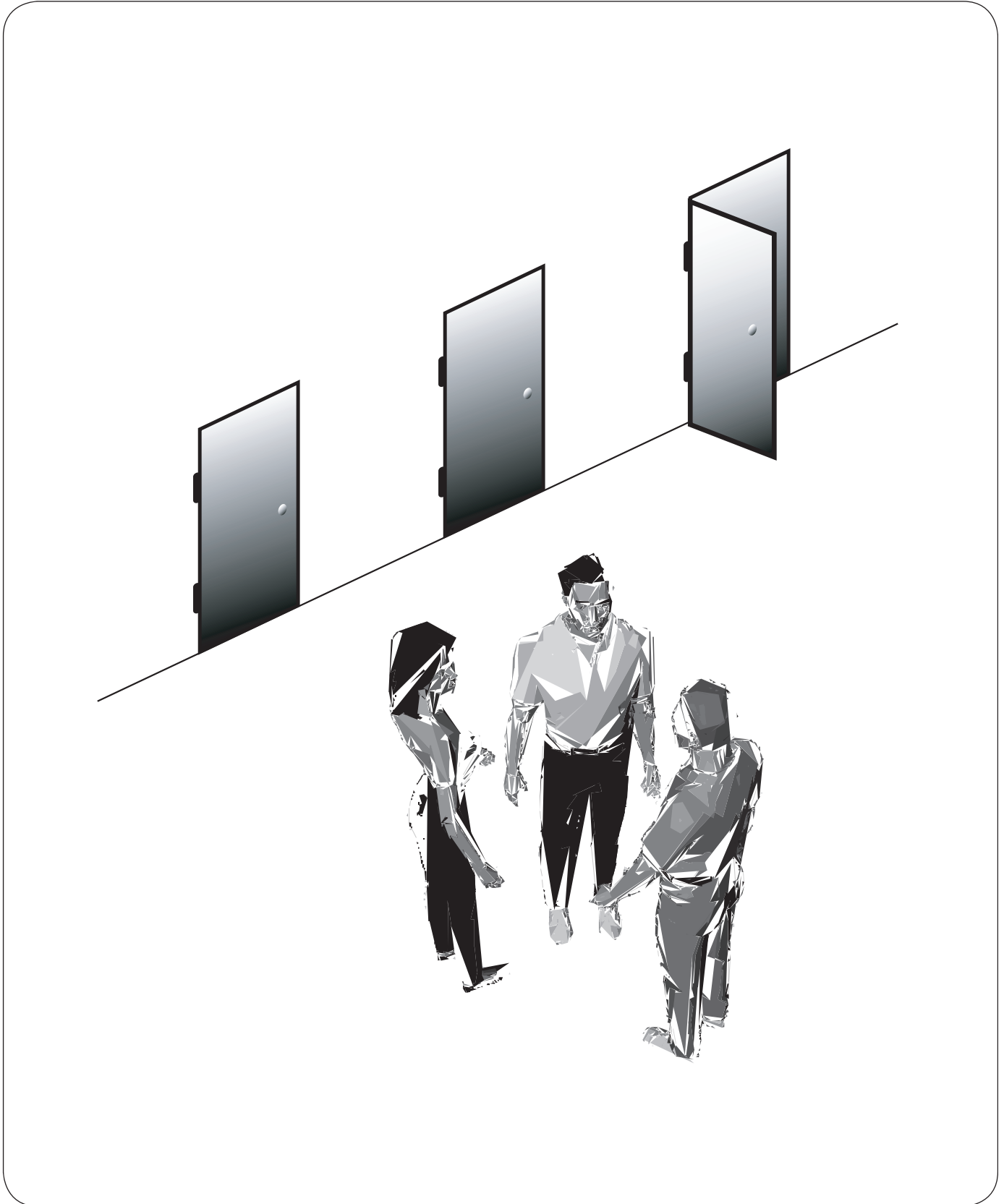




# Bewator Entro

User manual

GB



Copyright © 2005 Bewator AB, Solna.

Material from this manual may only be copied with the consent in writing of Bewator. Bewator reserves the right to alter both the content of the manual and the design of the product.

Document number: **81335-1 V5.0-GB**

Bewator AB is part of the Swedish Bewator Holding AB, which develops and markets a complete security product range that includes access control and alarm. Sales, installation and servicing are handled by a national dealer network. Actions (such as unauthorised manipulation, copying etc.) must not be taken with the software contained in the products and systems. Such actions are regarded as copyright violation and may result in imprisonment or fines and may likewise lead to an obligation to pay damages and compensation for using the software.

# Contents

CONGRATULATIONS ON YOUR CHOICE OF BEWATOR ENTRO!	6
You should be familiar with Windows	6
How the system works	7
IMPORTANT CONCEPTS	8
Security levels	8
Time schedules and time zones	9
Access groups	10
Access registration	10
Zones	10
PREPARATIONS	13
INSTALLING THE SOFTWARE	14
Creating a basic database and connection	14
PROGRAMMING - INSTALLER	17
Log on	17
Set time and date	17
Advanced system clock management	18
Programme names for segment controllers	19
Programme names and functions for doors	22
Programme IOR6 for Reservation system	23
Programme IOR6 for time control	23
Programme the IOR6 for special functions	24
Programme zones for reservation object	25
Random allotment of similar reservation objects	25
Alarm control in a reservation object	26
Programme Intruder Alarm zones	27
Other type of zones	29
Lift Control with IOR6	31
Card reader parameters	32
Personal code without card	32
Changing red LED function on readers	32
DYNAMIC IP ADDRESS (DHCP) AND DYNAMIC DNS	33
Background	33
Prerequisites	34
Static IP-addresses	34
Dynamic IP addresses	35
Configuring of DynDNS.org	35
Example where SR34i manage IP-addresses	36
Example when DynDNS.org manages IP-addresses	37
Installation and setup of DHCP	38
Basic configuration of database	38
Customise the database for DHCP	39
Decide on network settings for SR34i	40
Decide on login for SR34i	41
Apartment building – example 1	42
Apartment building – example 2	44
PROGRAMMING - USER	45
Start the system	45
Shortcuts	46
Time schedules – general	47
Time schedules – access control	47
Time schedules - Intruder Alarm zones	49
Enter specific half days, public holidays and holiday periods	49

General half-days, public holidays and holiday periods .....	50
Doors .....	52
Access groups .....	53
Persons .....	55
Register System Users .....	58
Access registration .....	59
Event and door filters .....	60
The calendar .....	62
Encryption functions in Local Area Network .....	63
Special computer setting in Entro .....	64
Supplementary information .....	65
<b>USING BEWATOR ENTRO .....</b>	<b>66</b>
Entrance .....	66
Switching on and off alarm systems .....	66
Entering the duress code .....	67
Setting/changing the PIN code .....	67
Caretaker functions .....	68
Searching registered persons .....	69
Import and export information about persons .....	70
Backup of event files .....	72
Backup of the database .....	72
View system resources .....	72
<b>DOOR AND EVENT MONITOR .....</b>	<b>73</b>
Multiple windows with different monitoring focus .....	73
Search events .....	74
Door operation from PC .....	75
Open/close all doors .....	76
Roll call .....	76
Reset blacklisted card .....	76
<b>PRINTOUTS .....</b>	<b>77</b>
Programmed information .....	77
Events .....	77
<b>WORKING WITH MULTIPLE SYSTEMS .....</b>	<b>78</b>
Logging in .....	78
Dialling the modem connected system .....	78
<b>BEWATOR ENTRO RESERVATION .....</b>	<b>80</b>
Set the Reservation options (System User) .....	81
Reservation operation (User) .....	81
Confirmation of reservation .....	81
Using the reservation object (User) .....	81
<b>IMPORTANT CONCEPTS - RESERVATION .....</b>	<b>82</b>
Time schedules .....	82
Flexible reservation in same interval .....	82
Reservation objects (single) .....	83
Reservation objects (grouped) .....	83
Machine and door control .....	83
Security levels .....	83
Access Groups .....	84
Persons and Member groups .....	84
Example 1 of Reservation .....	85
Example 2 of Reservation .....	86
<b>PROGRAMMING - RESERVATION .....</b>	<b>87</b>
Time schedules .....	87
Reservation object .....	88
Enter public holidays and holiday periods in Reservation .....	89
Decide on reservation authorities for access groups .....	89

---

**Give persons reservation authorities ..... 90**  
**Flexible reservation in same interval ..... 90**  
**Special Set-up – Reservation..... 91**  
**Using confirmations in Reservation ..... 92**  
**Example of confirmation ..... 93**  
**View and make reservations as Administrator ..... 95**

**RESERVE AND USE OBJECTS ..... 96**

**INTEGRATING WITH EXTERNAL APPLICATIONS (BAPSI)..... 97**

**NOTES ..... 98**

**IMPORTANT INFORMATION ABOUT THE ACCESS CONTROL SYSTEM..... 101**

## ***Congratulations on your choice of Bewator Entro!***

This manual is intended for the person responsible for the Bewator Entro access control system.

If you intend to also use the Reservation function – we have chosen to describe this in a separate chapter starting on page 80. Reservation uses a network based Entro system (which may not be installed in all applications).

Instructions on managing and running the programming, such as registering and deleting persons from the system, are found in the system's built-in Help function. How to use the Help function is described in the *Using Help* section below.

### ***You should be familiar with Windows***

Bewator Entro is designed to make programming of the information as easy as possible. It is however an advantage if you are familiar with the Windows environment. If you have no previous experience of Windows, we recommend that you take a basic course.

### ***Using Help***

Bewator Entro has a built-in Help function. Using Help you can display instructions on your screen about the task you are currently performing.

To open the Help function, click the **Help** button, or press F1 on the keyboard.

By clicking the right mouse button as you point to an object (a field, tab or similar) you can display a descriptive text about this particular object. Clicking the **question mark** button and then pointing to the object you need help on obtains the same effect.

### ***Entro manuals***

The software package includes the User and Installer manuals. The same documentation is also available from the program in pdf-format.

You need to have the Adobe Acrobat Reader installed in your computer to be able to read the manuals. This software can be downloaded free-of-charge from Adobes' web site.

## How the system works

Bewator Entro is an access control system. It is designed for use in both small and large companies, wherever there is a need to control which people should have access to the different doors and departments in the premises.

Next to the doors, card readers with keypads (optional) are installed. The card readers are connected to segment controllers, which, are programmed from a PC.

