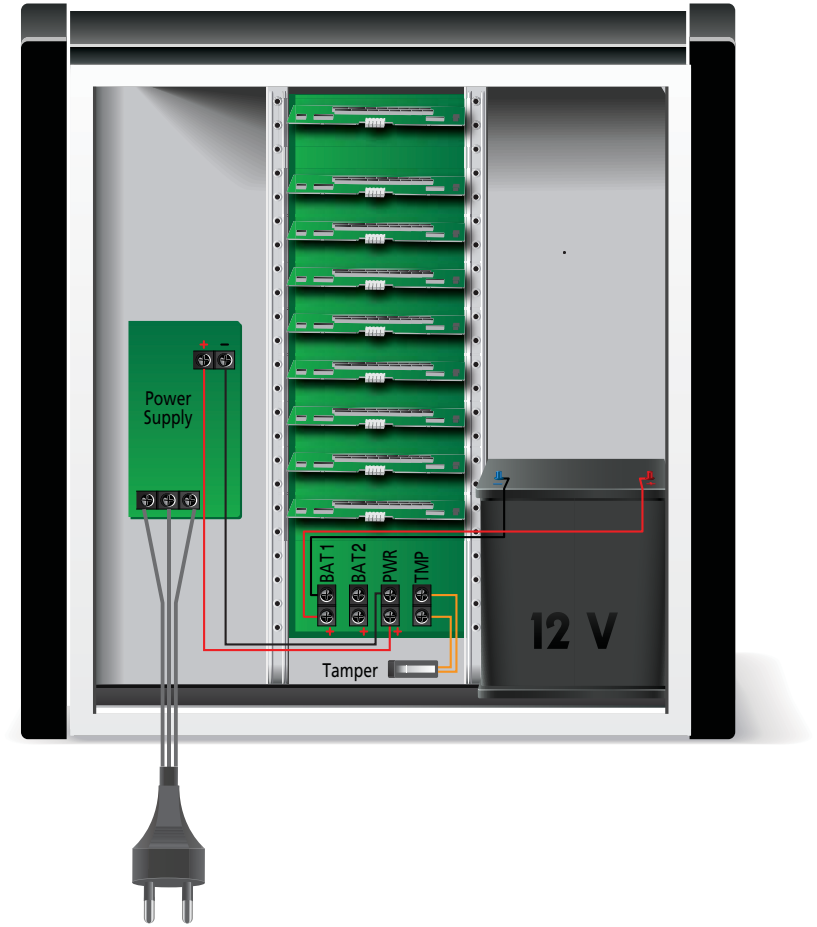


Figure 18: ME-00 – 9 Boards Tray Cabinet Housing Wiring

To wire the ME-00 9 Boards Tray Cabinet Housing:

1. Connect a 12-16VDC 1500mA transformer to the power terminal block, see Power Supply wiring section on page 30.
2. Connect the backup battery to the battery terminal block.

3. Connect a tamper switch to the tamper input terminal block, see General Purpose Inputs on page 36.

4.3 Power Supply

The following diagram illustrates the wiring between the DC adaptor and the ExpansE units, as well as the cabinet Power supply connection. It is recommended to add a 12VDC lead acid backup battery if the main power supply fails. Backup battery must be used if implementing the connection of lock devices to the units, when more than 1A of current is required.

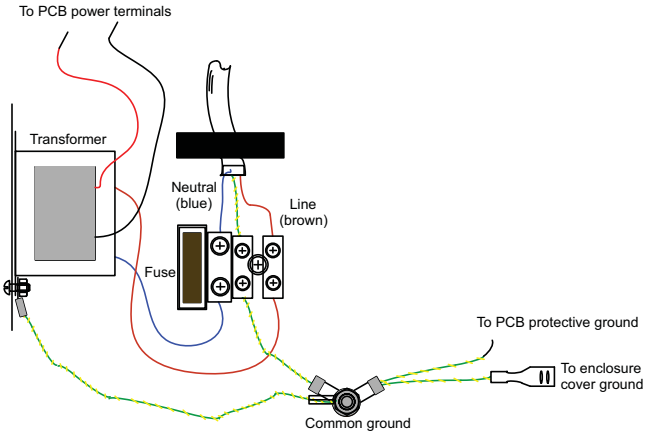


Figure 19: Wiring the Power Supply

4.4 RS-485 Daisy Chain

Daisy chain connection allows the connection of up to 32 EUs to the MU along a single serial line.

The MU is connected directly to the LAN network and the associated EUs are connected to the MU.

Note:
It is important to connect the Ground between all the connected units. The purpose of this connection is to have a single reference line.

At each end of the data line, a termination resistor of 120Ω may be required. Apply the resistor across the L1 and L2

connections. These termination resistors are especially important in long cable runs.

Note:
Other connections can optionally be used in addition to L1 and L2 for communication reference.

4.5 Inputs and outputs

The input and output connections detailed in this chapter are applicable to all inputs and outputs of the ExpansE system.

Input Types

Each input can be set as one of six input types – Normally Open, Normally Closed, Normally Open Supervised with 1 or 2 resistors, and Normally Closed Supervised with 1 or 2 resistors.

Inputs IN1, IN1A, IN2, and IN2A may be configured individually as either supervised or non-supervised inputs.

Non-supervised inputs have two states:

- Normal State – N.C. or N.O.
- Opposite State – N.O. or N.C.

Supervised inputs have three states:

- Normal State
- Abnormal State
- Trouble State.

The Trouble state is caused by either tampering with the input circuit or by faulty hardware installation. Once configured as supervised input, add a resistor of 2.2KΩ, 8.2KΩ, or both on the input circuit. See the following diagrams.

Normally Open Input Connection:

Normally Open Input has 2 states:

- Switch Open – Normal State:

  Loop resistance = Infinite (open circuit).
- Switch Closed – Abnormal State:

  Loop resistance = 0 (short circuit).

Normally Open Switch (N.O.)

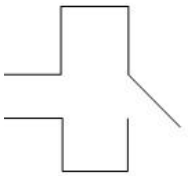


Figure 20: Normally Open Input Connection

Normally Closed Input Connection:

Normally Closed Input has two states:

- Switch Closed – Normal State:
  Loop resistance = 0 (short circuit)
- Switch Open – Abnormal State:
  Loop resistance = Infinite (open circuit)

Normally Closed Switch (N.C.)

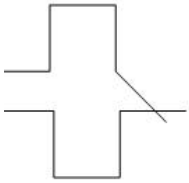


Figure 21: Normally Closed Input Connection

Normally Open Supervised Single Resistor Input Connection:

Connect an 8.2KΩ resistor in parallel to the input switch contacts.

Normally Open Supervised Input has 3 states:

- Switch Open – Normal State:
  Loop resistance = 8.2KΩ
- Switch Closed – Abnormal State:
  Loop resistance = 0 (short circuit)

- Open circuit across input terminals – Trouble State:

  Loop resistance = Infinite (open circuit)

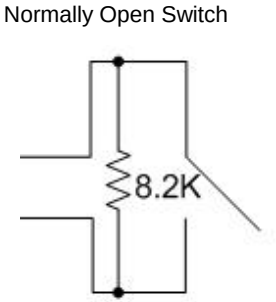


Figure 22: Normally Open Supervised Input (Single Resistor)

Normally Open Supervised Double Resistor Input Connection:

Connect a 2.2KΩ resistor in series to the input switch contacts.

Connect an 8.2KΩ resistor in parallel to the input switch contacts.

Normally Open Supervised Input has 3 states:

1. Switch Open – Normal State:

   Loop resistance = 10.4KΩ
2. Switch Closed – Abnormal State:

   Loop resistance = 2.2KΩ
3. Open circuit (Infinite loop resistance) or short circuit (0 resistance) across input terminals – Trouble State

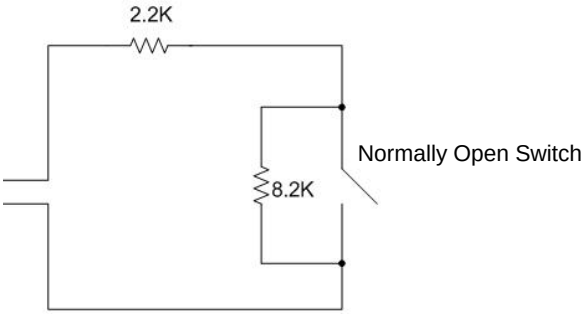


Figure 23: Normally Open Supervised Input (Double Resistor)

Normally Closed Supervised Single Resistor Input Connection:

Connect a 2.2KΩ resistor in series to the input switch contacts.

Normally Closed Supervised Input has 3 states:

- Switch Closed – Normal State:
  Loop resistance = 2.2KΩ
- Switch Open – Abnormal State:
  Loop resistance = Infinite (open circuit)
- Short circuit across input terminals – Trouble State:
  Loop resistance = 0 (short circuit)

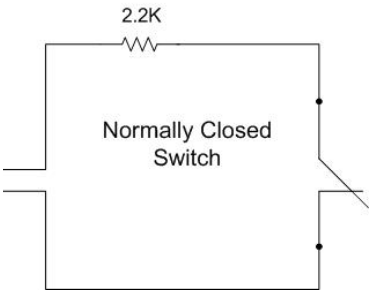


Figure 24: Normally Closed Supervised Input (Single Resistor)

Normally Closed Supervised Double Resistor Input Connection:

Connect a 2.2KΩ resistor in series to the input switch contacts.

Connect an 8.2KΩ resistor in parallel to the input switch contacts.

Normally Closed Supervised Input has 3 states:

- Switch Closed – Normal State:
  Loop resistance = 2.2KΩ
- Switch Open – Abnormal State:
  Loop resistance = 10.4KΩ
- Open circuit (Infinite loop resistance) or short circuit (0 resistance) across input terminals – Trouble State

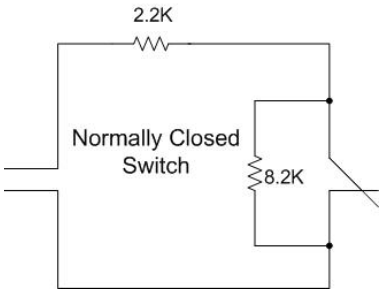


Figure 25: Normally Closed Supervised Input (Double Resistor)

Inputs Description

This chapter describes the inputs default operation.

Request to Exit Button (REX) Input

Use the REX Input to open a door directly. Typically, the REX input is connected to a Normally Open push button that is located inside the premises. The push button is generally located in an easy-to-access position and opens a door without reading a proximity card or PIN code.

Single door controller: Door 1 – IN 1
Double door controller: Door 1 – IN 1
Door 2 – IN 2

Door Monitor Input

The Door Monitor Input typically connects to a Normally Closed door sensing micro-switch for door status monitoring. Using Door Monitor enables many advanced options such as door forced alarm warning, door held open warning, interlocking doors and more. The following should be defined:

Single door controller: Door 1 – IN 1A
Door 1 – IN 1.A
Double door controller: Door 2 – IN 2A

General Purpose Inputs

These are free inputs that can be used for various functions. The following should be defined:

Single door controller: Door 1 – IN 2
Door 1 – IN 2A
Double door controller: No general purpose input available

General purpose inputs are suitable for most uses. For example, they might be used to detect tampering, to activate alarm sensors or for monitoring power supply failure.

Output Description

This chapter describes the inputs default operation.

Rosslare Security recommends the use of suppression diodes for all outputs that activate an inductive load.

Door Lock – Power Enabled Output

There are two types of door locking devices:

- Fail open (fail secure)
- Fail close (fail safe)

The following should be defined:

Single door controller: Door 1 – OUT 1
Double door controller: Door 1 – OUT 1
Door 2 – OUT 2

An ExpansE output can provide 12VDC power up to 1A for external door locks. For higher rated door locks an external UL 294 Listed power supply must be used to provide power to the door lock.

Note:
For UL installations, the installer must configure the system as fail-safe to comply with NFPA (National Fire Protection Association) regulations.

Elevator – Non-power Output

When using the elevator control output to close the elevator key relay switch, there is no need to supply power to the

circuit. There is an option to choose between Normally Open or Normally Closed circuits.

The circuit is based on wiring the common output together with either the N.O. or N.C. output to the elevator key switch thus closing the electric circuit.

4.6 Output Wiring

Figure 26 and Figure 27 below illustrate wiring for two main types of 12VDC electrical release mechanisms. Other electrical devices can be switched using the voltage free relay contacts.

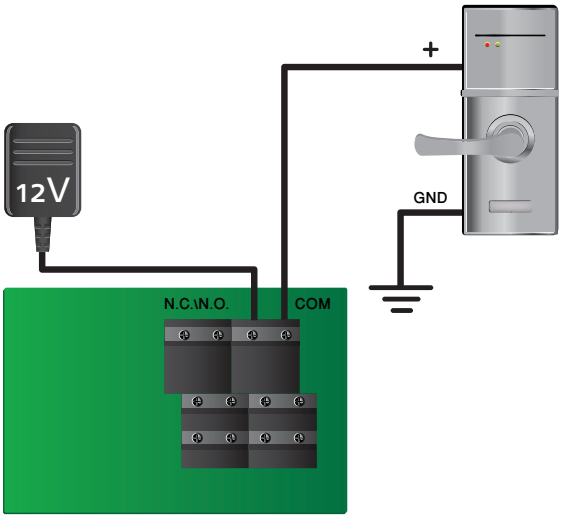


Figure 26: Power Enabled Output Wiring

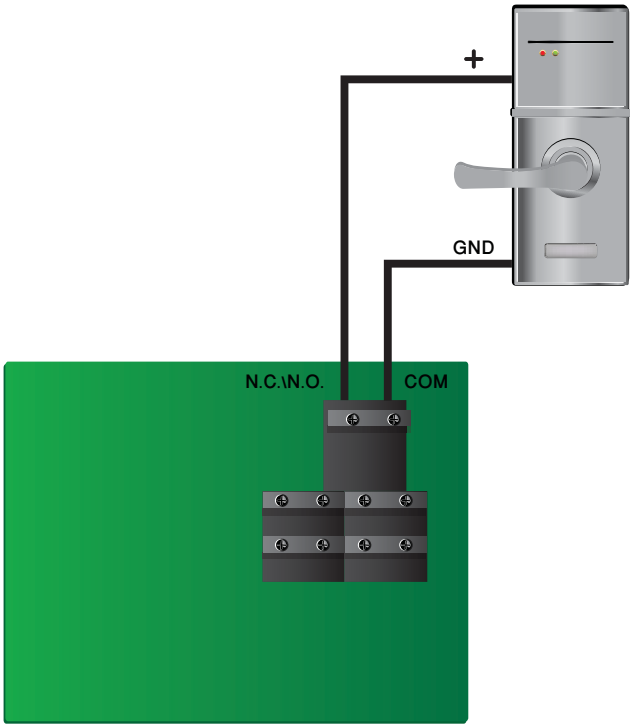


Figure 27: Non-Power Output Wiring

4.7 Mounting

This chapter shows how to mount and assemble each of the available boxes of the ExpansE system.

ME-01 Single Board Self Powered Metal Enclosure

The ME-01 is a sturdy, lockable, metal case that has room for a single MU or EU board along with a power supply and backup battery.

To install the ME-01:

1. Using the holes dimensions and locations shown in Figure 28, drill holes in the wall.
2. Insert masonry anchors into the drilled holes.

3. Wire the unit according to the wiring instructions as explained in the Wiring Instructions chapter, on page 21.
4. Mount the ME-01 enclosure onto the wall as shown in Figure 29, on page 40
5. Mount the MU or EU board in the enclosure using the spacers supplied and connect the in-box power and backup battery as shown in Figure 30, on page 40
6. Close and secure the enclosure.

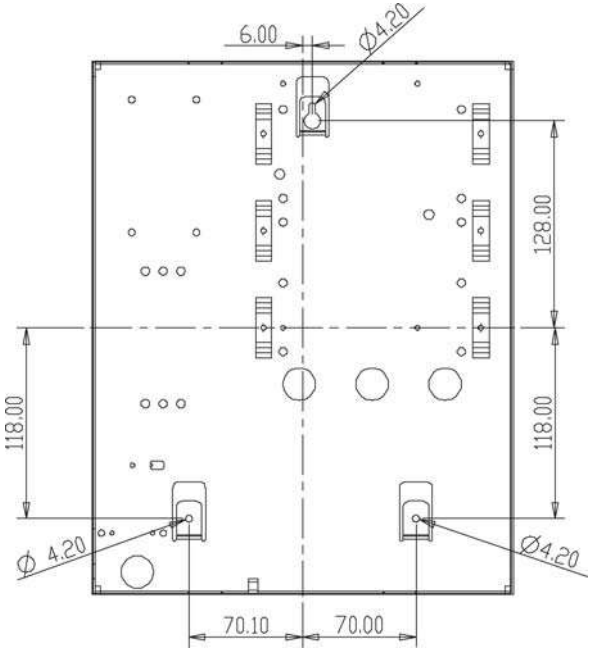


Figure 28: ME-01 Mounting Template

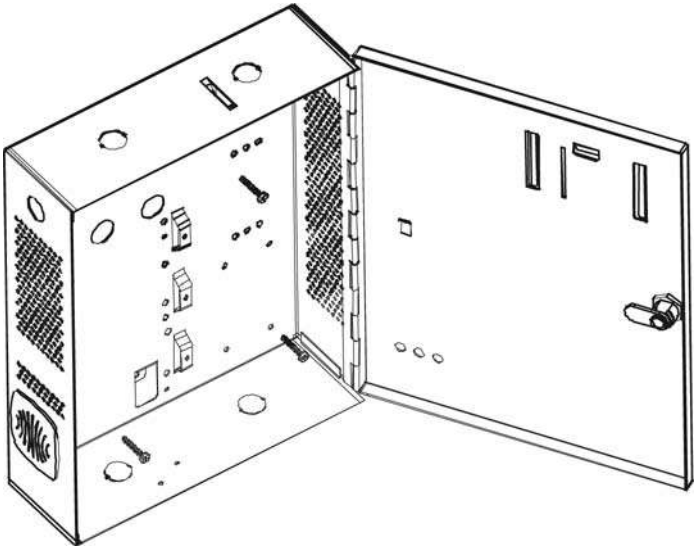


Figure 29: ME-01 Wall Mounting

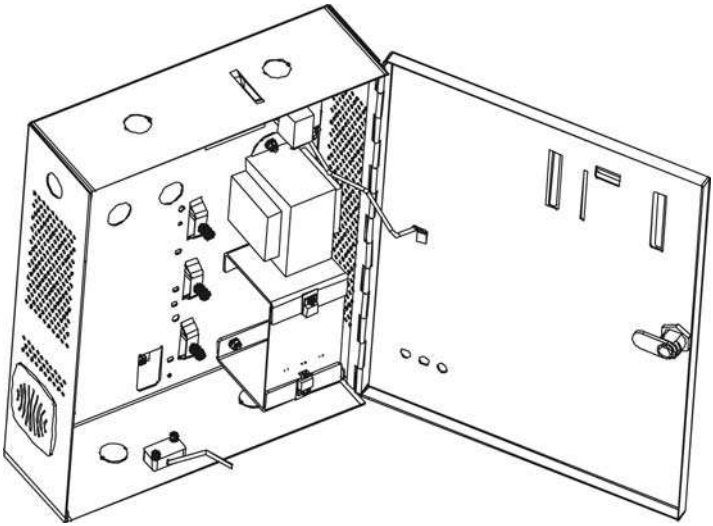


Figure 30: ME-01 Unit Mounting and In-Box Connections

ME-12 Single Board Self Powered Plastic Enclosure

The ME-12 specially designed plastic enclosure holds a single MU or EU board along with a power supply and backup battery.