If needed, Bewator Entro can control up to 1000 access control systems installed in different buildings. The systems may be connected directly to the PC, using the local area network or via a modem.

Bewator Entro consists of the following equipment:

- The **Bewator Entro software**. The software runs on a PC with Windows 98/2000/XP/NT4 or later.
  - 512 doors and 20 000 cards.
  - 240 time schedules and 480 access groups
  - 240 zones (alarm, anti-pass back, roll call and entrance limitation zones)
  - 16 system users in 4 levels + installer level
  - 14 holidays, 7 half days and 4 holiday periods in each time schedule

In Bewator Entro is an integrated software module for reservation functions, like time booking for sports arenas etc.

- 64 reservation objects (machine groups).
- Maximum of 10 IOR6 relays in each machine group.
- 32 time schedules with 24 intervals in each.
- Flexible interval reservation.
- Maximum number of reservations is 4000.
- Confirmations may be sent by e-mail.
- **SR34i Segment controllers**. Up to 16 segment controllers can be connected to the PC in a loop. Each segment controller is capable of controlling 4, 8, 16 or 32 doors. The information you programme in the PC is stored in all segment controllers. This brings the advantage of being able to use the PC for other purposes or shut it down when you are not programming or controlling the system.
- **CF8**. Memory card used in Reservation functions (mounted in SR34i).
- **Door controllers with remote readers**. The door controllers are connected to the segment controllers. A door controller controls one door, with one or two readers. This combination is designed for outside doors or other doors with higher requirements on function and security, e.g. alarm by-pass.
- **Door terminals DT05 or DT05Prox**. Simple card readers connected directly to a segment controller. They are installed indoors, next to doors with lower requirements on function and security.
- **Relay central IOR6**. Used for lift control and for machine/door control in Reservation applications or general timer functions. In version 5 also for summary alarm, emergency openings or power failure warning.
- **InfoPoint IP810**. Reservation terminal used for time booking at the reservation object. TCP/IP protocol for network connection is required.

## Important concepts

To be able to programme the system you have to be familiar with the following concepts:

- Security levels
- Time schedules and time zones
- Access groups
- Access registration
- Zones

If you intend to use the Reservation system – see section *Important concepts – Reservation* on page 82.

## Security levels

The security level determines what action is needed to open a door. The following security levels exist:

- **Door unlocked.** The door is unlocked.
- **Group code.** The door can be opened using a four-digit code, shared by a group of people.
- **Card only.** To open the door, a personal access card should be swiped through the card reader. If the card is lost or stolen it is easy to cancel the card.
- **Card + PIN.** The door is opened when the access card is swiped and a personal code belonging to this particular card has been entered.
- **Toggle – Group code.** Similar to Group code above. When the code is entered the first time, the door is opened and remains unlocked until the code is entered the second time.
- **Toggle – Card.** When the card is swiped the first time, the door is opened and remains unlocked until the card is swiped the second time.
- **Toggle – Card + PIN.** When the card is used and the code is entered the first time, the door is opened and remains unlocked until the card is used and the code is entered the second time.
- **Accompanied Access.** Two people, each swiping their cards and entering their codes within 15 seconds, are needed to open the door.
- **Closed door.** The door cannot be opened by the card reader, but only from an exit request button from the inside.
- **Locked door.** The door is completely disconnected from the system, which means that not even exit request operates.
- **Personal code without card.** Bewator Entro can be set so that users may choose a PIN code instead of a card. This will disable the *Group code* operation.

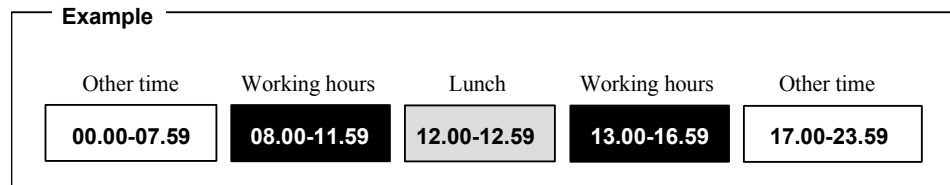
Using the security levels, you can determine the suitable type of protection for your premises. During the day, when there are people in the premises, **Group code** or **Card only** may be sufficient. During the night, the **Card + code** security level is perhaps more suitable.



## Time schedules and time zones

The purpose of creating **time schedules** is to give different people access to a door at different hours, and to determine security levels for a door at different hours.

In an average-sized company, the staff will probably have similar working hours. If this is the case, you may create a time schedule for these hours called, for example, **Office hours**. A time schedule covers 24 hours and can be divided into **time zones**.



**Time zone 1:** Working hours Mon.–Fri. 8.00–11.59, 13.00–16.59

**Time zone 2:** Lunch Mon.–Fri 12.00–12.59

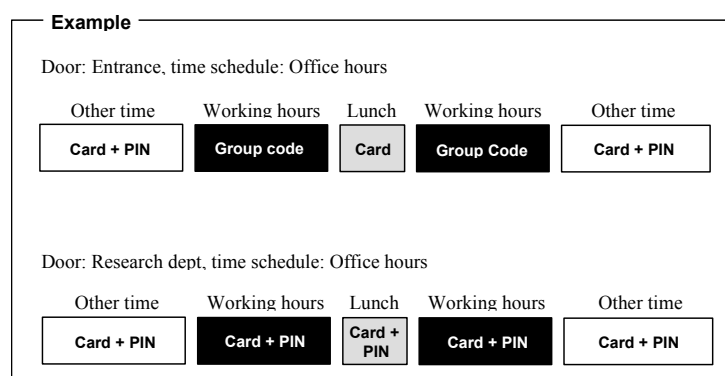
**Other time:** All time not in Time 1 & Time 2, including Holidays

**Note!** A time zone is valid from and including the first second in the first minute up to and including the last second in the last minute.

The purpose of dividing the time schedule into time zones is to be able to provide each door with a specific security level for each time zone. If you divide the time schedule into the time zones **Working hours**, **Lunch** and **Other time**, you can give the door a security level for each of these time zones. During office hours, when there are people in the building, perhaps **Group code** is suitable. During lunch, you can set the security level to **Card only**.

During the remaining time, i.e. nights and weekends, you could raise the security level to **Card + PIN**. If you only need two different security levels, it is sufficient to divide the time schedule (the 24 hours) into two time zones, i.e. **Time zone 1** and **Other time**.

During programming, you will be asked to enter security levels for one door at a time. If a door leads to a department requiring a high security level 24 hours a day, set the security level to **Card + PIN** for all three time zones.



If the company has workshop personnel with other working hours, you may create a second time schedule to determine the permissions for doors leading to the workshop premises.

You can programme up to 240 different time schedules with three time zones per time schedule. **Other time** is always one of the time zones.

## Access groups

In a large company with several different departments, you may have to divide the staff into different **access groups**. This way you can decide which doors the different groups should have access to – and during which hours they should have access to these doors. For example, you can programme so the reception staff does not have access to the research department during lunch; at the same time both the reception staff and the research staff should have access to common doors during all time zones. Each person may belong to six access groups at the most.

## Access registration

If desired, you can have information about transactions and other events printed regularly. You decide for which doors and during which time zones this should be possible. For example, you can request printouts of all transactions at night through the main entrance. The printout states which door has been used, what time and the names of the people who used the reader.

Bewator Entro furthermore offers the possibility to choose the types of events to be registered. For example, you can choose to show only whenever a door is left open or whenever an alarm occurs, or only show exceptions (i.e. not to show normal transactions.)

You may choose whether registered events should be printed or displayed on the PC's screen. If the events should be printed you can choose which printer they should be printed to.

Events are stored in event files on the PC's hard disk. To free disk space the system can be set so that event files are deleted after a specified time or when a specific file size is obtained.

## Zones

Zones are used to group a number of doors (readers) to have a specific function. In a corridor several doors may constitute a zone.

Different zone types can be created:

- Alarm zones
- Anti-pass back zones
- Roll call zones
- Entrance limitation zones
- Reservation objects
- Interlock zones (2 doors)

Doors in Zones are created in the Bewator *Installer* program.

## Alarm zones

An alarm zone includes one or several doors leading to the same alarm-protected area, where alarm by-pass is required at all doors. Alarm zones are defined in the Bewator Installer program.

It is possible to combine the functions of manually activating the alarm and/or automatically activating the alarm. I.e. if nobody activates it – Bewator Entro will.

The alarm control function enables you to determine which people should be authorised to activate and deactivate an intruder alarm system linked to Entro. As you are defining the access groups you will also be able to distribute the proper alarm by-pass authorisation.

The following authorisation types exist:

- **None.** No authorisation.
- **Activation.** Authorisation to activate the alarm system. E.g. suitable for cleaning staff, who will be there before the end of working hours, and will be the ones to activate the alarm.
- **Deactivation.** Authorisation to deactivate an alarm.
- **Activation/deactivation.** Authorisation to activate and deactivate an alarm.

## Anti-pass back zones

Creating **anti-pass back zones** is a way to further increase security. Anti-pass back means that a cardholder cannot enter a zone twice unless he has exited the zone. If a user violates anti-pass back, i.e. does not use his card to leave a zone and then tries to enter a zone, the card will be blacklisted.

On a door leading to an anti-pass back zone, an IN reader (on the outside of the door) and an OUT reader (on the inside of the door) should be installed. Remember that BCLINK readers with “sub-address” Entry and Exit respectively also will work with this function and do not require a “main address” like DC22, DC12, IOR6 etc.

Anti-pass back zones are defined in Bewator Installer. In Bewator Entro, it is possible to specify for how long a card should be blacklisted if a person violates anti-pass back (see the *Programming* chapter on page 65).

If anti-pass back zones have been defined, roll call zones are automatically created, enabling you to monitor a person’s whereabouts in the **Door and event monitor** (see the *Door and event monitor* chapter, the *Roll call* section on page 76).

**Note!** Anti-pass back works only with the *Card* or *Card+PIN* security levels.

## Roll call zones

Just like anti-pass back, roll call requires IN and OUT readers to be installed on either side of the doors belonging to the zone. By defining roll call zones a person's whereabouts in the premises can be monitored in the **Door and event monitor** (see the *Door and event monitor* chapter, the *Roll call* section on page 76).

The only difference between roll call and anti-pass back is that anti-pass back includes the feature that cards will be blacklisted if a user does not use his card to leave a zone he has previously entered.

Roll call zones are defined in Bewator Installer.

<b>Note!</b> Roll call works only with the <i>Card</i> or <i>Card+PIN</i> security levels.
--

## Entrance limitation zones

A building can have areas where limited access can be allowed. In a school dining hall for example, a card may grant the cardholder **one** meal a day. To prevent the card from being passed to other people, an entrance limitation zone can be created for this particular area (this is done in Bewator Installer).

In Entro, an access group can be created with the desired entrance limitations – either a counter (a certain number of entries are allowed) or limited access (e.g. once a day) or a combination of both.

In the dining hall example, the system could be set so that the card can be used once a day for 20 days.

Using entrance limitation with a counter, it is possible to specify an individual number of granted entries for each person in the access group.

## Reservation objects

If you intend to use Bewator Entro for reservation you have to set up the object (conference room, laundry etc.) as a zone. That is, you have to decide on which card reader to use for reserving your objects - as well as any doors/readers on the route to them.

Reservation can be used in many applications, e.g. conference rooms, laundries, sports arenas, tennis courts etc. Using some suitable time intervals, the users themselves can easily reserve times for access to the objects. Also the integrated function called *flexible interval reservation* offers possibilities to reserve different time intervals for each reservation.

You can even easily combine door access with relay activation for machine control, light control etc, so that these will only be active during the times you have reserved. For example, in a laundry room, machines can be randomly allocated to minimise the wear of individual washing machines.

You can read more about reservation in the chapter *Reservation*.

## Interlock zones

In some cases it is required to use two doors in an Interlock application. I.e. the first door must be closed before the second door can be opened.

You solve this by creating an Interlock zone with two doors where each door have a door monitor contact installed. When entering the doors in either direction Entro will monitor for a closed contact before the opening relay is activated in the next door.

## Preparations

It is important that, before starting to programme, you have the correct, basic information about the site you intend to set up and programme. Whether you have used Bewator Entro before or not, you will avoid many mistakes if you have planned correctly.

### Installation

Before you begin installing, you should consider the size and layout of the installation. How many segment controllers should be used? How many doors should each segment controller control?

Which controllers will use TCP/IP and need a valid IP-address? In which part of the network will the system be installed? Has the IT-Manager approved all network settings for the PC's and SR34i's? Will some of the SR34i use dynamic IP addressing ?

Should Bewator Entro control an intruder alarm? Which doors are included in the alarm zones? Should some of the alarm zones be timer controlled and activated automatically at certain hours?

We recommend that you do this in consultation with the end-user of the system.

A maximum of 16 segment controllers can be used in each Bewator Entro system. Each segment controller should be given a name and an address, from 1 to 16. For each segment controller, you will be asked to name and allocate addresses to the doors controlled by the segment controller.

### Programming

Before you start programming the system's basic information, you should think about how the system should function in the building. During which hours should entry through the main entrance be permitted? Do certain people need to have access 24 hours a day? Who should have access to the research department? How does the cleaning staff get inside the building in the morning or evening?

If you also intend to use reservation functions – see section *Important concepts – Reservation* on page 80.

You should also consider if anyone else should be able to programme the system and then create new **System users** with their own passwords. This is necessary if e.g. several PC are to be connected to Entro.

## Installing the software

The next step is to install the Bewator Entro software.

**Note 1!** If the system will use dynamic IP addressing technique (DHCP) on the local area network – you should read the chapter *Dynamic IP address (DHCP) and dynamic DNS*

**Note 2!** If you intend to use a modem, you will also find information in the Installation manual.

- 1 Normally the installation automatically starts when the CD is loaded. Otherwise go to the Windows Start menu; choose **Settings** and then the **Control panel**.
- 2 Double click the **Add/Remove Programs** icon.
- 3 Click **Install**.
- 4 Insert the CD in the CD ROM drive and click **Next**.
- 5 Follow the instructions on the screen.

Dependent if the system is new or not, different steps are performed to achieve the final solution. E.g. if it is the 1<sup>st</sup> or 2<sup>nd</sup> PC, exchange of PC, expansion with more SR34i etc, the Installer program is used in different ways.

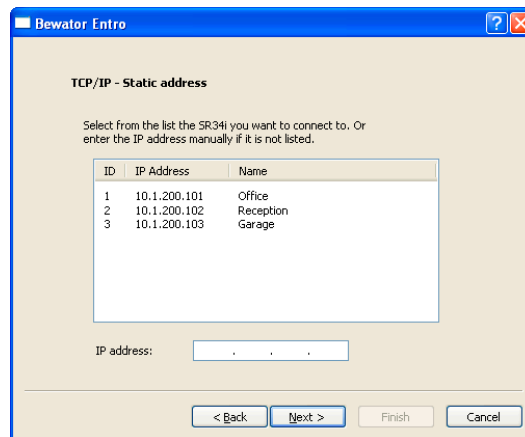
Sometimes you have to know the system name as well as the user name & password to be able to use the software. In the following section we describe how to install the software from scratch.

We use a wizard to create the initial communication link to an SR34i controller.

## Creating a basic database and connection

The first time you start the *Installer* program there is no database or information about any *connection* to use in the PC. Therefore a wizard starts requesting the necessary parameters. Depending of the selections made some of them might not be needed. Proceed like this:

- 1 Go to the Windows Start menu; choose Programs and then *Bewator Entro Installer*.
- 2 The wizard starts and you make the selections E.g:
  - New or existing system.
  - The name of the site.
  - How should this PC communicate with the site (TCP/IP, RS232 or modem)?  
If you select modem, enter the telephone number to the SR34i modem. In case of RS232 the software automatically detects the correct COM-port in the PC.
  - If you select **TCP/IP** then initially *static IP-address* is assumed for the SR34i. Proceed by clicking Next.
  - The software has checked in the local area network (often isolated by a router), for available SR34i's.
  - Click **Next** to see the available segment controllers.



- First you have the opportunity to complete these with the **correct IP-addresses**. In addition you can adjust the IP Address of *all* SR34i, not only the one chosen for the PC.
- You now have to select the SR34i you intend to use for connecting to this PC. **Note - only one can be used!**

If it is not listed, enter the correct IP-address to another, chosen SR34i and click Next.

Note – this indicates that the chosen controller is located outside the local network and its IP-address has to be set up in another way. The network must also be configured correctly to get the PC online.

- Click **Next**.
- 3 Enter a the name of the site (**Site name**).
  - 4 Enter a unique **System name**. Avoid names that could easily be found out by unauthorised people.

**Note!** It is very important that you make a note of the **system name**. If you have to replace the PC this system name must be entered before the system will work again.

- 5 Click **Finish** and the Installer main window is displayed.

Normally you will now see detected units (as below) where you then select either to programme all units or at least one SR34i (according to the chapter *Programming – Installer*) – and then create a connection according to the section *Create connection to store events*.

### Automatic detection of units

The *Installer* programme has embedded functions for “finding” addressed and connected segment controllers and door centrals. Subsequent expansions with additional units will also be found in then same way.

If the site is correctly installed, with appropriate addresses, you only need to step through each SR34i and door centrals according to following chapters. A list of units will be displayed on the screen as soon as login to *Installer* is done. An SR34i is displayed as \*Cxx and a door unit or IOR6 is displayed as \*\*Cxx:Dyy.

## Create connection to store events

When you have performed the steps in the previous section, the system still is in an “Installer state”, which means that any events are sent to the PC only as long as the PC is on-line. If you logout no events are buffered in the SR34i (neither sent to the PC later on at login)

To get the Segment Controller to store events you have to **create a correct connection**. When this is done the SR34i will know, any time you logon, which PC to receive and store events from.

Proceed as follows:

- 1 Go to the tab **Connections** (in the Installer program) and click **New**.
- 2 A wizard starts and you select **Bewator Entro – System administration** – and click **Next**
- 3 Enter a name of the connection, which **SR34i**, which **PC** and the **communication method**.
- 4 Finish.

You have now created the first correct connection between the PC and the Entro system.

- 5 Proceed according to chapter - *Programming Installer* to make all the necessary settings for the installed Entro units.

<p><b>Note!</b> We also recommend that you also <b>create System Users</b> (in Entro) to be able to manage the event filters, storing places and automatic logoff in a more flexible way.</p>
---



## Programming - Installer

Now you have installed and connected all parts of the hardware on the installation, installed the software Bewator Entro and created a *connection* for the PC. In this chapter we will describe how to perform the configuration needed for the system.

### Log on

- 1 Go to the Start menu; choose Programs and then Bewator Entro Installer. The log on window is displayed.



- 2 Enter <user name> (bewa) in the **User name** field and press TAB.
- 3 Enter <password> (pass) in the **Password** field.
- 4 Select the **System** to use (if several exist).
- 5 Click **OK**. The Bewator Entro Installer main window is displayed.

### Set time and date

Before starting to programme you should set the correct time and date. The clock is shown separately in the lower, right corner of the window.

Note that if any SR34i is set to TCP/IP and will get the time from an external SNTP timeserver – you cannot manually set the clock. See further next chapter.

Proceed as follows, if the system lets you correct the system clock:

- 1 Check that the indicators in the lower right corner of the Bewator Entro windows display ONLINE and DB UP TO DATE.
- 2 Start the *Installer or Entro* program.
- 3 Choose **Entro system clock** on the **System** menu.
- 4 Check that the correct date and time are displayed. If not, enter the current date and time in the **New date** and **New time** fields.
- 5 To disable automatic daylight saving time changes, remove the tick next to the **Automatically adjust clock for daylight saving changes** prompt.
- 6 Click **OK**.

## Advanced system clock management

You only have to make the steps below if you intend to let the Entro fetch its time externally and additionally allow each SR34i to adjust its time relatively to GMT.

Bewator Entro uses a Simple Network Time Protocol (SNTP) – which fetches an **international clock (GMT)** from an external SNTP process running on an external server – (on the LAN/Internet) – or an internal server (SR34i). SNTP is necessary for SR34i's that are network connected (TCP/IP). If in doubt, consult the IT manager.

If any network is used, the SR34i must be able to get the clock from a clock server – when TCP/IP is used. Every controller set to **Proxy** must also have this setting. This guarantees correct time in the system independent of where an SR34i is installed.

When you programme an SR34i as Proxy, it will need to know where to fetch the clock from. You can select internal or external.