To install the ME-12:

1. Using the holes dimensions and locations shown in Figure 31, drill holes in the wall.
2. Insert masonry anchors into the drilled holes.
3. Wire the unit according to the wiring instructions as explained in the Wiring Instructions chapter, on page 21.
4. Mount the ME-12 onto the wall as shown in Figure 32, on page 43
5. Mount the MU or EU board in the enclosure using the spacers supplied and connect the in-box power and backup battery as shown in Figure 33, on page 43, make sure to run the wires through the specifically designed wiring ducts.
6. Secure the backup battery and other loose components using the specifically designed openings and slots.
7. Close and secure the enclosure door.

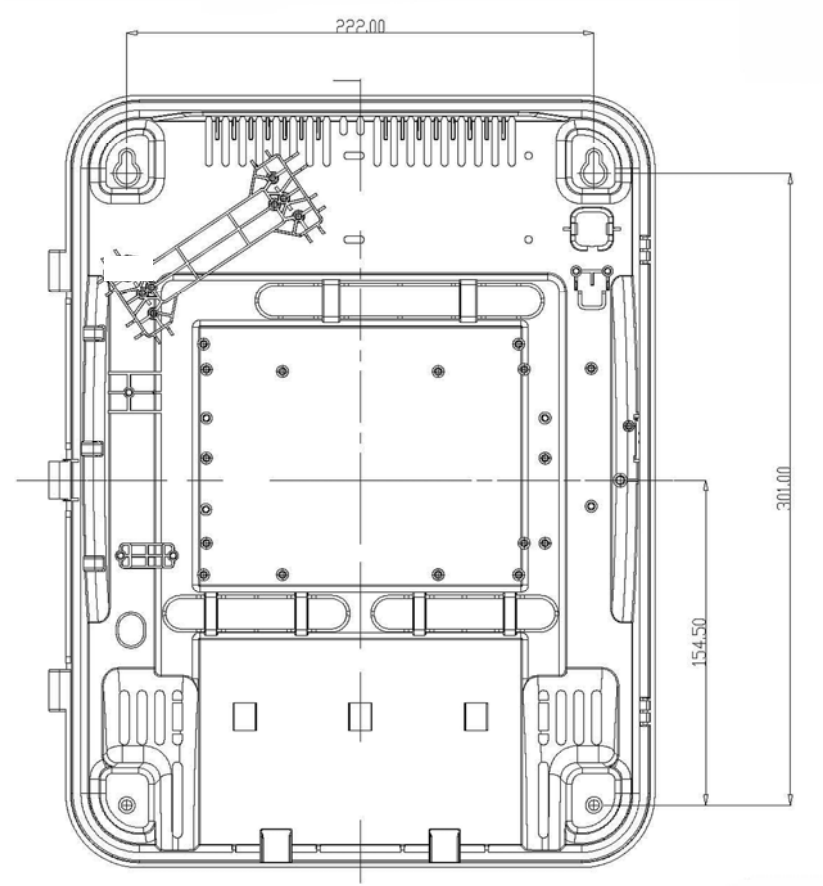


Figure 31: ME-12 Mounting Template

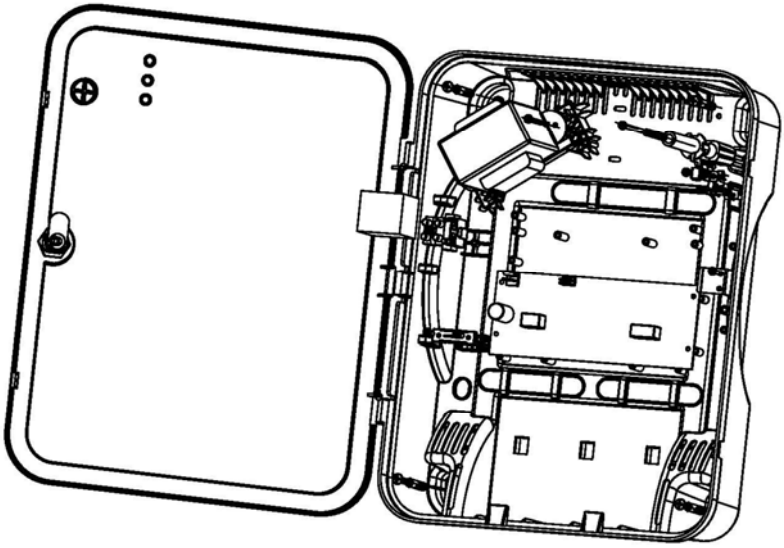


Figure 32: ME-12 Wall Mounting

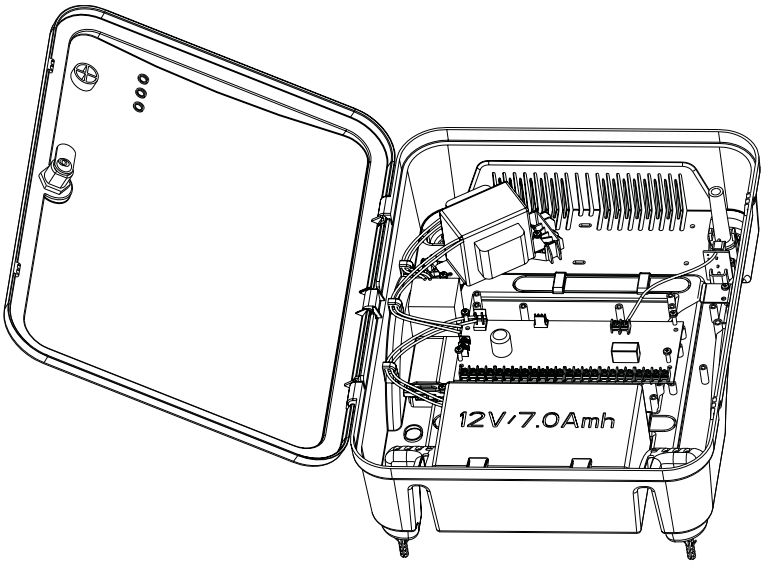


Figure 33: ME-12 Unit Mounting, In-Box Connections and wiring

ME-14 Compact Single Board Self Powered Enclosure

The ME-14 is a simple plastic casing suited for a singular MU or EU board.

To install the ME-14:

1. Open the ME-14 case using a screw driver.
2. Using the ME-14's backplate as a template drill holes in the wall, see also Figure 34 below for dimension reference.
3. Insert masonry anchors into the drilled holes.
4. Wire the unit according to the wiring instructions as explained in the Wiring Instructions chapter, on page 21.
5. Mount the ME-14 onto the wall.
6. Mount the MU or EU board in the case and reassemble the casing as shown in Figure 35, on page 45.

Note:
The ME-14 has no room for a backup battery charger. It can be used without a backup battery or by drawing lines from the MU backup battery to the unit.

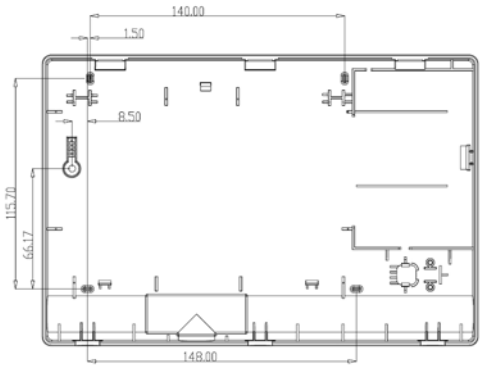


Figure 34: ME-14 Mounting Template

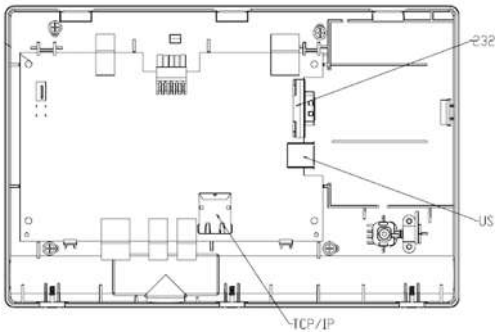


Figure 35: ME-14 Assembly

ME-00 9 Boards Tray Cabinet Housing

The ME-00 9 Boards Tray Cabinet Housing offers a cabinet that holds several MUs and/or EUs. The cabinet also holds several backup batteries as well as an embedded power supply, which powers all the connected units.

To install the ME-00:

1. Using the holes dimensions and locations shown in Figure 36, on page 46 drill holes in the wall.
2. Insert masonry anchors into the drilled holes.
3. Wire the cabinet as described in section 4.2 ME-00 9 Boards Tray Cabinet Housing Wiring, on page 28.
4. Slide and secure the individual units into the designated slots, ensure that each unit is secured in place to receive the power and communication directly from the rack as shown in Figure 37, on page 46.
5. Thread the wires through the designated holes in the rear of the rack as shown in Figure 38, on page 47, wire the individual units according to the wiring instructions as explained in the Wiring Instructions chapter, on page 21.
6. Mount the ME-00 onto the wall.
7. Close and secure the enclosure.

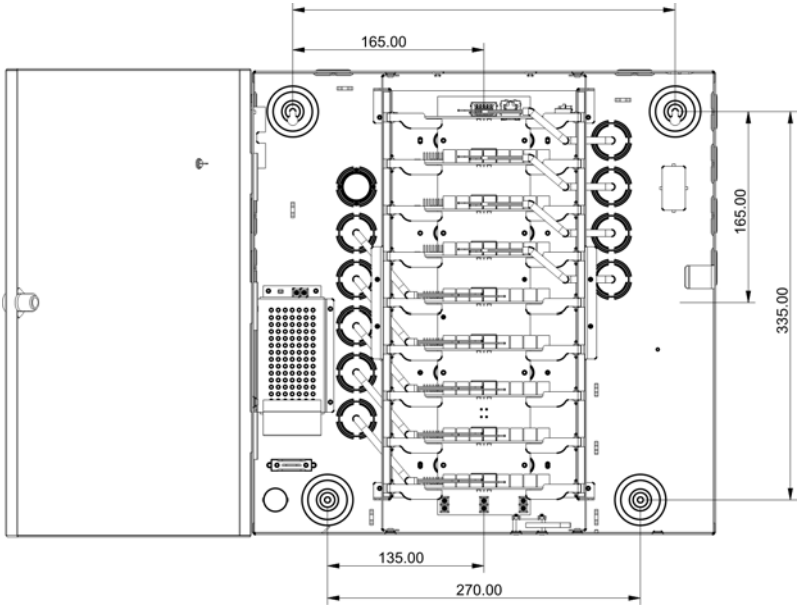


Figure 36: ME-00 Mounting Template

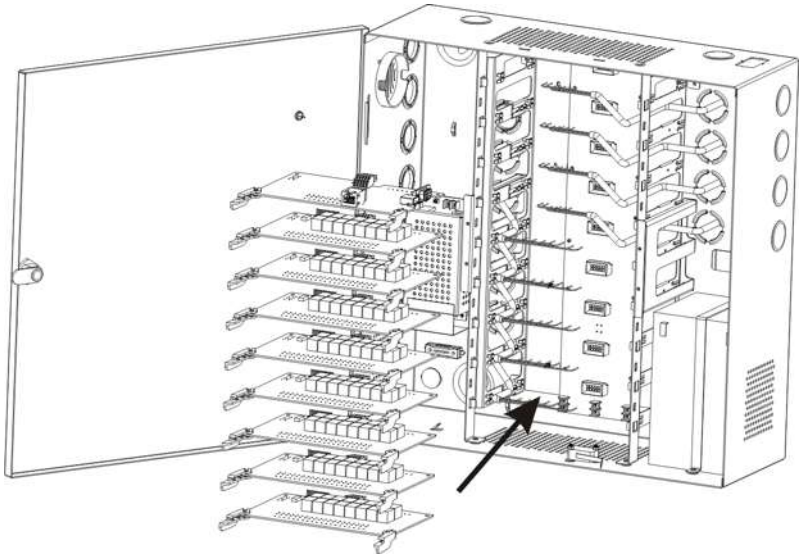


Figure 37: ME-00 Units Placement

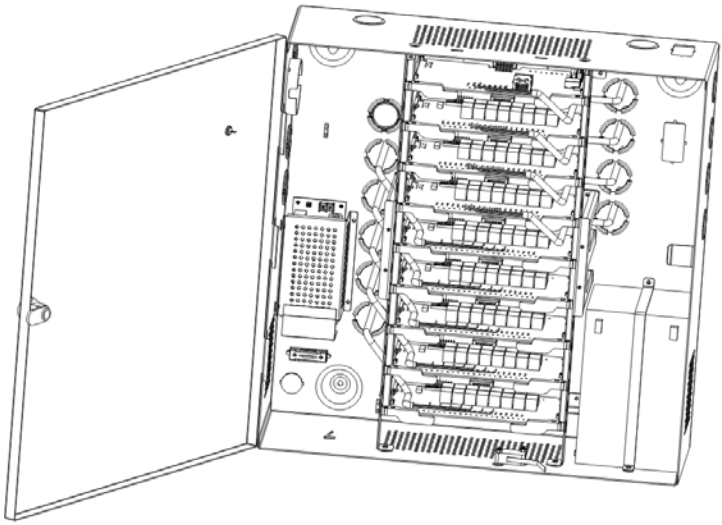


Figure 38: ME-00 Wiring Threads

4.8 DIP Switch Configuration

The ExpansE units have a DIP switch that controls a number of operating parameters including the device address and tamper settings.

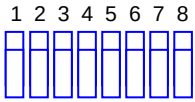


Figure 39: DIP Switch

The following is a list of DIP switch numbers in the units and their functions:

Switch #	Function
1	The ExpansE Units network address
2	
3	
4	
5	
6	Reserved for factory use, set to ON at all times
7	Front and Back Tamper switch Enabled/Disabled
8	

Note:
Power down the System before changing the DIP switches settings. After changes have been made, restart the system. The new settings are automatically defined after power up.

Network Addressing

The first 5 DIP switches are used to select the binary coded access control unit internal network address.

The default network address is set to "1".

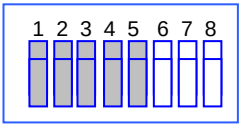


Figure 40: Internal Network Address DIP Switch Setting

Note:
For successful communications, the DIP switch must match the address set in the ExpansE web application.

The following table displays the 32 dip switch settings available:

Address	Switch 1	Switch 2	Switch 3	Switch 4	Switch 5
1	Off	Off	Off	Off	Off
2	Off	Off	Off	Off	On
3	Off	Off	Off	On	Off
4	Off	Off	Off	On	On
5	Off	Off	On	Off	Off
6	Off	Off	On	Off	On
7	Off	Off	On	On	Off
8	Off	Off	On	On	On
9	Off	On	Off	Off	Off
10	Off	On	Off	Off	On
11	Off	On	Off	On	Off
12	Off	On	Off	On	On
13	Off	On	On	Off	Off
14	Off	On	On	Off	On
15	Off	On	On	On	Off
16	Off	On	On	On	On

17	On	Off	Off	Off	Off
18	On	Off	Off	Off	On
19	On	Off	Off	On	Off
20	On	Off	Off	On	On
21	On	Off	On	Off	Off
22	On	Off	On	Off	On
23	On	Off	On	On	Off
24	On	Off	On	On	On
25	On	On	Off	Off	Off
26	On	On	Off	Off	On
27	On	On	Off	On	Off
28	On	On	Off	On	On
29	On	On	On	Off	Off
30	On	On	On	Off	On
31	On	On	On	On	Off
32	On	On	On	On	On

Note:
DIP switch #6 must be set to ON at all times.

Tamper Enabling

DIP switches 7 and 8 are used to enable or disable the front and back tamper capability.

Select the DIP switch setting as described in the table below to determine the tamper behavior.

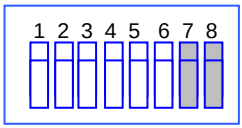


Figure 41: Tamper DIP Switch Setting

Back	Front	S7	S8
Enabled	**Enabled**	OFF	OFF
Enabled	**Disabled**	ON	OFF
Disabled	**Enabled**	OFF	ON
Disabled	**Disabled**	ON	ON

5. Communications

The ExpansE system utilizes several communication protocols for the various communication needs.

The MUs are connected to one another via an Ethernet network, this connection also allows access to the web based application used to manage the system.

RS-485 communication protocol is used to connect each MU to its associated EUs.

Note:

The EUs address is defined in the ExpansE web application.
It is important that the DIP switch and the software are set to the same address.

6. The ExpansE WEB Application

ExpansE's built-in Web application and networking capabilities provide faster and easier setup— software installation and computer configuration are not required. The control of all system configuration options and additional services, including real-time monitoring, can be performed from any panel and computer on the network.

Note:
For best performance use either Google chrome or Mozilla Firefox browsers.

6.1 Initial PC Configuration

Before accessing the ExpansE Web application you need to define your PC's IP to match that of the ExpansE's IP.

After Configuring the ExpansE Web application for the first time, remember to revert back to your original IP.

To define your PC's IP (Windows Xp):

1. Open the local area connection properties window, **Start→Control Panel→Network Connections→Local Area Connection**.

Figure 42: Windows XP – Control Panel

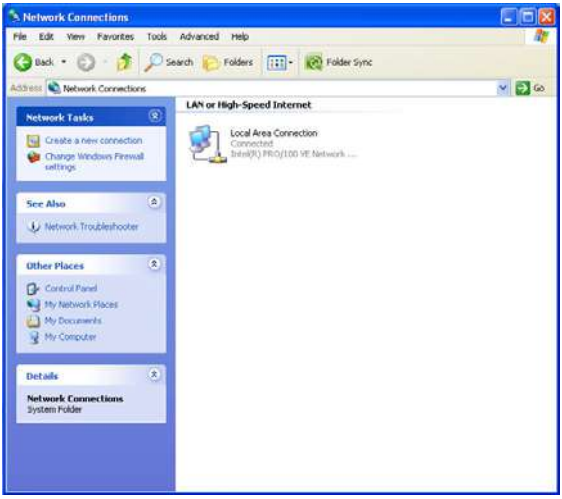


Figure 43: Windows XP – Network Connections

2. The *Local Area Connection Status* window opens. Click **Properties** to access the *Local Area Connection Properties* window.