In the menu **System/Entro System time** in *Installer* program are more choices for the system clock. Do like this:

- 1 Check that the indicators in the lower right corner of the Bewator Entro windows display ONLINE and DB UP TO DATE.
- 2 Click **Advanced**.
- 3 Select method for time server:
  - Internal time server (e g SR34i) and select controller.
  - External time server (e g via Internet) and enter IP-address.
- 4 Select if every SR34i is allowed to correct its time relatively to GMT time.  
If this is selected – every segment controller will display a new tab **Time** where the adjustment value is chosen (e g +1, +2 etc).
- 5 Exit
- 6 Check in the menu **System/Entro System time** and check the choice of **Automatic daylight saving time changes**.

## Programme names for segment controllers

Now programme the segment controllers. Dependent on how the SR34i's should communicate with each other, the parameters are set-up in different ways.

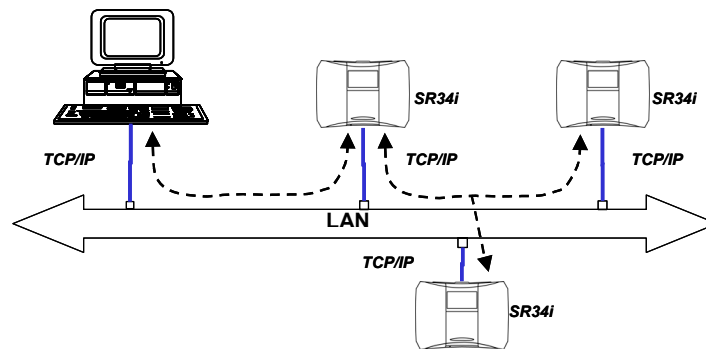
Remember that the basic parameters (like the IP address) initially can be set by using the integrated keypad in each SR34i. Which means that you fulfil the requirements for communicating with the PC, but set up the rest of the settings in the *Installer* program.

If you intend to use dynamic IP addressing for segment controllers you should read the chapter *Dynamic IP address (DHCP) and dynamic DNS* on page 33.

If a modem will be used – please refer to the *Installer Manual* for more information.

Here are two examples where a LAN is used – and one using direct RS232 cable.

### Create multiple SR34i for TCP/IP communication



In this case two methods can be used to set-up the SR34i segment controllers.

#### Programming via RS232

A PC is connected to every SR34i via RS232 connection. The information is transferred directly into every SR34i.

RS232 is the easiest method to use, when the segment controllers are placed in different geographical areas. It is important that these get the correct IP-address, system name and encryption key.

Every new SR34i is displayed as **\*\*Cx**. Now proceed according to the steps in the section *SR34i Programming*, to set the **IP-address**, **Proxy** and other necessary parameters.

#### Programming via TCP/IP

In this case the PC communicates with a dedicated SR34i whilst the other controllers will get the information from this one (via TCP/IP). If the system is new, you will already have had the opportunity to set up the correct **IP-address**.

In the Installer program, the first controller is shown. You now have to use the command **New** to create the rest of the controllers and to set the **IP-address**, **Proxy** and other necessary parameters according to the steps the section *SR34i Programming*.

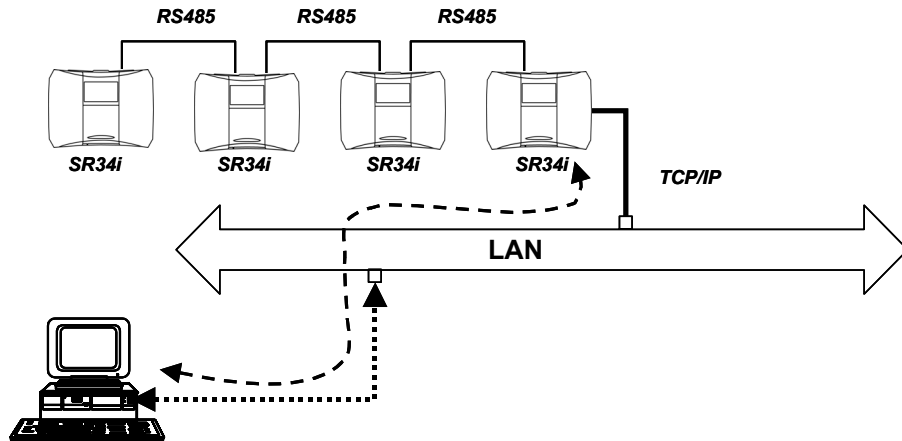
**Note!** Transferring the data to/from completely new SR34i will take some minutes (due to the load on the network). This also applies for updating the Door monitor program.

### Create multiple SR34i for combined TCP/IP and RS485 communication

The combination of a local network and RS485 requires that the controller used for TCP/IP has to be set-up as in the earlier section.

All other SR34i, using RS485, will be displayed with temporary symbols (\*\*c1, \*\*c2 etc.). The number refers to the segment controller's address.

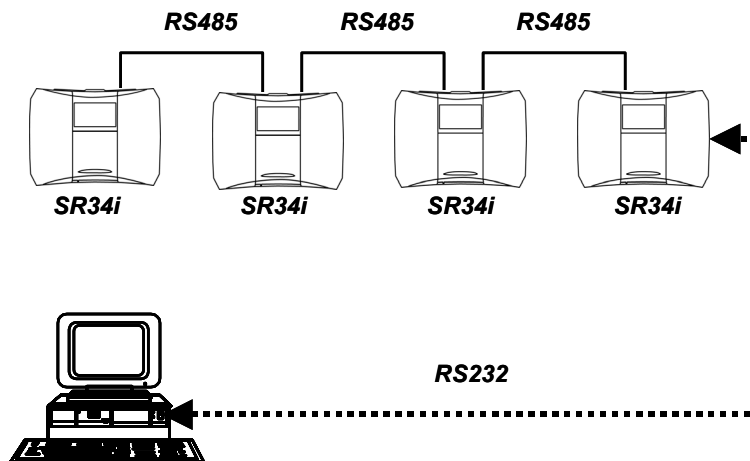
Then proceed with the steps in the section *SR34i Programming*.



### Create multiple SR34i for only RS485 communication

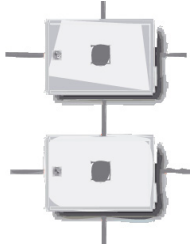
Systems intended for RS485 (no local network) – are set up via direct cable RS232. In this case all controllers will be displayed as \*\*C1, \*\*C2 etc – where the digit corresponds to the address jumper

Then proceed with the steps in the section *SR34i Programming*.



## SR34i Programming

**Note!** In a new TCP/IP based system, you will (when invoking the *Installer* program) have the opportunity to add more not yet configured SR34i that the software “finds” on the LAN. You will see them in a list. Just select any one of them to be included.



- 1 In the *Installer* program select the desired segment controller (if it is not already selected) and click **Edit**. **Tip** – You can also right-click and choose *New*, *Edit* or *Delete*.
- 2 In the **Name** field, enter the segment controller’s name. A suitable name is the room where the controller will be placed, e.g. Reception. Avoid using names that may later be confused with door names. If the controller will also be used for confirmation in reservation – see chapter *Using confirmations in Reservation*.
- 3 Mark the tick-box **Proxy** for SR34i using TCP/IP.  
  
If RS485 is used between *all* SR34is – but PC connection uses TCP/IP – the only need for proxy in the SR34i is for reaching an SNTP Time server. If there is a mix of RS485 and TCP/IP – the segment controllers using TCP/IP must have Proxy function.
- 4 Select the *Network* settings tab and enter the **IP-address**, **Netmask** and **Gateway**.  
  
When powering-up the controller – the IP-address will initially be **10.1.200.1xx** (where xx indicates how the address is set in the controller) – or the one stated initially when locally setting up SR34i.  
  
Enter the **Netmask**, which can filter the addresses for messaging on the LAN. Often the value 255.255.255.0 can be used. Enter the address for **Gateway** (if one exists.) This can be used to take care of rejected addresses (filtered by the Netmask). Enter the IP-address for any Domain Name Server if e-mail functions are to be used (see *Reservation*).
- 5 Enter the actual **SMTP server** (used in e.g. the Reservation system).
- 6 Enter the network identity for the segment controller.
- 7 Click on the tab *Time* (if displayed) and enter a **correction value** (+1, +2, -1, -2 etc). This should correspond to the geographical time zone where SR34i is installed. (Compare with GMT-time and the setting in an ordinary PC. I.e. +0 for Great Britain, +1 for Sweden and +2 for Finland).
- 8 Click **OK** and continue with the next segment controller until all the segment controllers on the system have been named.

## Programme names and functions for doors

The next step is to programme names and functions for the connected doors.

- 1 Start the *Installer* program.
- 2 Click the **Doors** tab. You will see the installed, addressed doors as \*\*C1:D1, \*\*C1:D2 etc.

**Note!** If an installed door is missing in the list, it means that the system has no communication with that door.

- 3 Select the desired door (if it is not already selected) and click **Edit**. Tip – You can also right-click and choose *New*, *Edit* or *Delete*.
- 4 In the **Name** field, enter the name for the door. Maximum 32 characters.
- 5 Check that the proper reader type is shown in the **Terminal type** field. If you are using zones, there may be a choice of readers if an EXIT reader is installed.
- 6 Click the **Relays** tab.
- 7 Select the checkbox **Use relay for alarm by-pass** if a monostable alarm (*locally*) will be used in this door. It can belong to a bistable alarm zone but cannot physically connect to the Intruder Alarm Control unit.

**Monostable function.** Used if you want to by-pass the alarm for a short amount of time (e.g. for an entrance). The by-pass time is equal to the opening time + the door held warning time. Doors with monostable function cannot connect and control the zones in an intruder alarm.

- 8 If the door central shall control a motorlock mark the tick-box for **Motorlock**.
- 9 Click the **Door control** tab.
- 10 If door monitor contacts are used, click the **Door monitor contact exists** check box. Enter whether the contact is closed or open when the door is closed.
- 11 If lock monitor contacts are used, click the **Lock monitor contact exists** check box. Enter whether the contact is closed or open when the lock is locked.
- 12 Enter, by choosing one of the alternatives **Lock at once when door is opened** or **Lock when door is closed again**, how the door is relocked after having been opened. This will be dependent on the type of lock installed.
- 13 If IOR6 lift control is used - see chapter *Lift Control* on page 31.
- 14 Click **OK**.
- 15 Continue with the next door until you have named all doors and described their function.

## Programme IOR6 for Reservation system

If any of the relays in an IOR6 are going to be used in a Reservation system, follow these instructions:

- 1 Start the *Installer* program
- 2 Click the **Door tab**. Normally a new IOR6 is displayed as \*\*Cx:Dy in the list of doors. Mark this, click Edit and step to item 7 below.

If you *manually* want to create a new IOR6 – proceed as follows:

- 3 Click **New**. The **Door properties** are displayed.
- 4 Enter the name of the relay central in the **Name** field.
- 5 Check and/or enter the address.
- 6 In the list box **Terminal type** - select IOR6.
- 7 Click the **IOR6 Relays** tab.
- 8 Mark the tick box **Reservation door** and/or **Reservation machine**.
- 9 Enter the name of each relay with digits. They will later be shown as the name of the IOR6 + the relay number.  
E g if the IOR6 is named "Washing room" and relay 3 it is shown as Washing room:3
- 10 Click on the list box on each relay and activate them as follows:
  - **Reservation – Door**. Means it will be used as an ordinary door opening relay and is activated for a specified opening time
  - **Reservation – Machine**. Means that this relay is activated the whole time the object is booked (e g a washing machine).
- 11 Click **OK**.

## Programme IOR6 for time control

In case you want to use the relays as a simple timer function, you set up the IOR6 as above but mark the tick-box **Time controlled** and select **Time controlled** in the list boxes.

These relays will be displayed in the *Entro* program and allow for choosing individual time schedules for them.

The system allows for separate opening time for the relays as well as relays 1 – 4 which can be activated via input signals (remote opening).

## Programme the IOR6 for special functions

The relay central can be used for a range of special functions. These are at the moment:

- Output for summary alarm (impulse)
- Input for monitoring a power failure signal (e.g. battery)
- Input for monitoring an “Emergency opening” signal to open all doors.
- Input for activating a relay (Exit button).

**Note!** Summary alarm is not possible in an IOR6 used for lift control applications. You must use another IOR6 in these cases.

The settings for this you find in the Installer – Doors where you mark the actual IOR6 (or creates a new). There are separate tabs for relays and inputs.

### Summary alarm – output

Proceed as follows:

- 6 Mark the tick box **Summary alarm** in the tab **Relays**.
- 7 Every relay in the IOR6 can optionally be configured for generating an output signal. The first time you select in list-box and select summary alarm a new menu is opened.
- 8 You then select for each relay an **event filter** to control the relay. Read more about filters in the section *Event and door filters* on page 60.
- 9 Select for how long **time** the relay shall be active.

### Power failure warning - input

Inputs can be setup to monitor signals from power supplies. Often used when a battery-backup power supply is installed. EG A signal can be sent from the PSU when the mains falls and batteries are used.

Proceed as follows:

- 1 Click the tab **Inputs**.
- 2 Click the list-box and choose **Power failure**.

### Emergency opening – input

An input can activate a function to set all doors unlocked. Usual when a fire alarm shall open doors.

Do like above – but select **Emergency opening** instead.

### Exit button - input

It is possible to set an input to activate a relay at a certain time. E.g. using a remotely open reservation door or allow for pushing a button in lift.

Do like above but select **Exit button** for corresponding relay.



## Programme zones for reservation object

- 1 Start the *Installer* program and click the **Zone** tab then click **New**.  
For new zones a wizard is invoked which will help you programme the required functions. For existing zones the tabs are shown (displaying the same information).
- 2 Enter the name of the object in the field Name.
- 3 Select **Reservation object** and click **Next**.
- 4 Mark **Available doors** (card readers) in the left windows. *All existing doors and IOR6 relays* in Bewator Entro are displayed and selected doors appear in right window.
- 5 Select the **Main Reader** for this object – i.e. the actual reservation reader.
- 6 Click **OK**.

Repeat for any other new reservation objects to programme.

If any relay central IOR6 are used in the reservation object you set up these according to the section *Programme IOR6 for Reservation system*.

Supplementary parameters for reservation are programmed in the Zone tab of the *Entro* program.

## Random allotment of similar reservation objects

If several similar objects are to be available for reservation, you can randomly allocate them to minimise the wear on individual equipment.

An example of this might be a laundry room with a couple of washing machines, where each is an object, which will be controlled by a relay in an IOR6 (machine control). All these individual objects are then grouped together and can be treated as one common, grouped object. The users are then allotted some of these individual objects when a reservation is done.

To create a grouped zone:

- 1 Create the individual objects as above.
- 2 Select the same **Main Reader** for all objects.
- 3 Select an IOR6 relay (as machine control) to control the object (e.g. a washing machine).
- 4 Finally you create a new object but select **Group of Reservation Objects** instead and mark the actual objects to group.

Doing this, will result in the main parameters (e.g. the maximum number of reservations) being the same for all objects.

## Alarm control in a reservation object

If you install an intruder alarm in premises that are also using reservation, you can use the card reader for alarm control in both monostable and bistable mode. You use a DC21 for this.

### Monostable mode

This method requires that the **DC22** used in the door must be set up for monostable mode. In the tab **Relays** (in the door properties in the *Installer* program), mark the tick-box **Use the relay for alarm by-pass**.

The alarm by-pass relay will change state during the *Opening time* + the *Door Held Warning Time* - and will automatically fall back.

### Bistable mode

Note that this method differs somewhat from the way Bewator Entro normally treats intruder alarm control (with alarm zones).

This mode will activate or deactivate an alarm section in the intruder alarm. Connection is done to the alarm by-pass relay in the **DC22**. Be sure that the tick-box **Use the relay for alarm by-pass** in the Relays tab is not marked.

<b>Note!</b> The actual zone in the intruder alarm can only be managed from this door.
--

**Activation** is performed with an alarm button connected to the Alarm button input of the DC22.

**Deactivation** is accomplished by a granted access to the reservation object. Usually the security level Card or Card+PIN will apply.

## Programme Intruder Alarm zones

Bewator Entro offers different methods to turn on a bi-stable intruder alarm zone:

- Using a valid card at the door terminal.
- Using a pushbutton connected to the Alarm button input.
- Using an external timer connected to the Alarm button input.
- Using a Bewator Entro Alarm time schedule (automatic).
- Use the intruder alarm manoeuvre functions. The alarm panel status signal is used to “follow” the status of the alarm central (feedback).

To turn off the alarm; following methods are valid:

- Using a valid card at the door terminal.
- Use the intruder alarm manoeuvre functions. (The alarm panel status signal is connected to the alarm input).

**Note 1!** Remember that any zones (e.g. Alarm zones) will work best if they reside in the same sub-net when several SR34i use TCP/IP (between related SR34i).

**Note 2!** Remember that any DC22s configured for monostable alarm cannot be wired for controlling any zone in the intruder alarm.

In cases where only one door is used to control an intruder alarm, you must still create an alarm by-pass zone for that door. Note that an alarm by-pass zone can be combined with both roll call and entrance limitation - but not with anti-pass back.

- 1 Start the *Installer* program and click the **Zones** tab, then **New**. For new zones a wizard is invoked which will help you programme the required functions. For existing zones the tabs are shown (displaying the same information).

**Tip** – You can also right-click and choose *New, Edit or Delete*.

- 2 Type the name of the zone in the **Name** field.
- 3 Select **Alarm zone**. You will also see any other functions this zone can be used for.
- 4 Click **Next**. In the **Entry doors/Available** box, select the door/s to be included in the alarm by-pass zone.
- 5 Click **Next**.
- 6 Select the door, which is **physically connected** to the intruder alarm control unit.
- 7 In the **Alarm by-pass relay operation** list box, select the alarm control method to be used.
 

**Bistable function.** Used if you want to fully control the intruder alarm. You may deactivate the alarm (after it has been activated) by using your card at the reader and entering your PIN code. To activate the alarm, press B and use your card at the reader (or B + card + PIN if this security level applies). You can use a push button (if fitted) connected to the alarm activation input of the DC22. Automatic alarm activation can be achieved by using a specific time schedule for alarm control.

**Bistable pulse.** This alarm by-pass method is similar to bistable function, but instead of the output remaining operated, a short pulse is generated for both the switch-on and switch-off operations.

- 8 In the **Alarm activation warning time** field, enter a duration for how long a warning buzzer should sound before the alarm is activated (between 0 - 1000 seconds = 16.5 minutes). The buzzer warns people still in the building that the alarm is about to be activated. If you enter 0 seconds the alarm by-pass relay changes its state immediately – without any buzzer warning.  
  
During this time the pre-warning alarm relay output will change state in all DC22 included in the actual alarm zone.
- 9 Select if the **Exit button** is allowed to abort the alarm activation cycle.
- 10 Choose which **Time Schedule** will be used for time controlled alarm activation. If you do not select any you have to manually activate it – or use an external signal (connected to the input for alarm activation).  
  
If you have not created time schedules (in the *Entro* program) – you click on the clock icon and select *New*, *Edit* or *Duplicate* a time schedule.
- 11 Click **Next**.
- 12 Mark the tick box **Use the ALARM BUTTON for ASF** if the intruder alarm's status signal will be connected. Then choose the logic Normally open or Normally closed. This signal connects to the Alarm input in the DC21. It tells Entro that the Intruder Alarm has been activated (or deactivated).
- 13 In the field **Timeout for ASF** you write the time in seconds, Bewator Entro will wait for the status signal – before it is seen as an activation failure. In this case Bewator Entro will go back to normal state (and accept normal accesses).
- 14 Mark the tick box **LED Control** to define how the red LED at the door terminal will be controlled. Either the LED is controlled by the feedback signal - or another external signal could be connected. This is the case if the red LED needs to flash in some way.
  - If choosing ASF – you also select how long time the red LED will be lit (after alarm activation.)
  - If you do not choose the ASF function – an external signal could still be connected. In this case choose only LED Input.
- 15 If you click on **Adjust** (at LED input) you can adjust the time to determine if the external signal from the alarm system should light or flash the red LED on the door terminal. Default (and maximum) value is 3.2 seconds. If it should flash – this period should be slightly longer than the pulse cycle of the external signal.
- 16 Click **OK**.

### ***Decide on security levels for alarm control***

- 1 Start *Entro* program and click on **Zone** tab.
- 2 Click on **Settings**.
- 3 Select the **security level** for activating and deactivating the intruder alarm. Click on the list box and choose *Card* or *Card+PIN*.