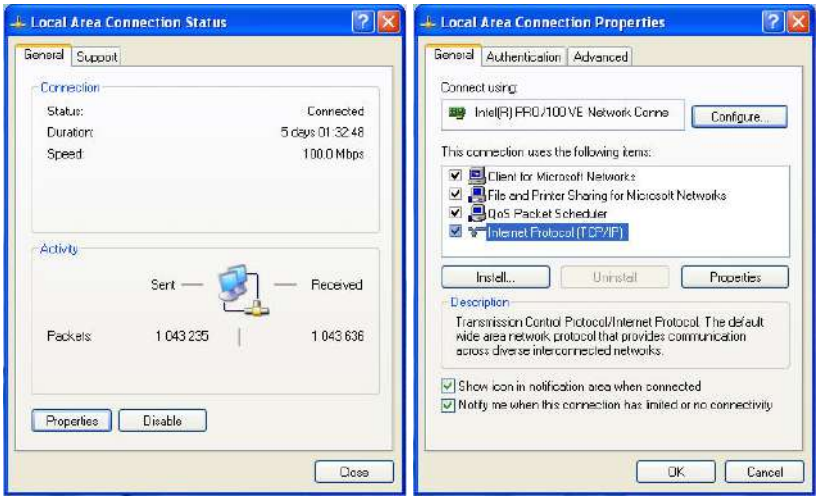


Figure 44: Windows XP – *Local Area Connection Status* and *Properties* windows

3. Select Internet Protocol (TCP/IP) and click properties. The *Internet Protocol (TCP/IP) Properties* window opens.

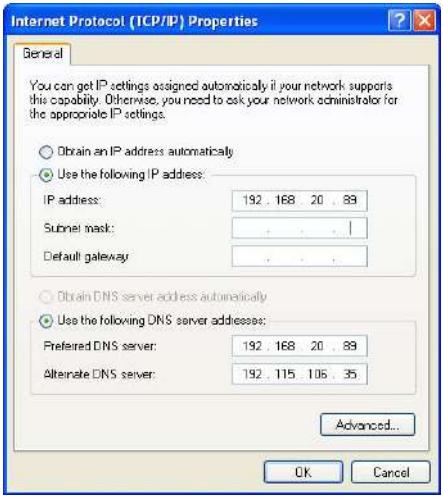


Figure 45: Windows XP – *Internet Protocol (TCP/IP) Properties* windows

4. Select the **Use the following IP address:** option and type **192.168.20.198** in the *IP address* field, **255.255.255.0** in the *Subnet mask* field and **192.168.20.1** in the *Default gateway* field.
5. Select the **Use the following DNS server address** option and type **192.168.20.2** in the *Preferred DNS Server* field, and **192.115.106.35** in the *Alternate DNS Server* field.
6. Click **OK** to save and exit the properties window.
7. After configuring the ExpansE Web application as described in section 6.2 Initial Access and Network Settings, on page 56, repeat the process with the correct network settings for your PC as provided by your IT professional.

To define your PC's IP (Windows Vista/7):

1. Open the *Network and Sharing Center* window, **Start→Control Panel→Network and Sharing Center**.

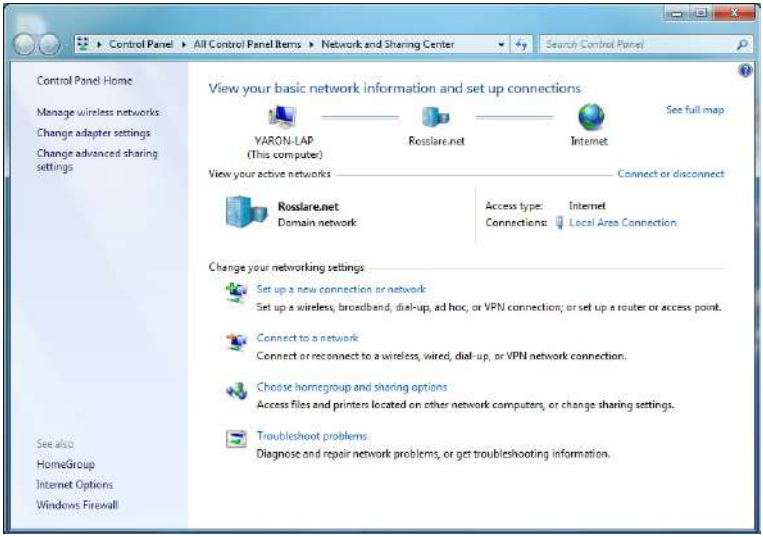


Figure 46: Windows Vista/7 – Network and Sharing Center

2. Click **Change adapter settings**, right click your connection and click **Status**.

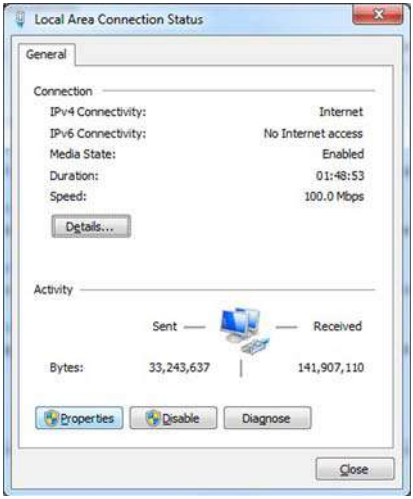


Figure 47: Windows Vista/7 – Network Connections

3. The *Local Area Connection Status* window opens. Click **Properties** to access the *Local Area Connection Properties* window.

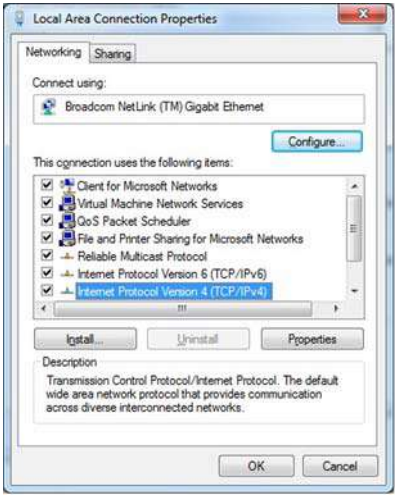


Figure 48: Windows Vista/7 – *Local Area Connection Properties* window

4. Select Internet Protocol Version 4 (TCP/IPv4) and click properties. The *Internet Protocol Version 4 (TCP/IPv4) Properties* window opens.

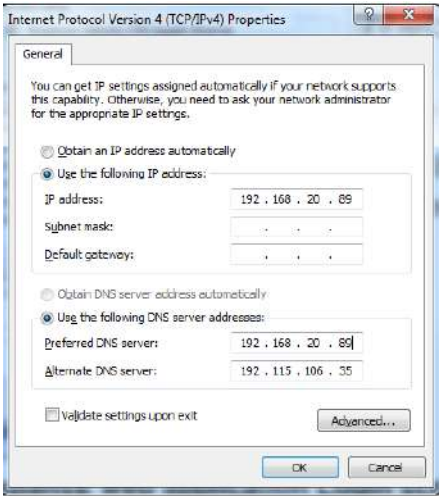


Figure 49: Windows XP – *Internet Protocol (TCP/IP) Properties* windows

5. Select the **Use the following IP address** option and type **192.168.20.198** in the *IP address* field, **255.255.255.0** in the

Subnet mask field, and **192.168.20.1** in the *Default gateway* field.

6. Select the **Use the following DNS server address** option and type **192.168.20.2** in the *Preferred DNS Server* field, and **192.115.106.35** in the *Alternate DNS Server* field.
7. Click **OK** to save and exit the properties window.
8. After configuring the ExpansE Web application as described in section 6.2 Initial Access and Network Settings, below, repeat the process with the correct network settings for your PC as provided by your IT professional.

6.2 Initial Access and Network Settings

The ExpansE web application requires no installation or unique PC setup, any computer connected to the same network as the ExpansE can access the application.

The ExpansE web based application automatically detects and configures connected units, it is therefore crucial that each system (MU and EUs) be connected and defined in the application separately.

To access & configure the ExpansE for the first time:

1. Open your web browser and type the default IP address 192.168.20.25 in the address line. The Login screen opens.

Note:
For best performance use either Google chrome or Mozilla Firefox browsers.

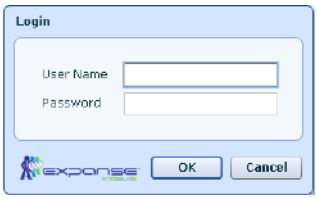


Figure 50: ExpansE web application Login screen

2. Type your **User name** and **Password**.

Note:
By default, the user name and the initial password is Admin. Type "admin" in the **User name** and **Password** fields.

3. Click **OK**.

   The ExpansE home page opens, see Figure 51, followed immediately by the settings window, see Figure 52, below and Figure 53, on page 58.

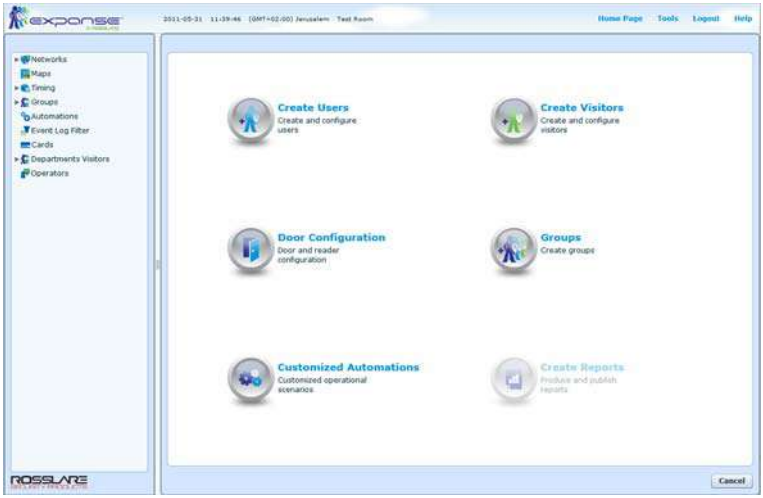


Figure 51: ExpansE web application Homepage

4. When accessing the application for the first time the system settings window opens automatically in order to configure the system. The same window can be accessed using the **Settings** link located on the main windows upper right corner.

Figure 52: System Settings – General Tab

5. Ensure that the *Master* option is selected; any additional MUs that are defined in the system will be defined as *Slaves*.

6. Define the ExpansE's network identity.

Note:
Contact your network administrator for assistance in finding the network parameters needed.

- Set the *IP Address* for the ExpansE MU
- Set the *Subnet Mask* for the ExpansE MU
- Set the *Default Gateway* for the ExpansE MU
- When defining slave MUs, type the IP Address of the master MU in the *Master IP* Address field.

Click the **Date and Time** tab to continue with the initial configuration.

7. Ensure that *Auto* option is selected and select your time zone from the *Timezone* list. The time and date will be automatically updated from either the Primary or Secondary time server.

   Alternatively
   Select the Manual option to define the date and time.
   - Type the date in the *Local Date* field or open the calendar by clicking the calendar icon and select the date.
   - Type or use the arrows to set the time in the *Local Time* field

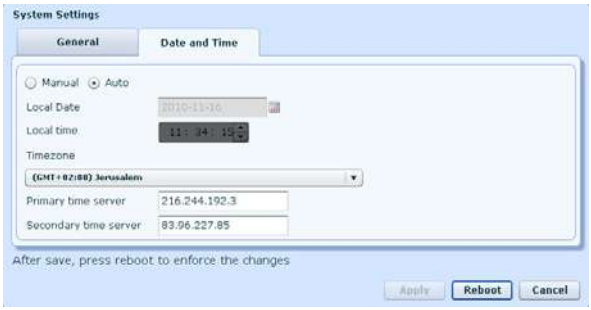


Figure 53: System Settings – Date and Time Tab

8. Click Apply to save the changes made.
9. Click reboot to restart the unit and implement the changes in the MU.

6.3 The ExpansE main window

The entire central functionality of the ExpansE web based application is available from its main window.

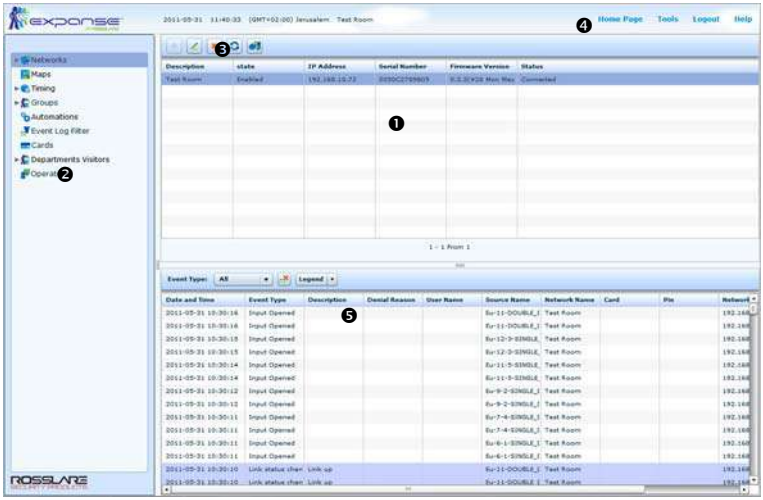


Figure 54: ExpansE web application Main Screen

The ExpansE web application's Main screen is divided into sections:

Section	Description
1 Display Area	Displays all items within the tree view selected element.
2 Tree View	Allows users to configure, monitor, and control every aspect of the ExpansE system. For more information, see Tree View, page 60.
3 Toolbar	Has toolbar icons which users can use for the key tasks required in managing access control across a facility. The available icons change according to the view selected. For more information, see Toolbar, page 62.
4 Menu Bar	Controls the software general operation and setup. For more information, see Menu Bar, page 60.

5 Event Window	Displays 200 events comprised of general status information, such as: Operator name, Client/Server mode, system readiness, system download, date, and time.

6.4 Tree View

The Tree View allows users to configure, monitor, and control every aspect of a facility's access control network. When the user selects an element from the tree, its content is shown in the main display area.

Networks

A network is a group of MUs each with up to 32 EUs. The ExpansE connects to the units across the Ethernet between MUs and RS-485 between EUs. The ExpansE system automatically detects and configures connected units, you only need to initialize it in the system. For more information, see Setting the Controllers, on page 65.

Maps

The Status Map displays the status of every door, reader, and alarm in the facility on user-selected floor plans.

The system can display multiple nested status maps, allowing users to show either the complete access control network or a specific area in detail.

Timing

Timing defines a weekly time period or set of time periods, for example, "Office Hours" or "Out of Office Hours". Door access rights, alarms, and input/output behavior can all be set to behave differently within each Timing set. For more information, see Defining Timing, on page 77.

Groups

Groups consist of access groups, input groups, output groups and elevator groups. An Access Group defines when each reader on the site will be available for access. All site personnel

are assigned to appropriate Access Groups. See Creating Access Groups, on page 79.

Input and Output groups define sets of outputs or inputs that should be managed together within a panel. See Configuring Inputs and Outputs, on page 71.

Elevator groups are similar to output groups but are dedicated to elevator control EUs and application. See Setting a 16 Relay Elevator Control Unit, on page 68 and Configuring Inputs and Outputs, on page 71.

Automation

Defines automated activities based on various input and output settings as well as other variables such as events and time zones.

Event log filter

The Events log filter allows you to define the type of events that are displayed and saved in the log file, by selecting those you wish to exclude, see Setting Event Log Filters, on page 95.

Cards

Lists all cards in the system and their statuses, and allows manual or automatic card addition to the system. For more information, see Defining Cards on page 86.

Departments and Visitors

The departments and visitors screen, lists all departments and users, as well as visitors. Each user is a member of a department. For each user, it is possible to assign a card and/or a PIN code, set access rights, personal details, and include an identification photograph. The setup also allows you to create visitors with their specific associated rights. See Defining Departments and Users, on page 87.

Operators

Operators are users with access privileges to the ExpansE web application. Different operators can be defined to have broader or more restricted security privileges, from complete

control over the system to the ability only to view one section. All Operator passwords are case-sensitive.

Only one operator with full administrator privileges can access the system simultaneously, other administrators trying to log in will only have read rights during that time.

Up to 20 users with read only privileges can access the system at the same time.

6.5 Toolbar

The toolbar controls key tasks required to manage access control across a facility.

The following toolbar icons are available:

General Icons

Icon	Name	Click icon to…
	Open Door Manually	Open the Door Manual Operation window. See Manual Door Control, on page 127.
	New	Create a new element of the selected type.
	Edit	Edit the selected element.
	Delete	Delete the selected item.
	Refresh	Refreshes the current view

Event type Icon

Icon	Name	Click icon to…
	Clear All Events	Clears all displayed Events. Click the drop-down arrow to change the view. The event are not erased and will be shown the next time you log in.

6.6 Menu Bar

The menu bar controls the general operation and setup of the application.

Homepage

The home page button, returns to the Homepage and enables access to one of several wizards. See chapter 8 Configuration Wizards on page 98.

Settings

Opens the MU setting window, see also Initial PC Configuration, on page 51.

Logout

Pressing the logout button, logs you out of the system, for security and management reasons only one operator with administrative rights can be logged in at one time.

Help Menu

The help menu opens the **About** screen which shows the system information.

Figure 55: ExpansE web application *About* Screen

6.7 Event Log

Every time access is granted or denied, for every door on a site an entry appears in the log file which is part of the static view of the ExpansE main window. Monitoring for potential door tampering or forced entry is logged, and displays of internal system warnings are also shown.

The events shown are defined in the event log filter window, see section 7.17 Setting Event Log Filters, on page 95.

You can also filter the view for a specific session using the even filter drop down list and clear the even logs shown using the clear all Icon on the event log tool bar.

7. How to Set Up a Site

This section outlines a recommended step-by-step process for configuring the ExpansE system.