**Note!** This selection will be set for all Alarm zones you create.

- 4 Click **OK**.

## Other type of zones

In the same way as an alarm zone is created one or more doors can form another type of zone. These could be:

- Anti pass back zone
- Roll call zones
- Entrance limitation zones.
- Interlock zone (two doors)

Follow these steps to programme zones, if required.

- 1 Start the *Installer* program and click the **Zones** tab, then **New**.

For new zones a wizard is invoked which will help you programme the required functions. For existing zones the tabs are shown (displaying the same information).

**Tip** – You can also right-click and choose *New, Edit or Delete*.

- 2 Type the name of the zone in the **Name** field.
- 3 Select the desired zone type. You will also see any other functions this zone can be used for.
- 4 Follow the instructions for the selected zone type below.

**Note!** You can also use sub-addressing technique when creating zones and selecting readers. This applies to reader type **BCLINK**, who can be addressed as **ENTRY** or **EXIT** when connected to the same door central.

### **Anti-pass back/Roll call**

As an anti-pass back zone is created a roll call zone is created as well. You can however create zones that are roll call zones only. The only difference between roll call and anti-pass back is that anti-pass back means that the card will be blacklisted if a person does not use his card to leave a zone he has previously entered.

This is how to create an anti-pass back or roll call zone:

- 1 In the **Entry doors/Available** box, select which is reader IN.

**Note!** The same reader can be an IN reader to one zone and an OUT reader to another.

- 2 In the **Exit doors/Available** box, select which is reader OUT.
- 3 If you have created an **Anti-pass back** zone – also start *Entro* program, select the Zone tab and click Settings.
- 4 Click the **Anti-pass back** tab and control the method of removing any blocking of anti-pass back violation. (Factory setting is automatic un-blocking in 10 minutes.)

## Entrance limitation

When you create this type of zone you then have to decide which access groups will be able to enter the zone. You will also need to specify the counter for each person.

- 1 In the **Entry doors/Available** box, select the doors to be included in the zone.
- 2 Click **OK**.
- 3 Start the *Entro* program and click the **Zones** tab.
- 4 Mark the name of the entrance limitation zone and click on **Edit**.
- 5 Click on **Entrance limitation** and select restriction type (both types can be selected).
  - **Decrement entries counter**. Means that a certain number of entries are granted in doors included in this zone. Later, in Bewator Entro, one or more access groups should be created with restricted access to these doors. Finally, the number of granted entries can be specified for each person.
  - **Limited access to this zone** (e.g. twice a day). If this alternative is selected, go to the **Settings of limited access** box and select the desired time restriction, e.g. twice a day. If needed, access can be limited further by choosing restrictions per time interval.

**Note!** If more than one entrance limitation zone is created, only one zone can have limited access.

## Interlock zone

If you create an interlock zone (with two doors) you must be sure that the doors have door monitor contacts mounted. Then do like this:

- 1 Create a new zone in the *Installer* program.
- 2 Select **Interlock**.
- 3 Select the two doors.
- 4 Exit.

Regardless which doors you select, the function is strongly dependant of how the readers and exit buttons have been mounted.

The most common may be, that there are readers at both doors into the zone that will unlock the “second” door automatically, as soon the first is closed.

Another example is that the “second” door instead has an exit button (into the zone). In this case the next door will not unlock automatically – you will have an exit button (out) mounted at that door. In doubt – please contact Bewator.

## Lift Control with IOR6

When applied to lifts, Bewator Entro can be used to restrict access to the different floors in a building. For lift control up to 32 IOR6 relay centrals can be connected to the Bewator Entro system, which means that altogether 192 floors can be controlled.

Note that neither IOR6 nor its master reader can be included in zones.

- 1 Start the *Installer* program
- 2 Click the **Door** tab. Normally a new IOR6 is displayed as \*\*Cx:Dy in the list of doors. Mark this, click **Edit** and step to item 7 below.

If you manually want to create a new IOR6 – proceed as follows:

- 3 Click **New**. The **Door properties** are displayed.
- 4 Enter the name of the relay central in the **Name** field.
- 5 Check and/or enter the address.
- 6 In the list box **Terminal type**- select IOR6.
- 7 Click the **IOR6 Relays** tab.
- 8 Mark that this IOR6 will be used for lift control.
- 9 Enter name of each relay with digits. They will later be shown as the name of the IOR6 + the relay number.  
E g if the IOR6 is named "Lift A" and relay "3" it is shown as Lift A:3
- 10 Click on the list box for each relay and activate them.
- 11 Click **OK**.
- 12 Click the tab **Doors** and mark the terminal intended as a **Master** for the IOR6.

**Tip!** A suitable name for the master door terminal is e.g. "Lift, floor". Door terminals are named on the **Doors** tab.

- 13 Click on **Edit** and click the tab **Lift Control** and mark the IOR6 -units that will be controlled by this terminal.
- 14 Click **OK**.

In **Bewator Entro**, the numbered floors (relays) are shown on the **Access groups** tab, in the door list under the name of the master reader. This way, it is very easy to select the floors to which the group should have access.

It is also possible to activate the relays according to the time schedule applied for the actual master reader. You find the set up for this in the IOR tab in the Door menu (*Bewator Entro*). You mark the tick-boxes in the time zone column for the relay to be activated. Relay 1 – 4 in every IOR6 can also be activated via a signal to exit button input (remote opening).

## Card reader parameters

If cards other than Bewator cards are to be used and if they will be read differently, you must change the card reader parameters.

- 1 Start the *Installer* program, choose **System settings** on the **System** menu.
- 2 Click the **Card reader parameters** tab.
- 3 Enter the type of access cards to be used in the system.
  - **Bewator standard** means that the system reads track 2 ISO format and positions 9-16 on the magnetic strip, or the last 8 positions if fewer than 16. (Standard Bewator cards are encoded like this).
  - If other cards are to be used and will be read differently, click **Custom**. Then enter from which digit position on the magnetic strip data should be read and how many digits should be read (8 at the most). Some newer readers can also read 16 digits. You should consult with Bewator if you are in any doubt about this.
- 4 Select in which way the digits shall be presented in Entro.

## Personal code without card

Generally, PIN code is used together with a card – during the *Card + PIN* security level. However, Bewator Entro offers each user the possibility of choosing a PIN code **instead of** a personal card. Note however that activating this function disables *Group code*.

This is how to activate the function:

- 1 Start the *Installer* program, choose **System settings** on the **System** menu.
- 2 Click the **Personal Code** tab.
- 3 Choose the **Use of personal code without cards** alternative.
- 4 Enter the desired number of digits to be used (4-8) in the PIN code. Any user-choosing PIN without card must choose a code consisting of the number of digits chosen here.
- 5 Click **OK**.

## Changing red LED function on readers

By default, the red LED is used to indicate an active alarm zone and will be lit on readers those are members of an alarm zone, once the alarm system is armed.

To disable this function and use the red LED for door locked indication, please proceed as follows:

- 1 Start the *Installer* program, choose **System settings** on the **System** menu.
- 2 Click on the **Reader red LED** tab.
- 3 Check the box **Use red LED for door locked indication**.
- 4 Click **OK**.

**Note!** This setting affects all readers on the system that are using BCLINK or RS485 connection (i.e. not Clock & Data readers). If this is checked it will not be possible to monitor alarm system status. We recommend **not** checking it if alarm zones are used.



# Dynamic IP address (DHCP) and dynamic DNS

Some network applications requires the SR34i to be able to use dynamic IP-addresses and where every controller is referred as a “name” and that the SR34i itself can perform a login (to the ISP).

This chapter describes specifically how to achieve this. There are some examples shown.

## Background

### Dynamic IP-addresses

In earlier versions of the Entro software, the SR34i is supposed to be addressed with a static *IP-address* – which is still the preferred method as long as the local area network (LAN) allows for this. (Think of a having the same telephone number all the time). Static IP-addresses are both faster and more secure.

In some facilities only one Internet Service Provider (ISP) is contracted, offering only accounts and connections using **DHCP** (*Dynamic Host Configuration Protocol*). This means that the host environment (at the ISP) “lease out” an IP-address for a short time, therefore the IP-address can be changed when the ISP renews the lease time. (We describe further on how this mechanism works in Entro).

As IP-addresses are not static, there must be a function that refers to a fixed name which can be “translated” to a concept the Internet can still understand – i e IP-addresses. This function is generally called **DNS** (*Domain Name Service*) and can be seen as a “name directory” with IP-addresses. The directory normally resides with the ISP and will itself also be accessed through an IP-address (which normally is supported together with the leased IP-addresses).

*E g a web browser can use the name [www.bewator.com](http://www.bewator.com) instead of the IP-address to Bewator. This works as long as the [www.bewator.se](http://www.bewator.se) always have the same IP-address (i e the DNS supersedes the need for remembering the IP-address to Bewator home page).*

When DHCP is used – and the ISP often changes the connected users'/computers' leased IP-address – also the DNS must be updated with new information. This is called **dynamic DNS** (DDNS) – and means that equipment can “ask” this service for the latest IP-address for a specific name.

*E g Think of changing your telephone number sometimes (because the amount of telephones are limited and an own line with a fixed number is more expensive). Still your friends have to be informed about the change – the telephone directory must be updated – each time the name is changed.*

### Login

The Internet Service Provider (ISP) sometimes needs to be sure that it is an authenticated user (SR34i) before any communication can be allowed. This requires a login with **User name** and **Password**. This is setup in each SR34i. Note that login procedures can be used/required even if static IP-addresses are used.

## Prerequisites

The following chapter describes the requirements needed to get different configurations working in a Bewator Entro system. See also further chapters on how the installation is performed.

**Note 1!** The End Users/Buyers IT-manager should always participate in the planning of a TCP/IP based Entro system. General knowledge about networking is also recommended.

**Note 2!** It might be convenient to have all SR34i available in front of you for DHCP software set up before mounting them in the correct place.

Simplified you can use handled IP-addresses in three different ways:

- 1 **All** SR34i have **static** IP-addresses (decided by IT-manager or ordered from ISP).
- 2 **One** SR34i has **static** IP-address (with name directory) – all others normally get leased, dynamic addresses (DHCP).
- 3 **All** SR34i gets **dynamic** addresses (DHCP).

## Static IP-addresses

Static IP-addresses can exist in both local area networks and/or where also the Internet is used (e g for reservation functions). Some ISP unfortunately do not allow for using static IP-addresses.

In a local area network environment (**in a company installation no special arrangements are needed**), the only aspect is how "isolated" the security system should be compared to an office network. I e if any routers, firewalls or similar software are separating the Bewator Entro from any other network equipment.

Of course the same applies for an apartment building if using the same type of network, or a company installation can use the advantage of the DHCP functions described in next section.

E g a SR34i can get a fixed IP-address (from IT-manager) and act as a host for the other SR34i, leasing the IP from an internal DHCP-server in the company.

## Dynamic IP addresses

At the moment few apartment buildings have a complete local area network installed. Instead an ISP offers different types of connection, broadband, cable or telephone modem and every tenant uses the Internet for communication to/from his home computer.

To get Bewator Entro running in an environment where **DHCP** and **Login** are used – some prerequisites must be fulfilled.

- 1 At least one ISP account (and physical connection) must exist. The goal is that every SR34i shall be able to access the Internet as well as being accessed from outside. Dependant on the ISP this can be offered in different ways.
- 2 The function for "**dynamic**" **DNS** (*Dynamic Domain Name Service*) must be established. The "Name directory" can be stored in one of two possible places:
  - One dedicated SR34i will act as "Dynamic DNS" requiring a static IP-address from the ISP, so that other SR34i's and the PC, know where the name directory is. The chosen SR34i will still be able to control door environments.
  - An externally offered public service called *DynDNS.org* is used to store the directory with network identities and IP-addresses. In this case an account with User name and Password has to be requested from this organisation. At the moment five different names are offered free-of-charge and five SR34i can immediately be used. If more SR34i are to be used an additional 20 names can be ordered for approx. \$10 annual fee (December 2004).

On the following pages two examples of how the IP-addresses can be managed.

## Configuring of DynDNS.org

Today, (December 2004) the instructions to configure an account with dyndns.org. are as follows,

- 1 Create a new account (User name and Password).
- 2 If you have your own domain you select *Custom DNS* – otherwise select **Dynamic DNS**. These choices will later be referred to in Entro.
- 3 Choose among the available domain names. If you chose **dynalias.net** an SR34i will get the network identity *Identity1.dynalias.net*.

It will be easier if you already have a list of *network identities* for all SR34i available. Note that this is not the same as the name of the controllers (as shown in a event log).

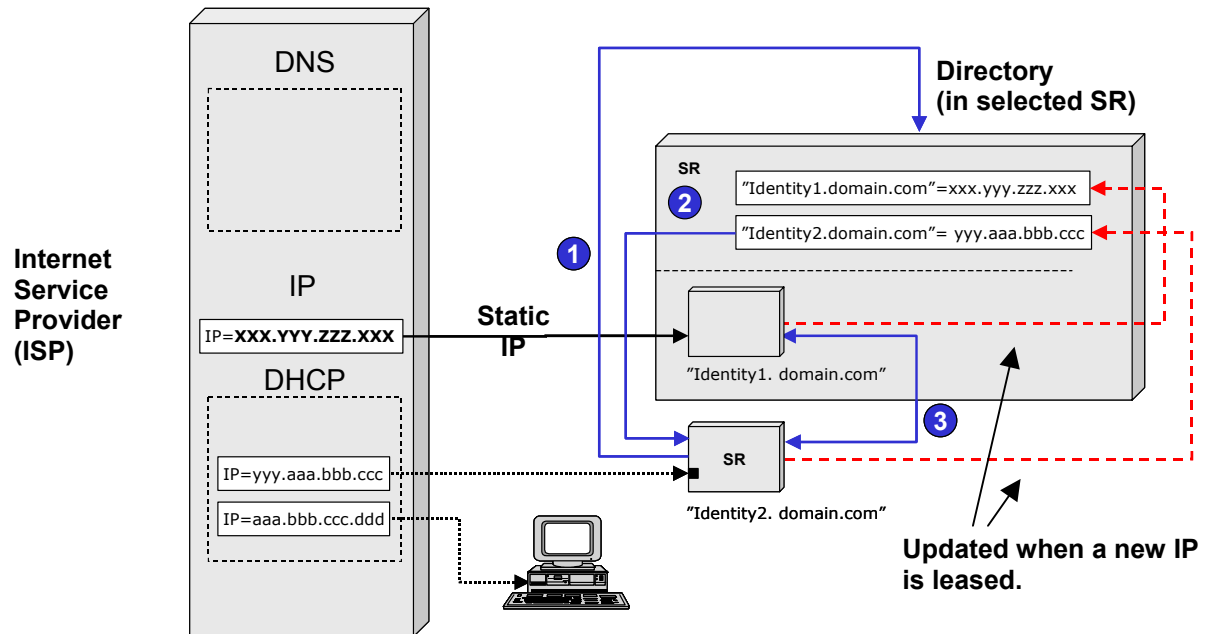
- 4 Carry on entering the identities for the remaining SR34i.
- 5 Finished.

You can read more about this on their web site by browsing to, [www.dyndns.org](http://www.dyndns.org)

## Example where SR34i manage IP-addresses

This solution requires at least one SR34i with static IP managing the “name directory” for all. (A *separate* Entro system can also use this dedicated SR34i for IP managing).

This method can be ideal for companies having a spare, static IP-address.



The following example shows what steps are performed when an SR34i #2 wants to communicate with SR34i #1:

- ① Segment controller #2 only knows the *network identity* for requested controller (Identity1.domain.com). Because communication only takes place when the IP-address is known – it has to send **request** for valid IP-address' for Identity1.domain.com. Because the SR34i (storing the name directory) has a known IP-address – the request is directly sent to this.
- ② A "name search" of **Identity1.domain.com** is done and the valid IP-address for Segment controller #1 is returned.
- ③ Now the message is sent from controller #2 to controller #1.

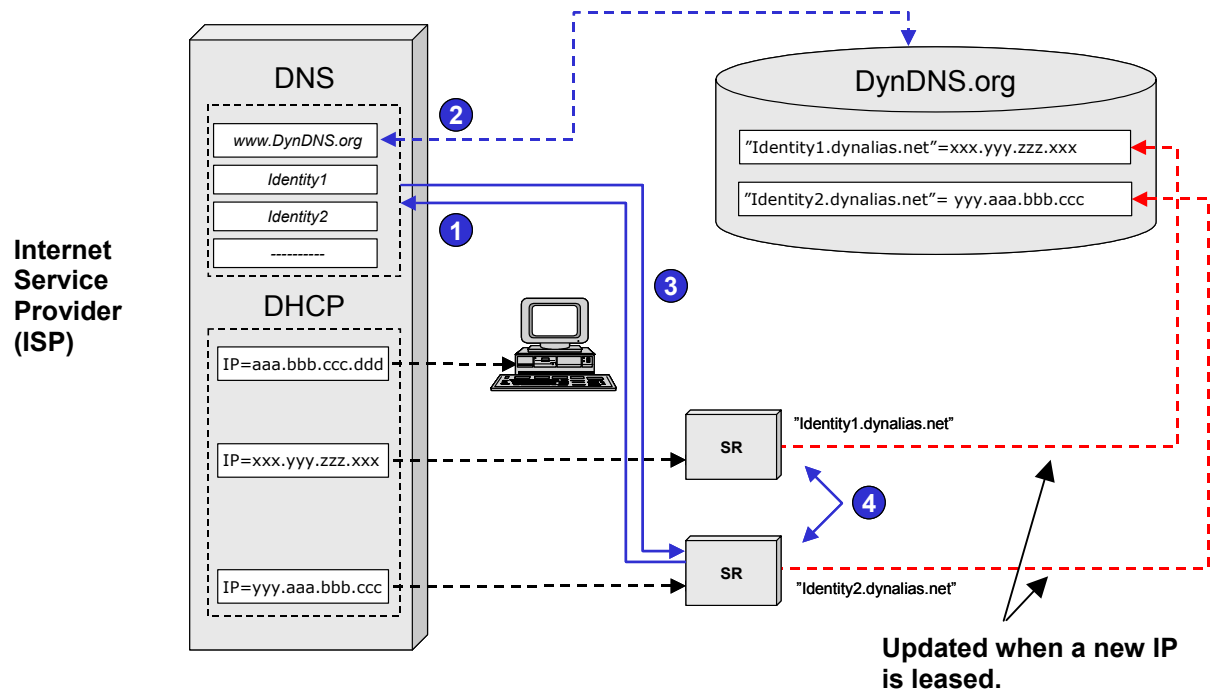
This sequence may be repeated every time any communication is established between the controllers. In principle a "name search" of IP-addresses works as a chain reaction. I.e every piece of equipment will search in his DNS, searching in his etc – until the identity is known.

If the ISP leases a new IP-address for any SR34i – that SR34i reports this to the SR34i storing the name directory.

Despite the SR34i's embedded name directory performing the search of IP-addresses, the information about the ISPs DNS must be entered, because this is used when requesting the e-mail server IP-address.

## Example when DynDNS.org manages IP-addresses

This method means that an account (with domain name) managing the “name directory” must be requested (and signed) with DynDNS.org.



Following steps are performed when an SR34i #2 wants to communicate with SR34i #1:

- ① Segment controller #2 only knows the *network identity* for requested controller (Identity1.domain.com). Because communication only takes place when the IP-address is known – it has to send **request** to the specified DNS for a valid IP-address for Identity1.domain.com.
- ② Dependant of the DNS having searched and “remembers” **Identity1.dynalias.net** and its IP-address or not, yet further searching must be done (to DynDNS). In principle a “name search” of IP-addresses works as a chain reaction. I e every piece equipment will search in his DNS, searching in his etc – until the identity is known.
- ③ When “name search” of Identity1.dynalias.net is completed, a valid IP-address for Segment controller #1 is returned to the controller asking.
- ④ Now the message is sent from controller #2 to controller #1.

This sequence may be repeated every time any communication is established between the controllers.

If the ISP leases a new IP-address for any SR34i – that SR34i reports this to the DynDNS.

## Installation and setup of DHCP

No new system components need to be installed but you should have the following information handy before starting to programme:

- Physical address (knobs) for SR34i (between 001 and 016).
- Suggested name of the segment controller (defined by the User). This will also be displayed in the event log (e.g. Controller House 1).
- Network identity for controllers (e.g. Identity1.dynalias.net)
- Information about dynamic DNS (either static IP for SR34i – or an account with user name + password at DynDNS.org).