Step	Action	Section
01	**Define the MU**	See Setting the Controllers, on page 65.
02	**Configure the various associated EUs**	See Setting a Door controller EU, on page 66, Setting a 16 Relay Elevator Control Unit, on page 68 and Setting an 8-Inputs/Outputs Interface on page 69.
03	**Configure the Readers**	See Configuring the Reader, on page 69.
04	**Configure inputs and outputs**	Configuring Inputs and Outputs, on page 71.
05	**Create Overview Maps**	See Creating Active Maps, on page 73.
06	**Define Time zones and Holidays**	See Defining Timing, on page 73.
07	**Create Access Groups**	See Creating Access Groups, on page 79.
08	**Create Input Groups**	See Creating Input Groups, on page 81.
09	**Create Output Groups**	See Creating Output Groups, on page 83.
10	**Create Elevator Groups**	See Creating Elevator Groups, on page 84.
11	**Set Automation behavior**	See Automation, on page 85.
12	**Define Cards**	See Defining Cards, on page 86.
13	**Define Departments and Users**	See Defining Departments and Users, on page 87

7.1 Setting the Controllers

The ExpansE network is set up of a master MU with several slave MUs, each with a network of EUs.

Each MU is automatically detected and configured but need to be initialized.

Note:
It is crucial that each sub system (MU and EUs) be connected and defined in the application separately.

To define the MU settings:

1. In the tree view, select **Networks**.

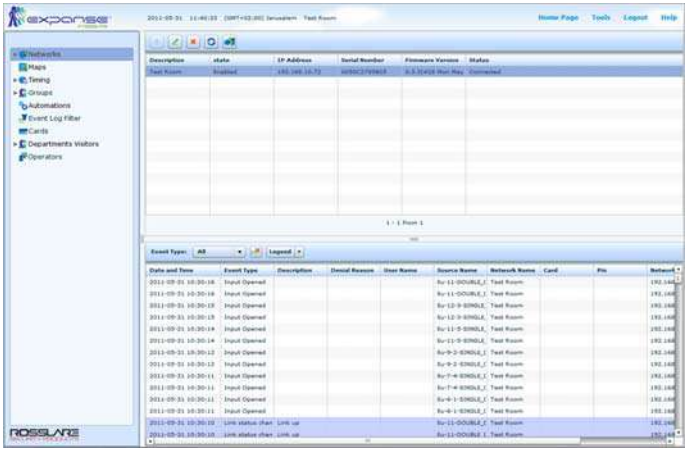


Figure 56: ExpansE web application *Networks* Screen

2. From the list of networks, double click one MU to open the MU Properties window.

Figure 57: *Network properties* window

3. Enter a description for the MU in the **Description** field
4. Check the **Enabled** checkbox, to enable the MU.
5. Click **OK** to save your settings and close the window.

   The connected EUs will appear in the tree view.
6. Double-click each EU found, or select and click the **Edit** icon, to open the EU Properties window.
7. Enter a description for the EU in the **Description** field
8. Check the **Enabled** checkbox, to enable the EU.
9. Click **OK** to save your settings and close the window.

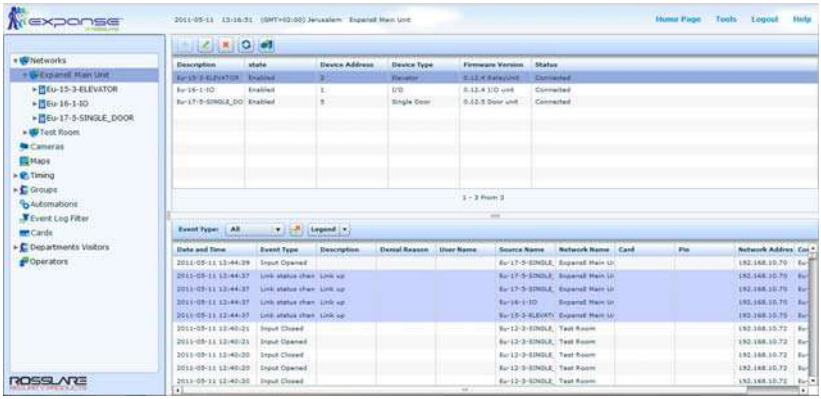


Figure 58: *Networks* Screen with connected EU's

7.2 Setting a Door controller EU

Each Door Controller controls one or two doors as well as inputs and outputs, each door can be configured individually.

Set the properties for each of the doors.

To set door properties:

1. In the tree view, click **Networks**.

   The available networks are listed in the display area.
2. Select a network and expand a panel in the tree view.

   Select a door to set its properties.
3. Click the Edit icon.

   The Door Controller Properties Window opens.

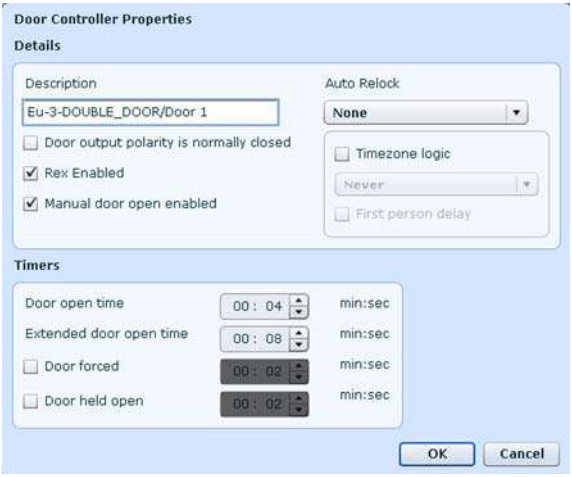


Figure 59: Door Controller Properties window

4. In the **Description** field, type a name for the door.
5. From the **Auto Relock** select box, select the event that causes the door to relock automatically
6. Determine the door polarity by checking or un-checking the **Door output polarity is Normally Closed** checkbox.

   Select this checkbox to ensure Fail Safe door opening if the Fail Safe door Lock Device power fails.
   Once enabled, the door output relay is activated when the door is closed, and is deactivated when the door is open. In this configuration, the Fail Safe lock device should be wired to the door relay N.O. (Normal Open) and COM (Common) terminals
7. Check the **REX enabled** checkbox to allow Requests to Exit for this door.
8. Check the **Manual Door Open Enabled** checkbox to allow operators to adjust the door manually. See Manual Door Control under Manual Operation, on page 127.
9. Sets the door's time zone logic behavior.
   - Select the **Timezone Logic** checkbox to initiate the time zone logic options and select an output from the list.
   - Check the **First person Delay** checkbox to keep the door locked until the first user opens it.

10. Set the duration for which the door stays unlocked by typing minutes and seconds in the **Door open time** field or use the associated up and down arrows.
11. Set the duration for which the door stays unlocked for users with Extended door open rights by typing minutes and seconds in the **Extended Door open time** field or use the associated up and down arrows.
12. Set the duration following which and when the door is forced open, an event occurs. Select the **Door forced** checkbox to use this timer and type the minutes and seconds in the associated field or use the up and down arrows.
13. Set the duration for which the door can be held open without raising an alarm event. Select the **Door held open** checkbox to use this timer and type the minutes and seconds in the associated field or use the up/down arrows.
14. Click **OK** to save your settings.
15. Define the Inputs and Outputs for the Dual Reader Door unit; see Configuring Inputs and Outputs, on page 71.

7.3 Setting a 16 Relay Elevator Control Unit

A 16 Relay Elevator Control Unit has 16 outputs and is associated to inputs in order to activate these outputs

Set the properties for each of the inputs and outputs for each of the elevator control EU's.

To set the 16 Relay Elevator Control Unit properties:

1. In the tree view, click **Networks**.

   The available networks are listed in the display area.
2. Select a network and expand a panel in the tree view.

   Select an elevator control EU to set its properties.
3. Define the inputs and outputs as explained in the Configuring Inputs and Outputs section on page 71.

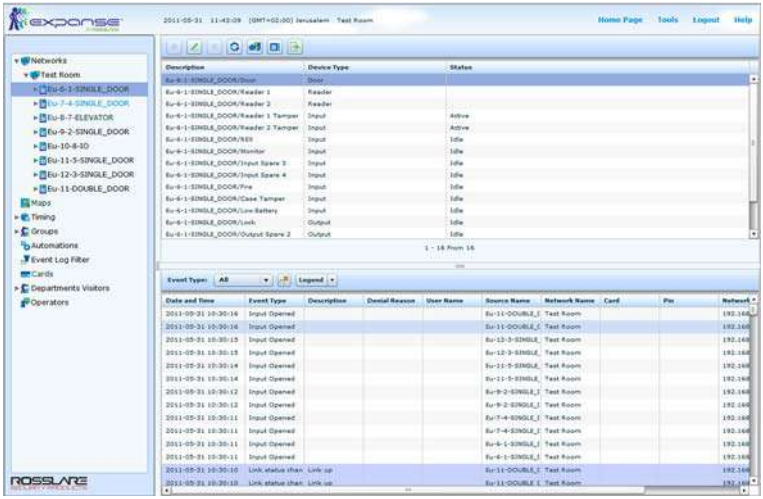


Figure 60: Elevator control EU window

7.4 Setting an 8-Inputs/Outputs Interface

Set the properties for each of the inputs & outputs for each of the eight inputs & outputs or the dedicated I/O control EU's.

To set dedicated 8-Inputs/Outputs Interface properties:

1. In the tree view, click **Networks**.

   The available networks are listed in the display area.
2. Select a network and expand a panel in the tree view.

   Select an I/O EU to set its properties.
3. Define the inputs and outputs as explained in the Configuring Inputs and Outputs section on page 71.

7.5 Configuring the Reader

Each Dual Reader Door Unit can be connected to one or two readers.

To configure a Reader:

1. In the Tree View, click **Networks**.

   The available networks are listed in the display area.
2. Select a network and expand the tree view.

3. Select a Dual Reader Door Unit and expand the tree view.
4. Select a reader to set its properties.
5. Click the **Edit** icon.

   The Reader Properties Window opens.

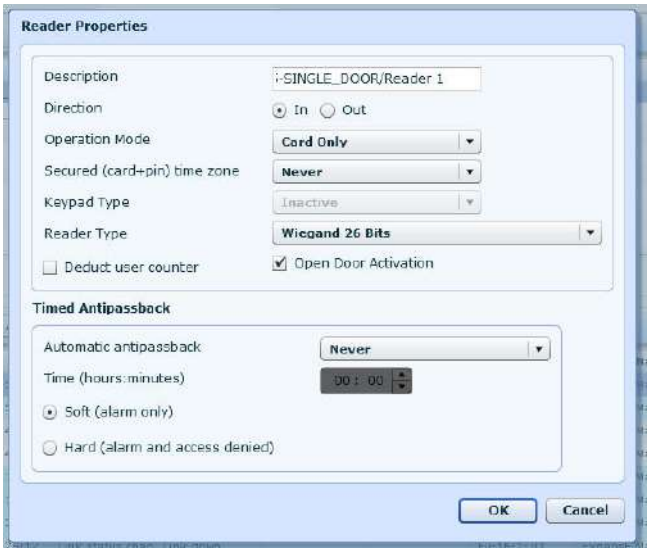


Figure 61: Reader Properties window

6. Select whether and when to apply antipassback rules from the **Automatic antipassback** list.
7. Set the time when to apply antipassback rules by typing hours and minutes in the **Time (Hours:Minutes)** field or use the associated up and down arrows.
8. Select either **Hard** or **Soft** antipassback application

   When hard antipassback is selected, an event is generated and the door does not open.
   When soft antipassback is selected, the door opens but an event is generated.
9. In the **Description** field, type a name for the reader.
10. Select whether the reader is allowing entry into the area or exit out of the area by selecting either the **In** or **Out** option.
11. From the Operation Mode list Select how the reader operates:

- **Inactive:** The reader is not in use.
- **Card Only:** The reader will accept RFID cards only.
- **PIN Only:** The reader will accept PIN inputs only.
- **Card or PIN:** The reader will accept both cards and PIN codes.
- **Card and PIN:** higher security – The reader requires both cards and PIN code for access.
- **Desktop:** The reader is inactive, but is being used to record new cards on the computer.
- **No Access Mode:** The reader will grant access to no users.

12. Using the **Secured (Card+PIN) time zone** list select a time zone during which access should be granted only after both the card and PIN are entered.

    The PIN must be entered within 10 seconds of card entry.
13. From the **Keypad Type** list, select the data transmission type for the type of keypad hardware.
14. From the **Reader Type** list, select the data transmission type for the reader hardware.
15. Check the **Biometric Reader** checkbox to allow use of Rosslare's biometric readers.
16. Check the **Deduct User Counter** checkbox to record this entry against the user's entry allowance counter.
17. Check the **Open Door Activation** checkbox to allow the reader to unlock the door.
18. Click **OK** to save your settings.

7.6 Configuring Inputs and Outputs

Inputs and outputs are available in each of the EUs. The number of Inputs and outputs depends on the type of EU.

To configure inputs and outputs:

1. In the Tree View, click **Networks**.

   The available networks are listed in the display area.
2. Select a network and expand the tree view.
3. Select one of the available EUs and expand the tree view.

4. Select an input to set its properties.
5. Click the **Edit** icon.

   The Input Properties Window opens.

Figure 62: Input Properties window

6. In the **Description** field, type a name for the input.
7. From the **Property** field select the type of input to be monitored.
   - **Normally Open/Close:** An input either in an open or closed state.
   - **Normally Open/Close 1 Resistor:** An input in an open, closed, or trouble state. This option is only available for supervised inputs.
   - **Normally Open/Close 2 Resistors:** An input in an open, closed, or trouble state, with additional checks for short-circuit and open-circuit tampering. This option is only available for supervised inputs.
8. Type the minutes and seconds in the **Start Delay** field or use the up and down arrows to set the delay time before this input becomes active. Note that on normally open input, the delay starts once the input contact is closed. On normally closed input, the delay starts once the input contact opens.
9. Click **OK** to save your settings.
10. Select an output to set its properties.
11. Click the **Edit** icon.

    The Output Properties Window appears.

Figure 63: Output Properties window

12. In the **Description** field, type a name for the output.
13. Click **OK** to save your settings.

7.7 Creating Active Maps

The Status Map displays the every enrolled unit in the system along with status indications for every door, input, output, antipassback rules, and alarms in the facility. The statuses are shown overlaid on a user-selected image such as floor plans, satellite image, etc.

To set-up a Status Map:

1. In the tree view, click **Maps**.

   The map management screen opens.

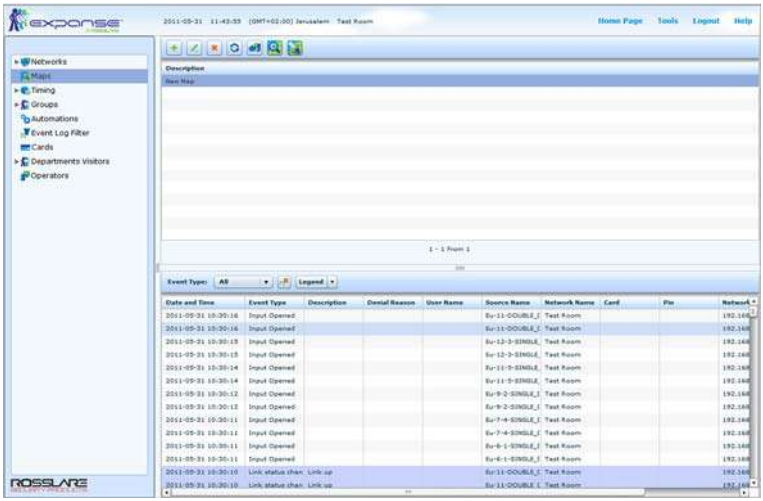


Figure 64: Map Management Screen

2. Click the New Element icon.

   The Map properties window appears.

Figure 65: Map Properties Window

3. Give the map a name. Type a description in the **Description** text box.
4. Click **Select Image** to select the image to be used in the map.

   The Select Image File Name window appears.

Figure 66: Select Image Window

Note:
The image files are taken from the MU's USB flash drive, the MU cannot import images and files from remote disk drivers.

5. Select a graphic file for the Status Map background. Click **OK**. The file selected is shown in the Map Image field.

   The files types supported are one of the following formats: jpg, gif, or bmp.

6. Add Networs to the map.
   - In the **Type** select box select *Network*. Click **Select**. The Select Network window opens

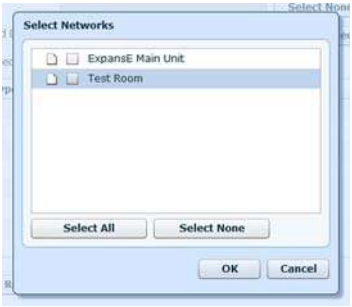


Figure 67: Select Networks Window

   - Select one or more networks from the list of available networks.
     You can also click **Select All** to select all of the available networks or **Select None** to deselect all of the networks.
   - Click **OK**. The device selected appears in the Selected Devices field.
   - Repeat the process for Controllers, Doors, Readers, Inputs, outputs, panels, etc.

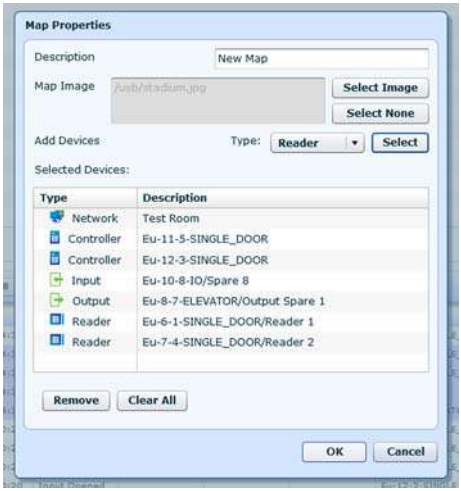


Figure 68: Map Properties Window – with devices

7. To remove devices from the list, select a device in the selected devices field and click **Remove**. To remove all of the devices click **Clear All**.

   Click **OK** to return to the map management window.

8. Click the **Design** icon to enter design mode.

Note:
It is highly recommended to add devices and place them in the design mode in batches to avoid clutter in large installations.

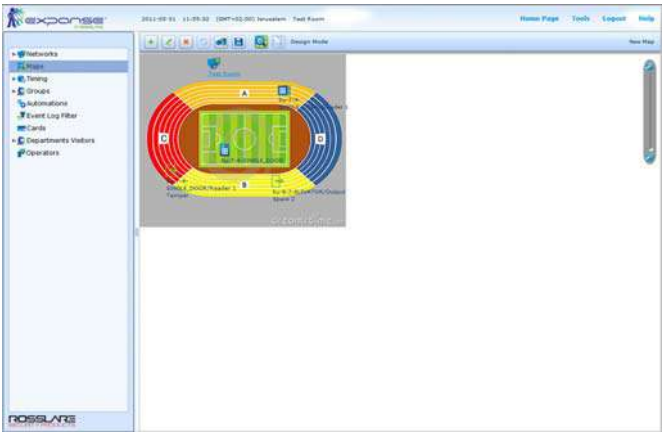


Figure 69: Map Design Mode

9. The objects appears on the status map. Drag each device to its correct position.

Note:
Status map icons can also be added to other status maps, indicating where the two map areas meet.

10. Click the **Run** icon to enter Run mode.

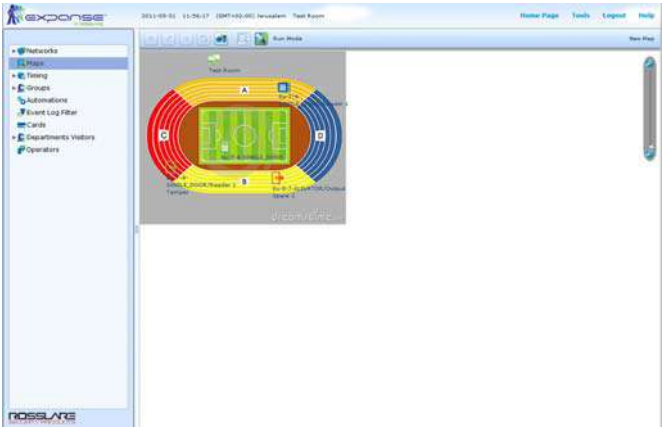


Figure 70: Map Run Mode

7.8 Defining Timing

Timing refers to a group of time periods within a week. Door access rights, as well as input and output behavior, can all be set to behave differently for each time zone. Many operations can be automatically enabled or disabled within a selected time zone.

To set a new time zone:

1. In the tree view, select **Timing,** and then **Time Zones**.

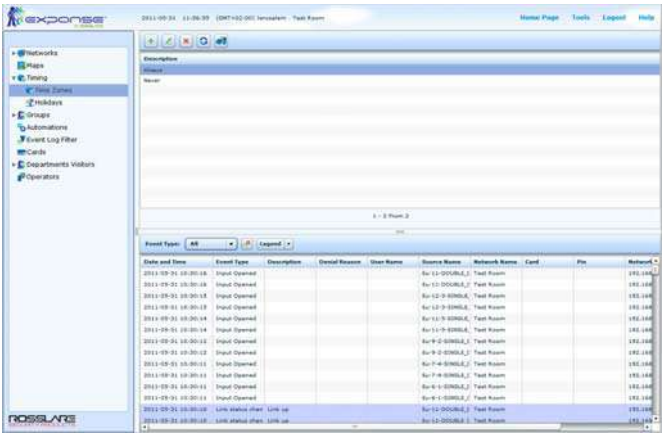


Figure 71: Timing window

2. On the toolbar, click the **New** icon to create a new time zone or select one of the time zones and click **Edit**.

The Time Zone Properties window opens.

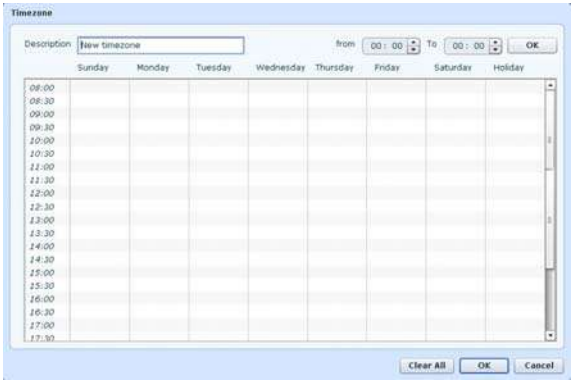


Figure 72: Time Zone Properties window

3. In the **Description** field, type a name for the time zone.
4. Set the start and end time of the time zone typing hours and minutes in the **From** and **To** fields or use the associated up and down arrows.
5. Select the days for which the time period is within the time zone. The "Holiday" day can be set to include national holidays.
6. Click the **Clear All** button to clear the selection.
7. Click **OK** to save your settings. The window closes and the display area displays the new time zone.

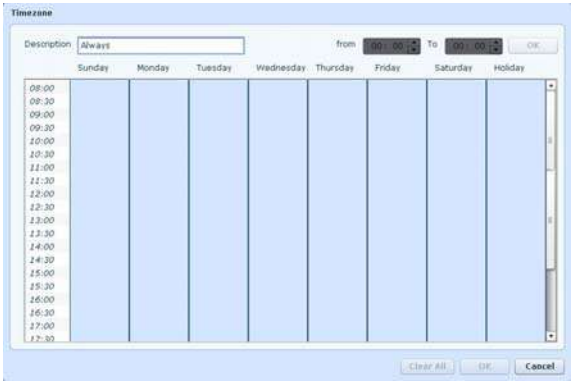


Figure 73: Time Zone window

8. In the tree view, select **Timing,** and then **Holidays**.

9. On the toolbar, click the **New** icon to create a new holiday or select one of the holidays and click **Edit**.

   The Holiday Properties window appears.

Figure 74: Holiday Properties window

10. In the **Description** field, type a name for the holiday.
11. Type the holiday's date in the **Date** field or open the calendar by clicking the calendar icon and select the date.
12. Check the **Every Year** checkbox to repeat the holiday on a yearly basis on the same date.
13. Click **OK** to save your settings.

7.9 Creating Access Groups

An access group includes a list of door readers and the time zones during which each of those door readers are available for access. Every user is assigned to an access group.

The Access Group window lists all the door readers defined in the database, and the time zones during which they can be accessed.

To create an access group:

1. In the Tree View, expand the **Groups** element and select **Access Groups**.

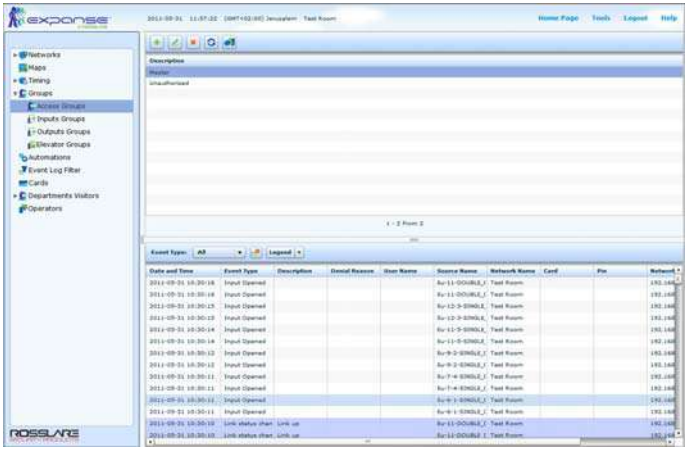


Figure 75: Access Group window

2. On the toolbar, click the **New** icon. The Access Group properties window opens.

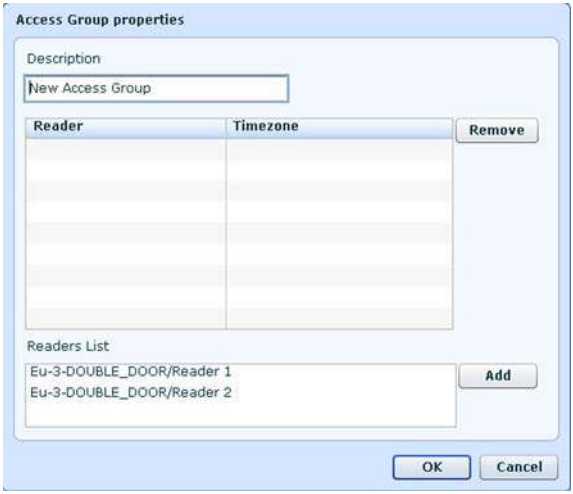


Figure 76: Access Group Properties window

3. In the **Description** field, type a name for the access group.
4. From the *Readers List* select the readers you wish to associate with this group and click **Add**.

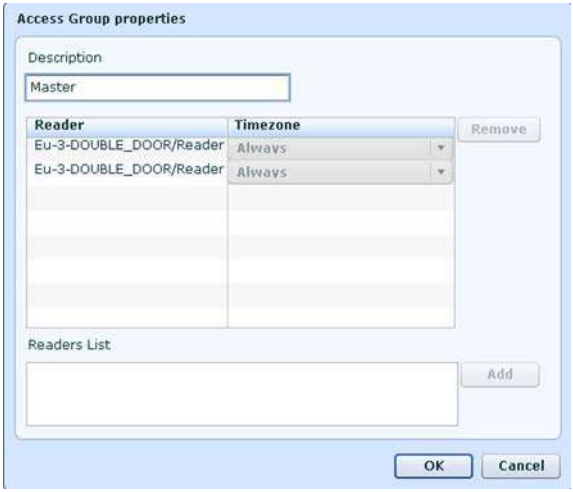


Figure 77: Access Group Properties Window with Associated Readers

5. For each of the readers select a time zone association.
6. Select a reader and then click **Remove** to remove the readers from the association list.
7. Click **OK** to save your settings.

7.10 Creating Input Groups

Input groups are a collection of Inputs from one or more panels that can be used in panel links to perform advanced operations.

To set an Input Group

1. In the Tree View, expand the **Groups** element and select **Input Groups**.
2. Click the **New** icon.

   A new input group is created.

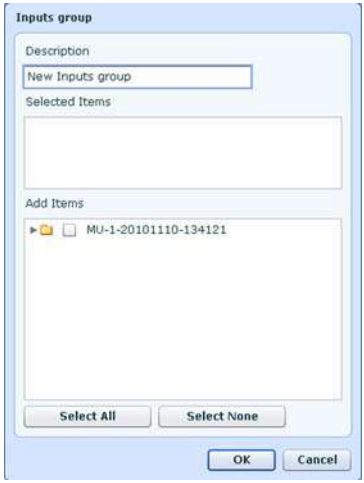


Figure 78: Input Group Window

3. In the **Description** field, type a name for the input group.
4. Within *Add Items* check all the inputs you wish to add.
5. Click **Select All** to add all of the inputs shown.
6. Click **Select None** to deselect all of the inputs selected.
7. All of the associated inputs will be shown in the *Selected Items* section.

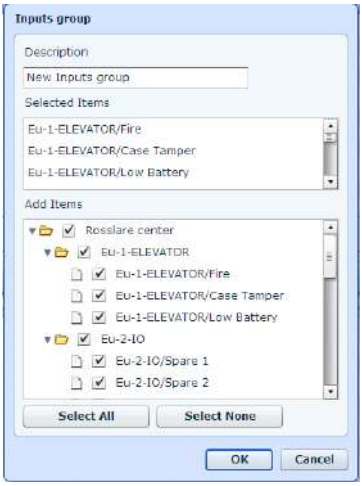


Figure 79: Input Group Window with Selected Inputs

8. Click **OK** to save your settings.

7.11 Creating Output Groups

Output groups are a collection of Outputs from panel or panels that can be used in panel links to perform advanced operations.

To set an Output Group

1. In the Tree View, expand the **Groups** element and select **Output Groups**.
2. Click the **New** icon.

   A new Output group is created.
3. In the **Description** field, type a name for the output group.
4. Within *Add Items* check all the outputs you wish to add.

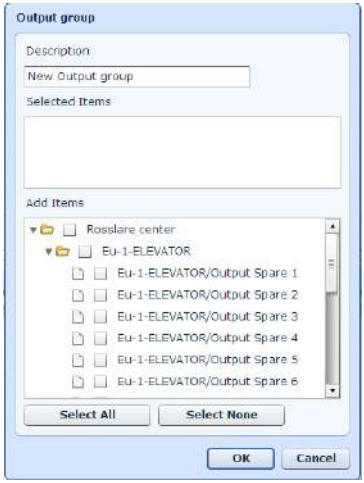


Figure 80: Output Group Window

5. Click **Select All** to add all of the outputs shown.
6. Click **Select None** to deselect all of the outputs selected.
7. All of the associated outputs will be shown in the *Selected Items* section.
8. Click **OK** to save your settings.

7.12 Creating Elevator Groups

Elevator groups are a collection of inputs and outputs from various EUs that can be linked to perform advanced operations, such as Elevator control.

To set an Elevator Group

1. In the Tree View, expand the **Groups** element and select **Elevator Groups**.
2. Click the **New** icon.

   A new Elevator group is created.
3. In the **Description** field, type a name for the elevator group.
4. In the *Reader List* section check all the readers you wish to add to the group.

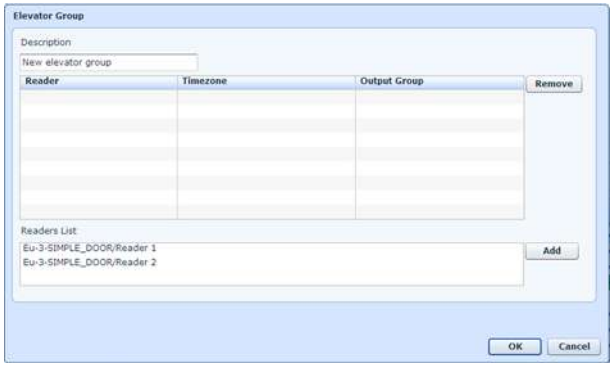


Figure 81: Output Group Window

5. All of the associated readers will be shown in the list.
6. For each of the selected readers select an associated **Timezone** and **Output Group**.
7. Click **OK** to save your settings.

7.13 Automation

Set various automated applications by associating various input and reader events with various output actions.

To define various automatic operations:

1. In the Tree View, expand the **Automation** element.
2. Click the **New** icon.

   A new automation activity is created.

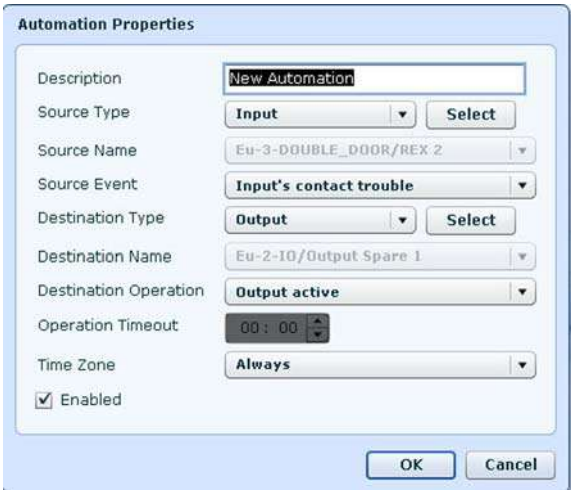


Figure 82: Automation Properties Window

3. In the **Description** field, type a name for the automated activity.
4. From the **Source Type** list, select the desired source and click **Select**.
5. From the **Source Name** list, select the specific source, this select box will only be available after you selected a source type.
6. Based on the source selected various events are shown in the **Source Event** list, select the event you wish to use.
7. From the **Destination Type** list, select the desired output type and click **Select**.

8. From the **Destination Name** list, select the specific output, this select box will only be available after you selected a destination type.
9. Based on the output selected various operations are shown in the **Destination Operation** list, select the operation you wish to perform.
10. Type the minutes and seconds in the **Operation Timeout** field or use the up and down arrows to set the a time frame for the operation timeout.
11. Select a time zone for this operation from the **Time Zone** list.
12. Check the **Enable** checkbox to enable the automated operation.
13. Click **OK** to save your settings.

7.14 Defining Cards

The ExpansE Web Based application database maintains a list of every user card or PIN that has ever been assigned. The Add Cards window defines:

- The type of reader needed to read the card
- The number of cards to create

To Define Cards:

1. In the Tree View, select **Cards**.
2. On the toolbar, click the **New** icon.

   The *Add Cards* window appears.

Figure 83: Add Cards Window

3. From the **Reader Type** list, select the type of reader appropriate for the cards being enrolled.
4. In the **Cards Quantity** field, type the number of cards to add.
5. Type the number of the first card in the set in the **Start From** field.
6. Set the **Facility Code** as required, and then click **OK**.

   A dialog reports that the operation has been completed.

7.15 Defining Departments and Users

Every user is grouped within a department. The ExpansE web based application stores contact details for each user, associated card details, and user access rights.

The User Properties window has three tabs:

- General tab displays identification and control information
- Details tab records user contact details
- Codes tab displays information about cards associated with the user

To create departments:

1. In the tree view, expand the Departments Visitors element and select Departments.

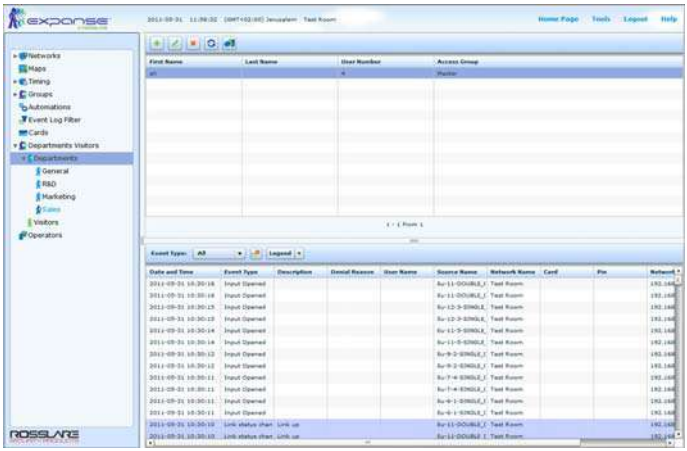


Figure 84: Departments / Users / Visitors Window

2. To create a new Department, click the **New** icon.

   The **Department** dialog appears.

Figure 85: Department Dialog

3. Type a name for the department, and then click **OK**.

To create users:

1. In the tree view, expand the Departments Visitors element.
2. Select a department and click the **New** icon.

   The User Properties window appears in the general tab.

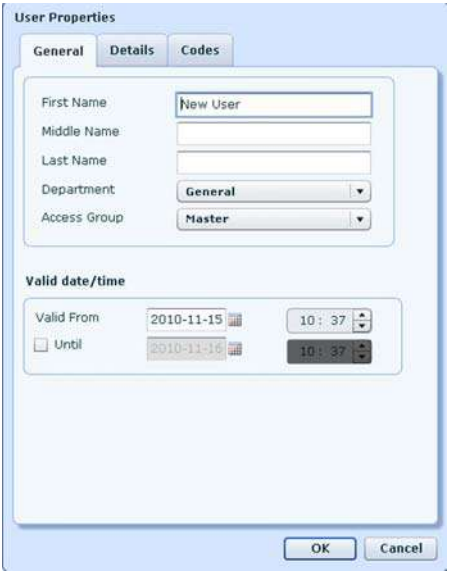


Figure 86: User Properties Window – General Tab

3. Type the user's first name in the **First Name** field.
4. Type the user's middle name in the **Middle Name** field.
5. Type the user's last name in the **Last Name** field.
6. From the **Department** Select box, associate the user to one of the departments you created
7. From the **Access Group** Select box, associate the user to an access group.
8. Set the access validity date and time. For limited access right, check the **Until** checkbox and set the final date and time.
9. Click the **Details** tab to continue.

Figure 87: User Properties Window – Details Tab

10. Set the Automation options:
    - Select an output group previously created from the **User Selected Output Group** select box.
    - Select an Elevator group previously created from the **Elevator Group** select box.
    - Check the **Access Granted Command** or **Access Denied Command** checkboxes to set the command activation method.
    - Check the **Handicapped** checkbox, to set handicapped privileges.
11. Set the counter options:
    - Check the **Enable Counter** checkbox to activate.
    - Check the **Set New Counter** checkbox to reset.
12. Set the access right options:
    - Check the **Antipassback Immunity** checkbox, to override any antipassback restrictions for this user.
    - Check the **Extended door open time** checkbox, to allow this user extended unlocked door duration. The extended duration is set for each door.
13. Click the **Codes** tab to continue.

Figure 88: User Properties Window – Codes Tab

14. Set the card associated to the user, you have one of several options to do so:
    - Click the **Add From List** button to select a card already added to the system.
    - Select a card from the list shown and click the **Remove** button to remove the card associated to the user.
    - Click the **Add Manually** button to type the card number then click the **Add From List** button to associate it with the user.
15. Define one or two PIN codes associated with the user:
    - Define the length of the PIN for this user, type or use the arrows in the **Digits** text box.
    - Type a PIN number based on the length defined in one or both of the **Code** text boxes.
    - Click the Auto Pin button to automatically generate a random PIN.
16. Click **OK** to save your settings.

7.16 Defining Visitors

The ExpansE web based application stores details for each visitor, associated card, and visitor access rights.

To create visitors:

1. Expand the **Departments Visitors** element, and select **Visitors**.
2. On the toolbar, click the **New** icon. The User Properties – visitor window open in the General tab.

Figure 89: User Properties Visitor Window – General Tab

3. Type the visitor's first name in the **First Name** field.
4. Type the visitor's middle name in the **Middle Name** field.
5. Type the visitor's last name in the **Last Name** field.
6. From the **Access Group** Select box, associate the visitor to an access group.
7. Set the access validity date and time. For limited access right, check the **Until** checkbox and set the final date and time.
8. Click the **Details** tab to continue.

Figure 90: User Properties Visitor Window – Details Tab

9. Set the Automation options:
   - Select an output group previously created from the **User Selected Output Group** select box.
   - Select an Elevator group previously created from the **Elevator Group** select box.
   - Check the **Access Granted Command** or **Access Denied Command** checkboxes to set the command activation method.
   - Check the **Handicapped** checkbox, to set handicapped privileges.
10. Set the counter options:
    - Check the **Enable Counter** checkbox, to activate the counter.
    - Check the **Set New Counter** checkbox, to reset the counter.
11. Set the access right options:
    - Check the **Antipassback Immunity** checkbox, to override any antipassback restrictions for this visitor.
    - Check the **Extended door open time** checkbox, to allow this user extended unlocked door duration. The extended duration is set for each door.

12. Click the **Codes** tab to continue.

Figure 91: User Properties Visitor Window – Codes Tab

13. Set the card associated to the visitor, you have one of several options to do so:
    - Click the **Add From List** button to select a card already added to the system.
    - Select a card from the list shown and click the **Remove** button to remove the card associated to the visitor.
    - Click the **Add Manually** button to type the card number then click the **Add From List** button to associate it with the visitor.
14. Define one or two PIN codes associated with the visitor:
    - Define the length of the PIN for this visitor, type or use the arrows in the **Digits** text box.
    - Type a PIN number based on the length defined in one or both of the **Code** text boxes.
    - Click the Auto Pin button to automatically generate a random PIN.
15. Click the **Visitor** tab to continue.

Figure 92: User Properties Visitor Window – Visitor Tab

16. Type an identification for the user in the **Visitor identification** field.
17. Select the department hosting the user from the Hosting department list, add a host from the Hosting User list.
18. Type any additional comments in the Comment field.
19. Set the access validity for the visitor by setting the validity date and time.
20. Click **OK** to save your settings.

7.17 Setting Event Log Filters

You can set which events are viewed in the event log view and which are not.

To set the event log filter:

1. In the tree view, select the Event Log Filter option.
2. Click the **New** icon.

   The Event filter window opens

Figure 93: Even Filter Window

3. In the **Description** field, type a name for the event filter rule.
4. Select the devices associated with the event filter rule from the *Selected Devices* section. Click **Select All** to add all of the devices. Click **Select None** to deselect all of the devices selected.
5. Select the source type from the **Source Type** list.
6. Select which events will NOT appear in the log file nor be saved in the system by checking the checkbox next to each event.
7. Check the Enabled checkbox to activate the filter.
8. Click **OK** to save your settings.

7.18 Defining Operators

Operators are people with access to the ExpansE web application. The default operator name is administrator.

Different operators have wider or more restricted security rights, from complete control over the system to the ability only to view one section. All Operator passwords are case-sensitive.

To define operators:

1. In the tree view, select the Operator option.
2. Click the **New** icon.

   The Operator Properties window opens

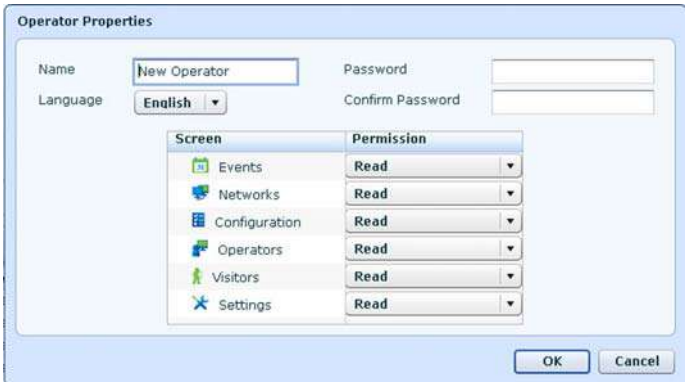


Figure 94: Operator Properties Window – New

3. Type the Operator's name in the **Name** Field.
4. Type the operators' password in the **Password** field, retype the password in the **Confirm Password** field to confirm it.
5. Set the user interface language for this operator using the **Language** select box
6. Set the operators permission rights for each of the screens.
7. Click **OK** to save your settings.

Note:
Up to one administrator can be logged in simultaneously.

8. Configuration Wizards

The ExpansE web based application has several wizards for quick and simple configuration the wizards can be accessed at any time from the application's home page.

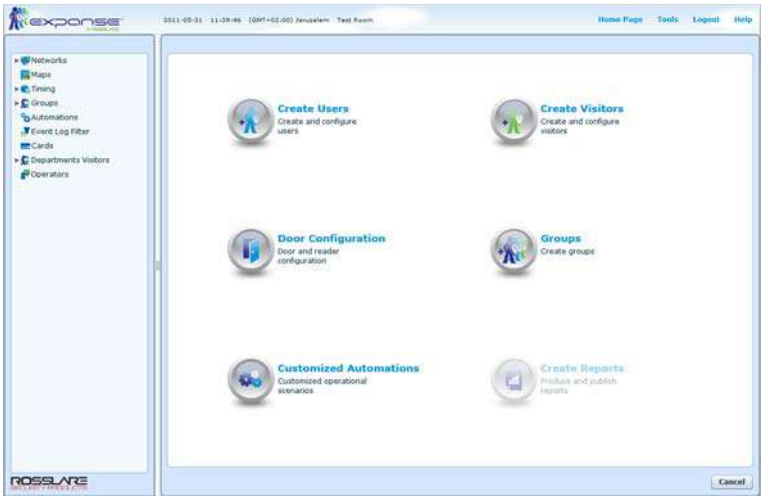


Figure 95: ExpansE Wizards

8.1 Customized Automation Wizard

This wizard guides you in the process of associating various input and reader events with various output actions to create automated activities.

To use the Automation Wizard:

1. From the ExpansE homepage click on the customized automation icon.

Figure 96: Customized Automation Wizard Icon

2. The customized automation welcome page appears.

Figure 97: Customized Automation Wizard Welcome Page

3. Type a name for the process in the automation description field and click **Next>** to continue. The Source page appears.

Figure 98: Customized Automation Wizard Source Page

4. Pick the source type from the **Source Type** list and click **Select**.
5. Select the name of the source to use from the **Source Name** list which will appear after selecting a source type.
6. Select the event initiating the automated activity from the **Source Event** List.
7. Click **Next>** to move on to the next step, the Destination page appears.

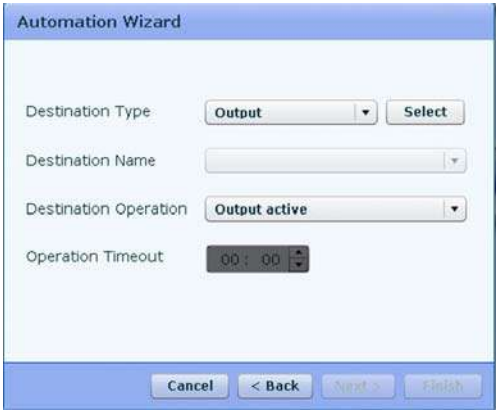


Figure 99: Customized Automation Wizard Destination Page

8. Pick the destination type from the **Destination Type** list and click **Select**.
9. Select the name of the destination to use from the **Destination Name** list which will appear after selecting a destination type.
10. Select the operation of the automated activity from the **Destination Operation** List.
11. Type the minutes and seconds in the **Operation Timeout** field or use the up and down arrows to set the a time frame for the operation timeout.
12. Click **Next>** to move on to the next step, the Activation page appears.

13. Select a time zone for this operation from the **Time Zone** list.
14. Check the **Enable** checkbox to enable the automated operation.
15. Click **Next>** to complete the wizard process. The Automation Wizard Complete page appears.

Figure 100: Automation Wizard Complete Page

16. Click **View Report** to open the automation report window.

Figure 101: Automation Wizard –Report Window

17. Click **OK** to close the window and return to the automation Wizard Complete page.
18. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

8.2 Create Users Wizard

The Create Users wizard guides you through the process of adding users, setting the user basic parameters, assigning a user to groups (if created, see Creating Access Groups, on page 79), assigning user departments and other credentials.

To use the user setup wizard:

1. From the ExpansE homepage click on the create user icon.

Figure 102: Create User Wizard Icon

Figure 103: User Wizard Welcome Page

2. The user wizard welcome page opens, click **Next>** to move on to the next step. The user details page opens.
3. Set the user details:
   - Type the user's first name in the **First Name** field, this field is mandatory.
   - Type the user's middle name in the **Middle Name** field if applicable.
   - Type the user's last name in the **Last Name** field.
   - From the **Department** Select box, associate the user to one of the departments you created

- From the **Access Group** Select box, associate the user to one of the access groups you created

Figure 104: User Wizard – User Details Page

4. Click **Next>** to move on to the next step, the Access Validity page opens.
5. Set the access validity date and time. For limited access right, check the **Until** checkbox and set the final date and time.

Figure 105: User Wizard – Validity Page

6. Click **Next>** to move on to the next step, the Automation page opens.

Figure 106: User Wizard – Automation Page

7. Set the Automation options:
   - Select an output group previously created from the **User Selected Output Group** select box.
   - Select an Elevator group previously created from the **Elevator Group** select box.
   - Check the **Access Granted Command** or **Access Denied Command** checkboxes to set the command activation method.
   - Check the **Handicapped** checkbox, to set handicapped privileges.
8. Click **Next>** to move on to the next step, the Access rights page opens.

Figure 107: User Wizard – Access Rights Page

9. Set the counter options:
   - Check the **Enable Counter** checkbox, to activate the counter.
   - Check the **Set New Counter** checkbox, to reset the counter.
10. Set the access right options:
    - Check the **Antipassback Immunity** checkbox, to override any antipassback restrictions for this user.
    - Check the **Extended door open time** checkbox, to allow this user extended unlocked door duration. The extended duration is set for each door.
11. Click **Next>** to move on to the next step, the card association page opens.

Figure 108: User Wizard – Card Association page

12. Set the card associated to the user, you have one of several options to do so:
    - Click the **Add From List** button to select a card already added to the system.
    - Select a card from the list shown and click the **Remove** button to remove the card associated to the user.
    - Click the **Add Manually** button to type the card number and associate it with the user.
13. Click **Next>** to move on to the next step, the PIN code association page opens.

Figure 109: User Wizard – PIN code association page

14. Define one or two PIN codes associated with the user:
    - Define the length of the PIN for this user, type or use the arrows in the **Digits** text box.
    - Type a PIN number based on the length defined in one or both of the **Code** text boxes.
    - Click the Auto Pin button to automatically generate a random PIN code.
15. Click **Next>** to complete the wizard process. The User Wizard Complete page opens.

Figure 110: User Wizard Complete Page

16. Click **View Report** to open the user report window.

Figure 111: User Wizard – User Report Window

17. Click **OK** to close the window and return to the User Wizard Complete page.
18. Click **Add new user** to return to step 3 and repeat the process for an additional user. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

8.3 Create Visitors Wizard

The Create Visitor wizard guides you through the process of adding users that are defined as visitors.

To use the visitor setup wizard:

1. From the ExpansE homepage click on the create visitor icon.

Figure 112: Create Visitor Wizard Icon

2. The Visitor wizard welcome page opens, click **Next>** to move on to the next step. The user details page opens.

Figure 113: Visitor Wizard Welcome Page

3. Set the user details:
   - Type the user's first name in the **First Name** field, this field is mandatory.
   - Type the user's middle name in the **Middle Name** field if applicable.
   - Type the user's last name in the **Last Name** field.
   - From the **Access Group** Select box, associate the user to one of the access groups you created

Figure 114: Visitor Wizard – Visitor's Details Page

4. Click **Next>** to move on to the next step, the Access Validity page opens.

5. Set the access validity date and time. Check the **Until** checkbox and set the final date and time for the visitor's access rights.

Figure 115: Visitor Wizard – Validity Page

6. Click **Next>** to move on to the next step, the Automation page opens.

Figure 116: Visitor Wizard – Automation Page

7. Set the Automation options:
   - Select an output group previously created from the **Output Group** select box.
   - Select an Elevator group previously created from the **Elevator Group** select box.

- Check the **Access Granted Command** or **Access Denied Command** checkboxes to set the command activation method.
- Check the **Handicapped** checkbox, to set handicapped privileges.

8. Click **Next>** to move on to the next step, the Access rights page opens.

Figure 117: Visitor Wizard – Access Rights Page

9. Set the counter options:
   - Check the **Enable Counter** checkbox, to activate the counter.
   - Check the **Set New Counter** checkbox, to reset the counter.
10. Set the access right options:
    - Check the **Antipassback Immunity** checkbox, to override any antipassback restrictions for this visitor.
    - Check the **Extended door open time** checkbox, to allow this visitor extended unlocked door duration. The extended duration is set for each door.
11. Click **Next>** to move on to the next step, the card association page opens.

Figure 118: Visitor Wizard – Card Association page

12. Set the card associated to the visitor, you have one of several options to do so:
    - Click the **Add From List** button to select a card already added to the system.
    - Select a card from the list shown and click the **Remove** button to remove the card associated to the visitor.
    - Click the **Add Manually** button to type the card number and associate it with the visitor.
13. Click **Next>** to move on to the next step, the PIN code association page opens.

Figure 119: Visitor Wizard – PIN code association page

14. Define one or two PIN codes associated with the visitor:
    - Define the length of the PIN for this visitor, type or use the arrows in the **Digits** text box.
    - Type a PIN number based on the length defined in one or both of the **Code** text boxes.
    - Click the Auto Pin button to automatically generate a random PIN code.
15. Click **Next>** to move on to the next step, the host association page opens.

Figure 120: Visitor Wizard – Host association page

16. Define the visitor's host details:
    - Type identification, such as a company name, for the visitor in the **Visitor identification** text box.
    - Select the department hosting the visitor from the **Hosting department** select box.
    - Select the user within the selected department hosting the visitor from the **Hosting user** select box.
    - Type comments if applicable in the **Comment** text box.
    - Check the **Until** checkbox and set the date and time for the conclusion of the scheduled visit.
17. Click **Next>** to complete the wizard process. The Visitor Wizard Complete page opens.

Figure 121: Visitor Wizard Complete Page

18. Click **View Report** to open the Visitor report window.
19. Click **OK** to close the window and return to the Visitor Wizard Complete page.
20. Click **Add New Visitor** to return to step 3 and repeat the process for an additional visitor. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

8.4 Doors Wizard

The doors wizard guides you through the process of adding doors to the system and configuring them.

To use the Doors wizard:

1. From the ExpansE homepage click on the doors icon.

Figure 122: Doors Wizard Icon

2. The Doors wizard welcome page opens, click **Next>** to move on to the next step. The door selection page opens.

Figure 123: Doors Wizard Welcome Page

3. Select the door EU you wish to define from the list of EUs under each MU.

Figure 124: Doors Wizard – Door Selection Page

4. Click **Next>** to move on to the next step, the Door Details page opens.

Figure 125: Doors Wizard – Door Details Page

5. Define the Door details:
   - Type a description for the selected door in the **Description** text box.
   - Determine the door polarity by checking or un-checking the **Door output polarity is Normally Closed** checkbox. Select this checkbox to ensure Fail Safe door opening if the Fail Safe door Lock Device power fails.
     Once enabled, the door output relay is activated when the door is closed, and is deactivated when the door is open.
     In this configuration, the Fail Safe lock device should be wired to the door relay N.O. (Normal Open) and COM (Common) terminals
   - Check the **REX enabled** checkbox to allow Requests to Exit for this door.
   - Check the **Manual Door Open Enabled** checkbox to allow operators to adjust the door manually. See Manual Door Control under Manual Operation, on page 127.
   - Select the **Timezone Logic** checkbox to initiate the time zone logic options and select the desired output from the list.
   - Check the **First person Delay** checkbox to keep the door locked until the first user opens it.
6. Click **Next>** to move on to the next step, the Door Timers page opens.

Figure 126: Doors Wizard – Door Timers Page

7. Define the various timers for the doors:
   - Set the duration for which the door stays unlocked by typing minutes and seconds in the **Door open time** field or use the associated up and down arrows.
   - Set the duration for which the door stays unlocked for users with Extended door open rights by typing minutes and seconds in the **Extended Door open time** field or use the associated up and down arrows.
   - Set the duration following which and when the door is forced open, an event occurs. Select the **Door forced** checkbox to use this timer and type the minutes and seconds in the associated field or use the up and down arrows.
   - Set the duration for which the door can be held open without raising an alarm event. Select the **Door held open** checkbox to use this timer and type the minutes and seconds in the associated field or use the up/down arrows.
8. Click **Next>** to move on to the next step, the Reader Properties page opens.

Figure 127: Doors Wizard – Reader Properties Page

9. Define the reader properties associated with the door:
   - In the **Description** field, type a name for the reader.
   - Select whether the reader is allowing entry into the area or exit out of the area by selecting either the **In** or **Out** option.
   - From the Operation Mode list Select how the reader operates:
     - **Inactive:** The reader is not in use.
     - **Card Only:** The reader will accept RFID cards only.
     - **PIN Only:** The reader will accept PIN inputs only.
     - **Card or PIN:** The reader will accept both cards and PIN codes.
     - **Desktop:** The reader is inactive, but is being used to record new cards on the computer.
     - **No Access Mode:** The reader will grant access to no users.
   - Using the **Secured (Card+PIN) time zone** list select a time zone during which access should be granted only after both the card and PIN are entered.
     The PIN must be entered within 10 seconds of card entry.
   - From the **Keypad Type** list, select the data transmission type for the type of keypad hardware.
   - From the **Reader Type** list, select the data transmission type for the reader hardware.

- Check the **Open Door Activation** checkbox to allow the reader to unlock the door.
- Check the **Deduct User Counter** checkbox to record this entry against the user's entry allowance counter.

10. Click **Next>** to complete the wizard process. The Door Wizard Complete page opens.

Figure 128: Door Wizard Complete Page

11. Click **View Report** to open the door report window.

Figure 129: Door Wizard – Report Window

12. Click **OK** to close the window and return to the Door Wizard Complete page.
13. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

8.5 Groups Wizard

The Groups wizard guides you through the process of creating the various available groups in the system: Access groups, Input Groups, Output Groups, and Elevator groups.

Access Groups

This section describes the use of the Groups wizard when creating Access Groups.

To create access groups using the Groups wizard:

1. From the ExpansE homepage click on the groups icon.

Figure 130: Groups Wizard Icon

2. The Groups wizard welcome page opens, choose Access Groups from the **Select Group** select box.

Figure 131: Groups Wizard Welcome Page

3. Click **Next>** to move on to the next step. The Access group definition page opens.

Figure 132: Groups Wizard – Access Group Definition Page

4. In the **Description** field, type a name for the access group.
5. From the *Readers List* select the readers you wish to associate with this group and click **Add**.
6. For each of the readers select a time zone association.
7. Select a reader and then click **Remove** to remove the readers from the association list.
8. Click **Next>** to complete the wizard process. The Groups Wizard Complete page opens.

Figure 133: Groups Wizard Complete Page

9. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

Input Groups

This section describes the use of the Groups wizard when creating Input Groups.

To create input groups using the Groups wizard:

1. From the ExpansE homepage click on the groups icon.

Figure 134: Groups Wizard Icon

2. The Groups wizard welcome page opens, choose Input Groups from the **Select Group** select box.

Figure 135: Groups Wizard Welcome Page

3. Click **Next>** to move on to the next step. The Input group definition page opens.

Figure 136: Groups Wizard – Input Group Definition Page

4. In the **Description** field, type a name for the input group.
5. Within *Select inputs* check all the inputs you wish to add.
6. Click **Select All** to add all of the inputs shown.
7. Click **Select None** to deselect all of the inputs selected.
8. Click **Next>** to complete the wizard process. The Groups Wizard Complete page opens.

Figure 137: Groups Wizard Complete Page

9. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

Output Groups

This section describes the use of the Groups wizard when creating Output Groups.

To create output groups using the Groups wizard:

1. From the ExpansE homepage click on the groups icon.

Figure 138: Groups Wizard Icon

2. The Groups wizard welcome page opens, choose Output Groups from the **Select Group** select box.

Figure 139: Groups Wizard Welcome Page

3. Click **Next>** to move on to the next step. The Output group definition page opens.

Figure 140: Groups Wizard – Output Group Definition Page

4. In the **Description** field, type a name for the output group.

5. Within *Select outputs* check all the inputs you wish to add.
6. Click **Select All** to add all of the output shown.
7. Click **Select None** to deselect all of the outputs selected.
8. Click **Next>** to complete the wizard process. The Groups Wizard Complete page opens.

Figure 141: Groups Wizard Complete Page

9. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

Elevators Groups

This section describes the use of the Groups wizard when creating Elevators Groups.

To create elevators groups using the Groups wizard:

1. From the ExpansE homepage click on the groups icon.

Figure 142: Groups Wizard Icon

2. The Groups wizard welcome page opens, choose Elevators Groups from the **Select Group** select box.

Figure 143: Groups Wizard Welcome Page

3. Click **Next>** to move on to the next step. The Elevators group definition page opens.

Figure 144: Groups Wizard – Output Group Definition Page

4. In the **Description** field, type a name for the elevator group.
5. Within *Reader List* select and click **Add** for all the readers you wish to add to the group.
6. For each reader:
   - Select a time zone association from the **Timezone** select box.
   - Select the associated output group from the **Output Group** select box.
7. Select a reader and then click **Remove** to remove the readers from the association list.
8. Click **Next>** to complete the wizard process. The Groups Wizard Complete page opens.

Figure 145: Groups Wizard Complete Page

9. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

9. Manual Operation

In addition to automated monitoring and control of the access control network, it is also possible to control the network directly from the ExpansE web based application.

9.1 Manual Door Control

The Door Manual Operation window allows an operator to open or close a selected group of doors directly.

To manually open or close a door:

1. On the toolbar, click the **Open Door Manually** icon.

   The Door Manual Operation window opens.

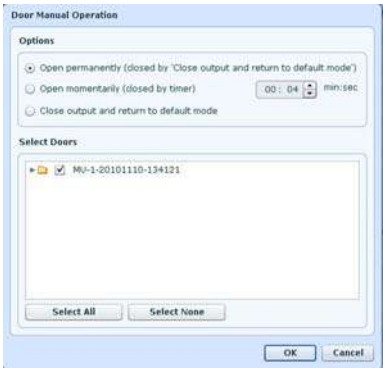


Figure 146: Door Manual Operation window

2. Select an option:
   - **Open permanently -** All selected doors are opened.
   - **Open momentarily -** All selected doors are opened for the time set in the timer box.
   - **Close output -** Close the selected doors and return to default mode.
3. Select the checkboxes of those doors to which to apply the operation.

   Click **OK** to perform the operation.

Note:
Door Manual Operation can only control doors that have been set as Manual Door Open Enabled in the Door Properties window.

10. ExClouds PC Set-Up

This section refers to the ExClouds software required for reports production. For more on this software contact your dealer.

10.1 Minimum Requirements

- Supported Operating Systems;
  - Windows XP SP3
  - Windows Server 2003 SP2
  - Windows Vista SP1 or later
  - Windows Server 2008 (not supported on Server Core Role)
  - Windows 7
  - Windows Server 2008 R2 (not supported on Server Core Role)
- Supported Architectures:
  - x86
  - x64
  - ia64 (some features are not supported on ia64 for example, WPF)
- Hardware Requirements:
  - Recommended Minimum: Pentium 1 GHz or higher with 512 MB RAM or more
  - Minimum disk space:
    - x86 – 850 MB
    - x64 – 2 GB

10.2 ExClouds Software Installation

The ExClouds installation is done in two steps, first install the actual ExClouds software followed by the report module as described in detail in this chapter.

To install the ExClouds Software:

1. Locate the ExClouds Setup.exe file in the CD provided or in the folder where you saved the installation package you received from Rosslare and run it. The Welcome screen appears.

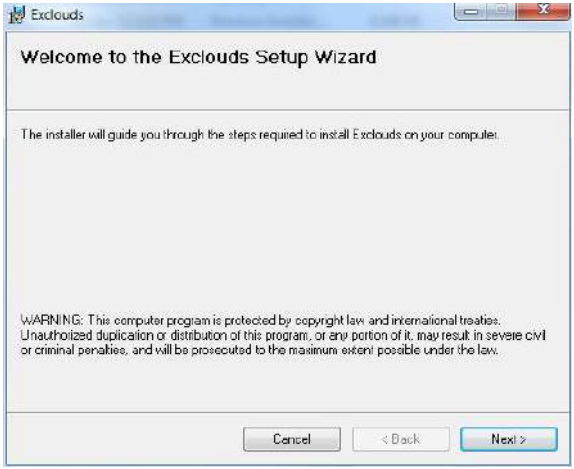


Figure 147: ExClouds Setup wizard welcome screen

2. Click **Next >** to begin the installation. The *Select Installation Folder* window appears.

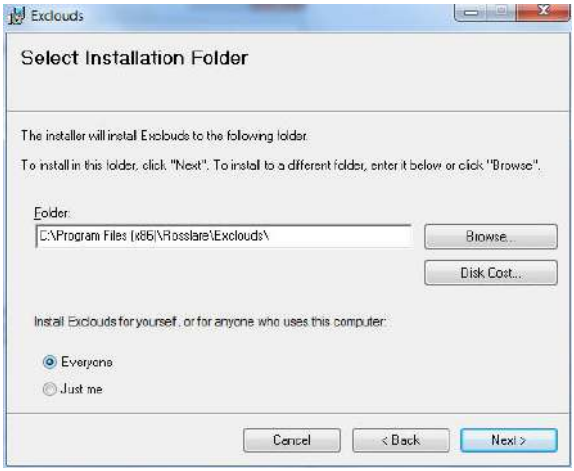


Figure 148: ExClouds Select installation folder screen

3. Type the installation location in the **Folder** field. Alternatively use the **browse…** button to select the location. Use the **Disk Cost...** button to show available space on your computer

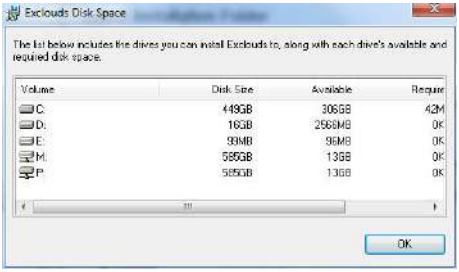


Figure 149: ExClouds Disk Space screen

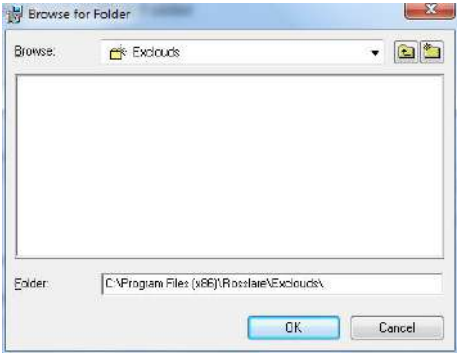


Figure 150: ExClouds Browse for Folder screen

4. Select the availability of the software to users using the computer between **Everyone** or **Just me**, and click **Next >** to continue. The *Confirm Installation* window appears.

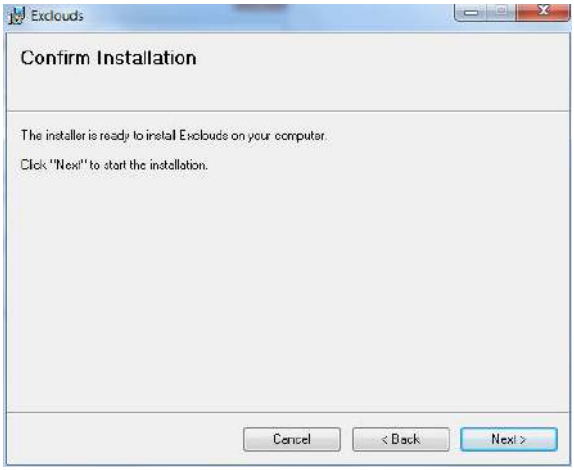


Figure 151: ExClouds *Confirm Installation* screen

5. Click **Next >** to confirm the installation and to initiate the installation process. The *Installing ExClouds* window appears. Once the progress bar indicating the installation process is complete, the *Installation Complete* window will appear automatically.

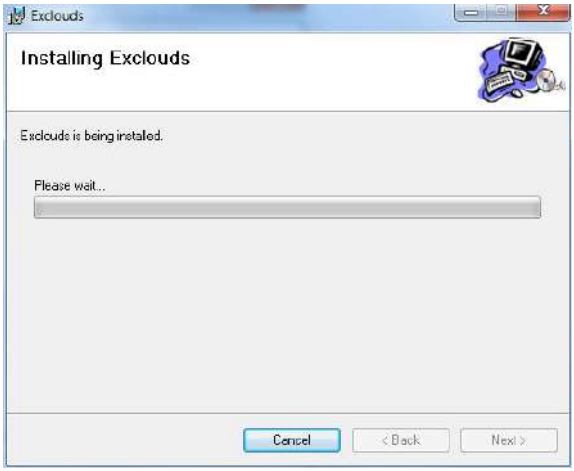


Figure 152: ExClouds *Installing ExClouds* screen

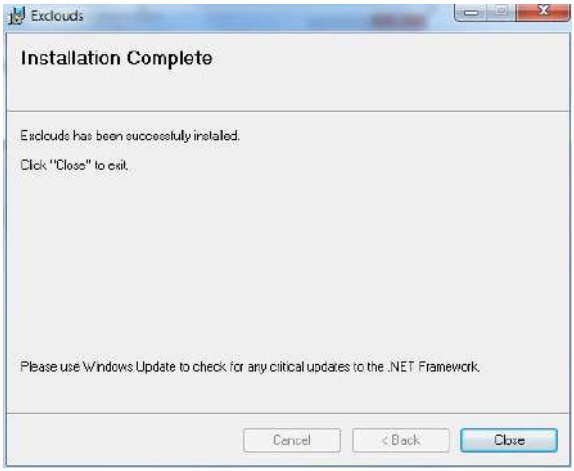


Figure 153: ExClouds *Installation Complete* screen

6. Click **Close** to exit the installation setup.
7. Locate the CRRedist2008_x86.msi file in the same location as the setup file and run it. The software will install

automatically. Once complete the installation window will close automatically.

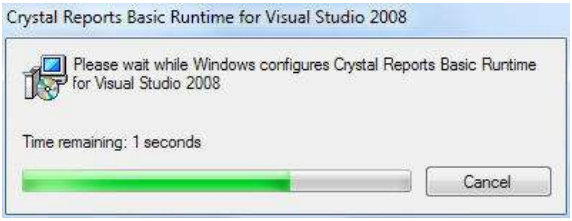


Figure 154: Reporting Software Installation

10.3 ExClouds Setup

This section shows how to start the ExClouds software and how to configure it to work with the ExpansE web application.

To configure the ExClouds software:

1. Click the ExClouds icon  from either the desktop or the start menu. The ExClouds software login screen opens.

Figure 155: ExClouds *Login* screen

2. Enter your password and click **Login**. The default password is *admin*.
3. Enter your password and click **Login**. The default password is *admin*. The ExClouds main window opens

Figure 156: ExClouds *Main Window*

4. Click the **Settings** Icon, the *Option* window opens

Figure 157: ExClouds *Option Window*

5. Define the Host ExpansE system by entering the ExpansE's IP in address In the **Host** field.
6. Enter the ExpansE's user name in the **Username** field
7. Enter ExpansE's password corresponding with the user name entered in the and **Password** field
8. Define the ExClouds password in the **Login Password** and **Confirm Password** fields and click **Save**.
9. Open the *Database Option* window by clicking the **Database** icon

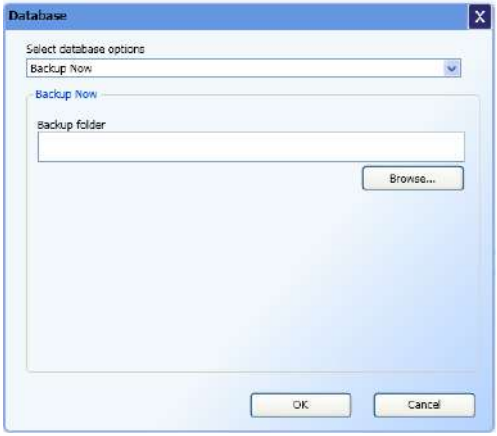


Figure 158: ExClouds *Database Option Window*

10. Choose between uploading the Database and backing up the existing database if the system is already configured and running.
11. You can initiate the various reports directly from the ExClouds software by selecting the desired report from the tree view on the left. See the various report options and complete instruction on each report in chapter 11 Reports Wizard, on page 135.

11. Reports Wizard

In order to create reports or run the reports wizard the ExClouds software needs to be installed.

First time users please refer to Chapter 10 ExClouds PC Set-Up, on page 128, before attempting to run the reports wizard.

11.1 Initiating the Report Wizard

The Report wizard guides you through the process of creating various reports from the ExpansE web application as described in detailed in this chapter.

To initiate the report wizard:

1. Click the ExClouds icon  from either the desktop or the start menu. The ExClouds software login screen opens.

Figure 159: ExClouds *Login* screen

2. Enter your password and click **Login**. The default password is *admin*. The ExClouds main window opens with the optional reports open on the left.

Figure 160: ExClouds main window with report option open

3. Select the desired report and follow the wizard steps as described in detail in the following sections.

11.2 Creating Roll Call Reader Report

A roll call reader report generates a report showing access granted events for specific readers based on specific times.

To create a roll call reader report:

1. Initiate the reports wizard as described in Initiating the Report Wizard, on page 135.
2. Select the **Roll Call Readers Report** located under **Live Report**. The *Roll Call Readers* Welcome screen opens.

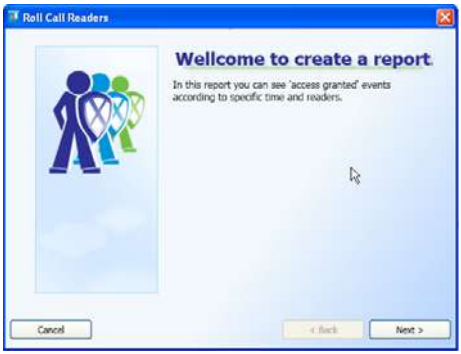


Figure 161: Roll Call Readers Wizard – Welcome screen

3. Click **Next>** to start defining the report options. The *Parameter* screen opens.

Figure 162: Roll Call Readers Wizard – Parameter screen

4. In the parameter screen select the readers desired for the report from the list of available readers on the left and click **Add**. You can also use the **Add All** button to select all of the readers available.

   To remove readers from the selection list, select the reader from the list on the right, to remove from the report and click **Remove** alternatively you can click the **Remove All** button to remove the entire list of readers.
5. Define the number of days you wish to view in the report by typing the number in the **Days** field or using the scroll-bar.

   Check the Hours option to define a specific number of hours, then type the number in the **Hours** field or use the scroll-bar.
6. Click **Next>** to define the look of the report in the report design template screen.

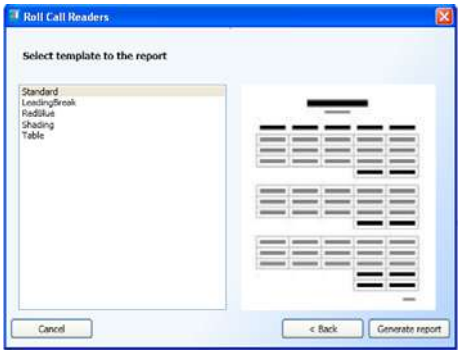


Figure 163: Reports wizard – Report Design Template screen

7. Select the desired report template from the list of available templates, a preview will appear on the right.
8. Click the **Generate Report** button to issue the report.

11.3 Creating Last Known Position Report

The last known position report creates a report showing the last valid entry for all of the users in the system for the last day.

To create a last known position report:

1. Initiate the reports wizard as described in Initiating the Report Wizard, on page 135.
2. Select the **Last Known Position Report** located under **Live Report**. The *Last Known Position* Welcome screen opens.

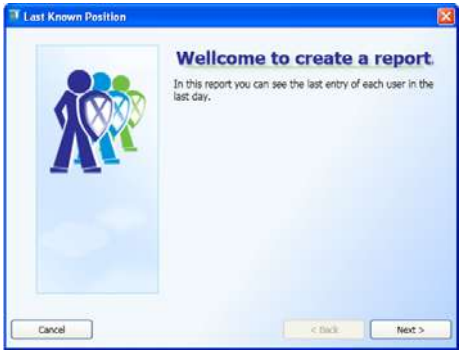


Figure 164: Roll Call Readers Wizard – Welcome screen

3. Click **Next>** to define the look of the report in the report design template screen, see Figure 163: Reports wizard – Report Design Template screen, on page 137.
4. Select the desired report template from the list of available templates, a preview will appear on the right.
5. Click the **Generate Report** button to issue the report.

11.4 Creating System Report

The system report is the most detailed report available, it shows various (or all) events for selected devices based on event types and specified time frames.

To create a system report:

1. Initiate the reports wizard as described in Initiating the Report Wizard, on page 135.
2. Select the **System Report** located under **Interactive Report**. The *System Report* Welcome screen opens.

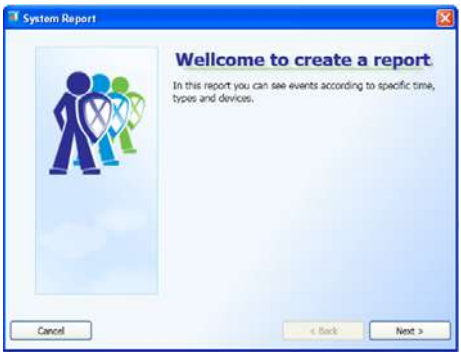


Figure 165: System Report Wizard – Welcome screen

3. Click **Next>** to start defining the report options. The *Device Selection Screen* opens

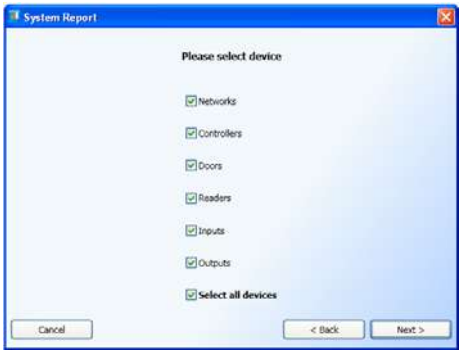


Figure 166: System Report Wizard – Device Selection screen

4. Select the devices you wish to include in the report by checking or un-checking the box adjacent to each of the available devices. Alternatively check the Select all devices option.

   The available devices are: Networks, Controllers, Doors, Readers, Inputs and outputs.

5. Click **Next>** to continue. The *Event Selection Screen* opens.

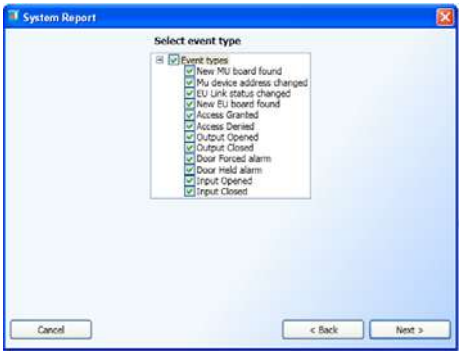


Figure 167: System Report Wizard – Event Selection screen

6. Select the events you wish to include in the report by checking or un-checking the box adjacent to each of the available events.
7. Click **Next>** to continue. The *Network and Controller Selection Screen* opens.

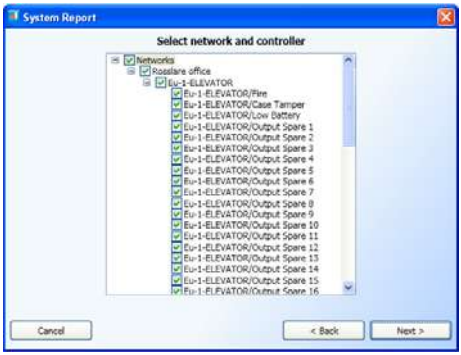


Figure 168: System Report Wizard – Network & Controller Selection

8. Select the networks and/or controllers you wish to include in the report by checking or un-checking the box adjacent to each of the available controllers or networks.
9. Click **Next>** to continue. The *Producing period Screen* opens.

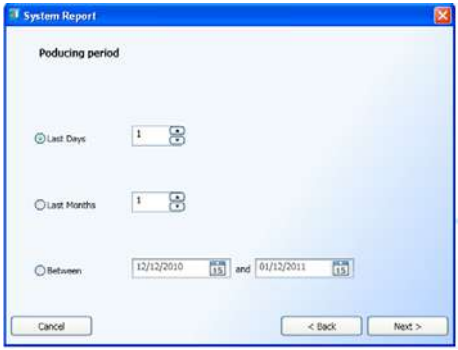


Figure 169: System Report Wizard – Producing period screen

10. Select the desired time frame for the report by either selecting a number of days, the number of months or a time frame based on actual dates.
11. Click **Next>** to continue. The *Report save option Screen* opens.

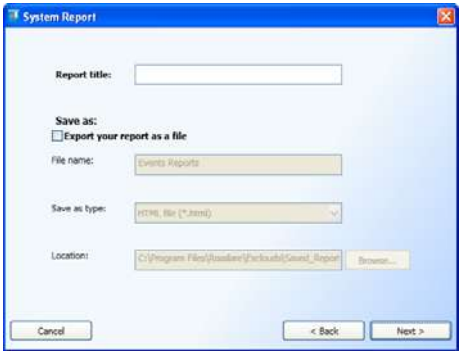


Figure 170: System Report Wizard – Report save option screen

12. In the **Report title** field type a name for the report for easier location and retrival.
13. To save the report as a file, check the **Export your report as file** option. Give the file a name by typing it into the **File name:** field, select the type of file you wish to save from the **Save as type:** file option list, and enter or **Browse** the file **Location**.

14. Click **Next>** to define the look of the report in the report design template screen, see Figure 163: Reports wizard – Report Design Template screen, on page 137.
15. Select the desired report template from the list of available templates, a preview will appear on the right.
16. Click the **Generate Report** button to issue the report.

11.5 Creating an Attendance Report

The attendance report is the most commonly report used; it allows the creation of time & attendance reports defined by readers, users and specific time frames.

To create an attendance report:

1. Initiate the reports wizard as described in Initiating the Report Wizard, on page 135.
2. Select the **Attendance Report** located under **Interactive Report**. The *Attendance Report* Welcome screen opens.

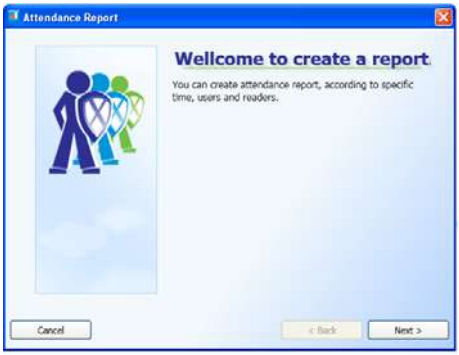


Figure 171: Attendance Report Wizard – Welcome screen

3. Click **Next>** to start defining the report options. The *User Selection Screen* opens

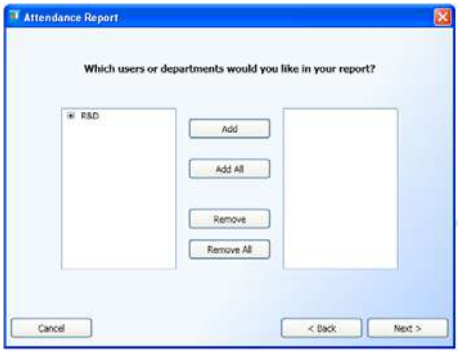


Figure 172: Attendance Report Wizard – User Selection screen

4. In the user selection screen select the departments or specific users for the attendance report from the list of available departments and users on the left and click **Add**. You can also use the **Add All** button to select all of the users.

   To remove users or entire departments from the selection list, select a line from the list on the right, and click **Remove** alternatively you can click the **Remove All** button to remove the entire list of users.
5. Click **Next>** to continue. The *Reader Selection Screen* opens

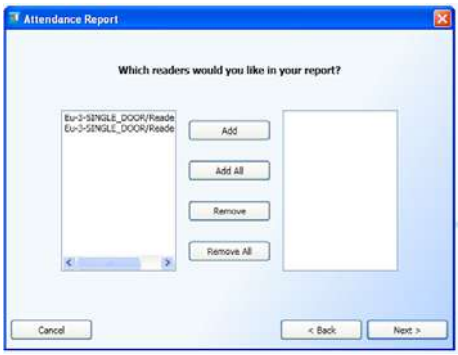


Figure 173: Attendance Report Wizard – Reader Selection screen

6. Select the readers associated with the desired report from the list of available readers on the left and click **Add**. You can also use the **Add All** button to select all of the readers available.

To remove readers from the selection list, select the reader from the list on the right, and click **Remove,** alternatively you can click the **Remove All** button to remove the entire list of readers.

7. Click **Next>** to continue. The *Time & attendace option Screen* opens

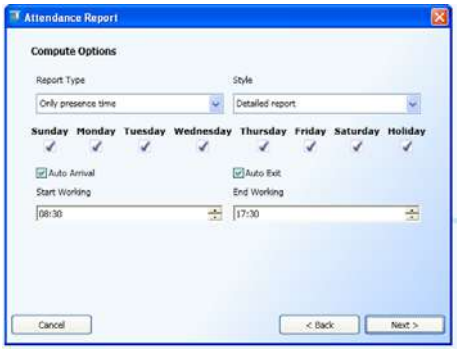


Figure 174: Attendance Report Wizard – T&A Options screen

8. define the various partameters for the time & attendance report.

   Select the **Report Type** , the report **Style**, and the relevant days for the report. Define the normal working hours using the **Start Working** and **End Working** select boxes, you can also define Automatic entry and exit in case of missing information by checking the **Auto Arrival** and **Auto Exit** checkboxes respectively.

9. Click **Next>** to continue. The *Producing period Screen* opens.

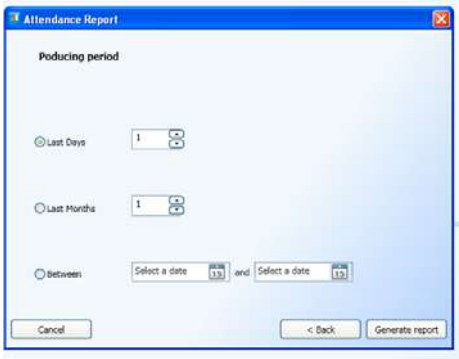


Figure 175: Attendance Report Wizard – Producing period screen

10. Select the desired time frame for the report by either selecting a number of days, the number of months or a time frame based on actual dates.
11. Click **Next>** to continue. The *Report save option Screen* opens.

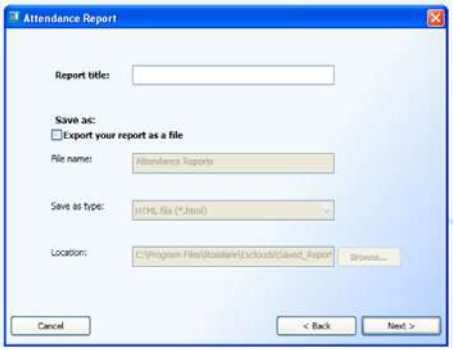


Figure 176: Attendance Report Wizard – Report save option screen

12. In the **Report title** field type a name for the report for easier location and retrival.
13. To save the report as a file, check the **Export your report as file** option. Give the file a name by typing it into the **File name:** field, select the type of file you wish to save from the **Save as type:** file option list, and enter or **Browse** the file **Location**.

14. Click **Next>** to define the look of the report in the report design template screen, see Figure 163: Reports wizard – Report Design Template screen, on page 137.
15. Select the desired report template from the list of available templates, a preview will appear on the right.
16. Click the **Generate Report** button to issue the report.

Appendix A. Limited Warranty

ROSSLARE ENTERPRISES LIMITED S (Rosslare) TWO YEARS LIMITED WARRANTY is applicable worldwide. This warranty supersedes any other warranty. Rosslare's TWO YEARS LIMITED WARRANTY is subject to the following conditions:

Warranty

Warranty of Rosslare's products extends to the original purchaser (Customer) of the Rosslare product and is not transferable.

Products Covered By This Warranty and Duration

ROSSLARE ENTERPRISES LTD. AND / OR SUBSIDIARIES (ROSSLARE) warrants that the EXPANSE Access Control system, to be free from defects in materials and assembly in the course of normal use and service. The warranty period commences with the date of shipment to the original purchaser and extends for a period of 2 years (24 Months).

Warranty Remedy Coverage

In the event of a breach of warranty, ROSSLARE will credit Customer with the price of the Product paid by Customer, provided that the warranty claim is delivered to ROSSLARE by the Customer during the warranty period in accordance with the terms of this warranty. Unless otherwise requested by ROSSLARE ENTERPRISES LTD. AND / OR SUBSIDIARIES representative, return of the failed product(s) is not immediately required.

If ROSSLARE has not contacted the Customer within a sixty (60) day holding period following the delivery of the warranty claim, Customer will not be required to return the failed product(s). All returned Product(s), as may be requested at ROSSLARE ENTERPRISES LTD. AND /OR SUBSIDIARY'S sole discretion, shall become the property of ROSSLARE ENTERPRISES LTD. AND /OR SUBSIDIARIES.

To exercise the warranty, the user must contact Rosslare Enterprises Ltd. to obtain an RMA number after which, the product must be returned to the Manufacturer freight prepaid and insured

In the event ROSSLARE chooses to perform a product evaluation within the sixty (60) day holding period and no defect is found, a minimum US$ 50.00 or equivalent charge will be applied to each Product for labor required in the evaluation.

Rosslare will repair or replace, at its discretion, any product that under normal conditions of use and service proves to be defective in material or workmanship. No charge will be applied for labor or parts with respect to defects covered by this warranty, provided that the work is done by Rosslare or a Rosslare authorized service center.

Exclusions and Limitations

ROSSLARE shall not be responsible or liable for any damage or loss resulting from the operation or performance of any Product or any systems in which a Product is incorporated. This warranty shall not extend to any ancillary equipment not furnished by ROSSLARE, which is attached to or used in conjunction with a Product, nor to any Product that is used with any ancillary equipment, which is not furnished by ROSSLARE.

This warranty does not cover expenses incurred in the transportation, freight cost to the repair center, removal or reinstallation of the product, whether or not proven defective.

Specifically excluded from this warranty are any failures resulting from Customer's improper testing, operation, installation, or damage resulting from use of the Product in other than its normal and customary manner, or any maintenance, modification, alteration, or adjustment or any type of abuse, neglect, accident, misuse, improper operation, normal wear, defects or damage due to lightning or other electrical discharge. This warranty does not cover repair or replacement where normal use has exhausted the life of a part or instrument, or any modification or abuse of, or tampering with, the Product if Product disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection and testing to verify any warranty claim.

ROSSLARE does not warrant the installation, maintenance, or service of the Product. Service life of the product is dependent upon the care it receives and the conditions under which it has to operate.

In no event shall Rosslare be liable for incidental or consequential damages.

Limited Warranty Terms

THIS WARRANTY SETS FORTH THE FULL EXTENT OF ROSSLARE ENTERPRISES LTD. AND IT'S SUBSIDIARIES' WARRANTY

THE TERMS OF THIS WARRANTY MAY NOT BE VARIED BY ANY PERSON, WHETHER OR NOT PURPORTING TO REPRESENT OR ACT ON BEHALF OF ROSSLARE.

THIS LIMITED WARRANTY IS PROVIDED IN LIEU OF ALL OTHER WARRANTIES. ALL OTHER WARRANTIES EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE SPECIFICALLY EXCLUDED.

IN NO EVENT SHALL ROSSLARE BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, OR FOR ANY OTHER INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF USE, LOSS OF TIME, COMMERCIAL LOSS, INCONVENIENCE, AND LOSS OF PROFITS, ARISING OUT OF THE INSTALLATION, USE, OR INABILITY TO USE SUCH PRODUCT, TO THE FULLEST EXTENT THAT ANY SUCH LOSS OR DAMAGE MAY BE DISCLAIMED BY LAW.

THIS WARRANTY SHALL BECOME NULL AND VOID IN THE EVENT OF A VIOLATION OF THE PROVISIONS OF THIS LIMITED WARRANTY.

Appendix B. Technical Support

Asia Pacific, Middle East, Africa

Rosslare Security Products Headquarters
905-912 Wing Fat Industrial Bldg,
12 Wang Tai Road,
Kowloon Bay Hong Kong
Tel: +852 2795-5630
Fax: +852 2795-1508
E-mail: support.apac@rosslaresecurity.com

United States and Canada

1600 Hart Court, Suite 103
Southlake, TX, USA 76092
Toll Free:+1-866-632-1101
Local:+1-817-305-0006
Fax: +1-817-305-0069
E-mail: support.na@rosslaresecurity.com

Europe

Global Technical Support & Training Center
HaMelecha 22
Rosh HaAyin, Israel 48091
Tel: +972 3 938-6838
Fax: +972 3 938-6830
E-mail: support.eu@rosslaresecurity.com

South America

Presbitero Actis 555, Oficina 31.
San Isidro. Buenos Aires. Argentina
Tel: +5411-5273-6383
Tel: +305-921-9919
E-mail: support.la@rosslaresecurity.com

Web Site: www.rosslaresecurity.com

ROSSLARE
SECURITY PRODUCTS

www.rosslaresecurity.com

0706-0960230+00

TÜVRheinland®
ISO 9001:2008
Cert. No. 01 100 6925
ISO 14001:2004
Cert. No. 01 104 6925

RoHS COMPLIANT