## Basic configuration of database

We recommend that you start from a *temporary* solution that works with static IP-addresses in the SR34i, and then convert to dynamic when all information is set and programmed.

You can also wait with mounting the SR34i and instead have them in front of you and if necessary connect them to each other. The software setup is much easier if you can connect each controller via RS232 (see below).

Several parameters in the Entro database must be set to fit into a network application **based on DHCP**. Every SR34i will at power-up (after delivery) get an IP-address which probably doesn't suit the rest of the network. Therefore we recommend that the basic parameters are prepared in the PC and downloaded to the **SR34i via RS232** serial cable.

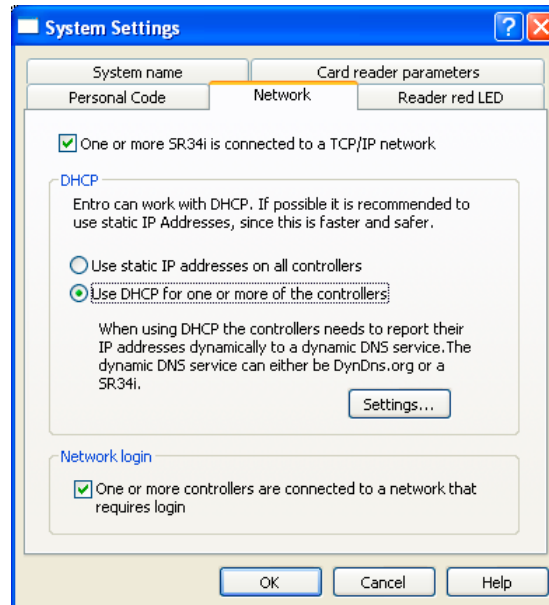
**Note!** The programming of the SR34i is done manually and one of the SR34i must be connected to a COM-port in a PC. Be sure to have the necessary RS232 cables between the SR34i and the PC available.

## Customise the database for DHCP

You must now decide on how the segment controller should communicate with each other. **All SR34i using TCP/IP** must have the **Proxy** tick box marked.

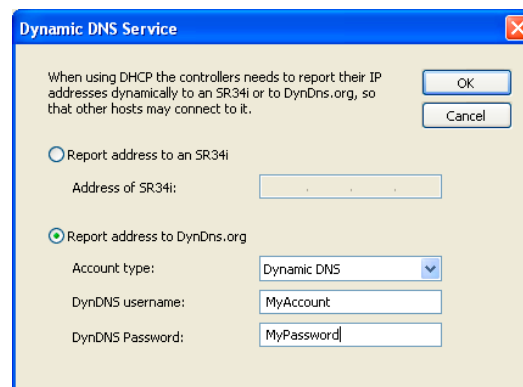
Proceed as follow to allow for DHCP-function.

- 1 Start the *Installer* program; choose **System settings** on the **System** menu.
- 2 Click the **Network** tab and the tick box **Use DHCP for one or more controllers**. Note that still some may use static IP-address.



- 3 When you have made your selection above yet another dialog box is shown where you select one of the following:
  - Use an *SR34i* as dynamic DNS server and enter the **IP-address**.
  - Use *DynDNS.org* and enter the **Account type**, **User name** and **Password**.

The screen shot shows a setup where DynDNS is used for managing the IP-addresses.



- 4 OK.

## Decide on network settings for SR34i

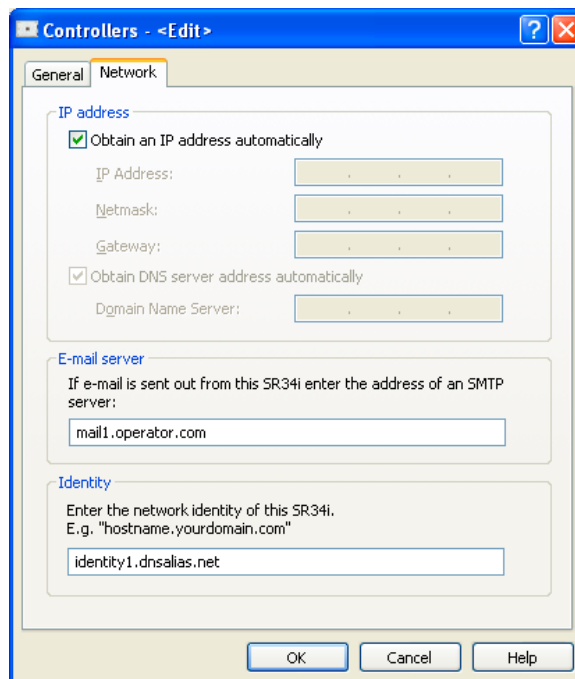
When the system allows for DHCP in SR34i some more settings must be considered.

When DHCP is selected, every controller automatically gets an IP-address and a general DNS (used for later search of IP-address to DynDNS.org).

Proceed as follows:

- 1 Start *Installer* and select an SR34i in the tab **Controllers**.
- 2 Click **Edit** - or double-click the name.
- 3 Go to the Network tab and mark the tick-box Obtain an IP address automatically.
- 4 Enter in the field **Identity** the name for the controller. If DynDNS is used it might be e.g. *House1.dyndns.net*, *Identity1.dynalias.net* or similar.
- 5 If the controller also is used for confirmations in a reservation system, enter the name of the **e-mail server**. This is obtained from the ISP. E.g. *mail1.telia.com*.
- 6 Click OK.
- 7 Repeat the steps for each SR34i using DHCP.

The screen shot below shows the above settings.





## Decide on login for SR34i

Some Internet Service Providers (ISP) requires a login. In Entro this means that every SR34i must be able to login with User name and Password.

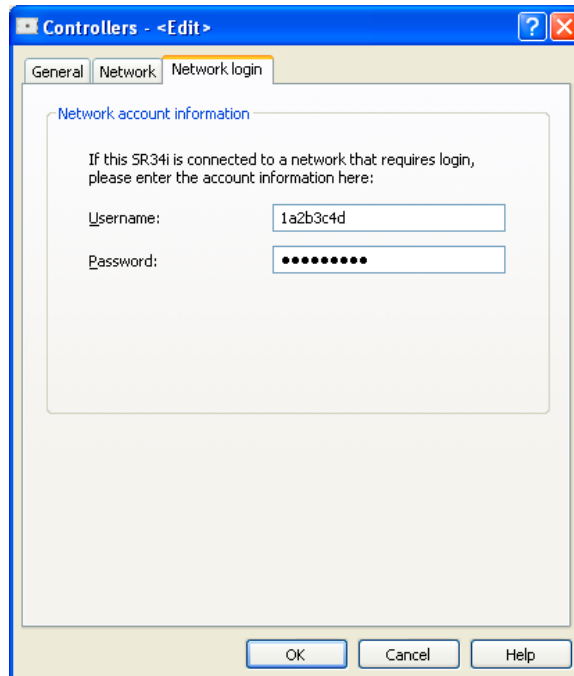
More information about the requirements should be available from the ISP.

**Note!** DHCP and/or login are not dependent of each other.

Proceed as follows:

- 1 Start *Installer* and select an SR34i in the tab **Controllers**.
- 2 Click **Edit** - or double-click the name.
- 3 Go to the tab **Network login**.
- 4 Enter **User name**.
- 5 Enter **Password**.
- 6 If the controller has a static IP address, you enter the IP-address to the DNS-server – otherwise not.
- 7 Click **OK**
- 8 Repeat the steps for each SR34i using login.

The screen shot below shows the above settings.



## Apartment building – example 1

We assume that an apartment organisation shall install a new Bewator Entro system in three different houses, where we use three SR34is. We now describe how the controllers are configured with **DHCP** and we use **DynDNS** because the ISP does not allow static IP addresses. Also Internet login is required for communication.

A laundry room also exists in one of the buildings where the Entro reservation system shall be used, the tenants will use their home PC to make bookings and get confirmations.

The requirements for this are:

- A LAN must exist in each building where SR34i is installed.
- An Internet account must be available to allow for identities for the SR34is.
- One SR34i must also have the CF8 flash memory installed for reservation functions.
- The final system will have an administration PC installed.

The three controllers can be prepared in advance (before mounting) because they include a battery keeping the information (database) until the final installation is done.

Follow these steps:

- 1 Sign up for an account with domain name **dynalias.net**, User name **MyAccount** and the password **MyPassword**.
- 2 Apply these settings to the SR34i:

<b>SR34i</b>	<b>Name (in log)</b>	<b>Network ID</b>	<b>Login information</b>
1	Controller House 1	house1.dynalias.net	<user1> + <password>
2	Controller House 2	house2.dynalias.net	<user2> + <password>
3	Controller House 3	house3.dynalias.net	<user3> + <password>

- 3 Install the software in the PC according to chapter *Basic setup of database (for DHCP)*. Enter *House1.dynalias.net* as network ID for the first controller (that the PC will use for communication).
- 4 Configure according to chapter *Customise the database for DHCP* and select **Login** and **Use DHCP for one or more controllers**.
- 5 Select the alternative to report to **DynDNS.org** and enter the Account type *Dynamic DNS*, User name *MyAccount* and password *MyPassword* and exit.
- 6 Programme all SR34i manually with the **New** button and enter name etc.
- 7 Proceed with the tab **Network** and mark the tick-box **Obtain an IP address** automatically (also the DNS address will then be allotted).
- 8 Enter the **Identity** according to the above table. I e *House1.dynalias.net* etc. Simultaneously you enter the name of the ISPs e-mail server (e g *mail1.telia.com*) to prepare the controller to send confirmations.
- 9 Click the tab **Network login** and enter the details <user1> + <password> and exit.
- 10 Set up all SR34i in the same way.

### **Download database to SR34i**

When the information for all SR34i and their network settings is saved in the PC, you must be sure the database is downloaded to each of the controllers. This is made through RS232 because the network is not yet running, and is adequately made when the overall system software is installed.

- 1 Jumper to correct address in SR34i, power-up and connect only the first controller via **RS232** to COM port in PC.
- 2 Start *Installer* and wait for the database to download (the icons become green) and shut down the program complete (right-click on the icon and select Close Entro).
- 3 Address, connect and download to the rest of the controllers each at a time via RS232.
- 4 Mount the CF8 card in chosen SR34i. (Be sure you have the correct CF8 content)
- 5 Mount all controllers in the correct place and verify that local area network sockets are available (and connected to the ISP).  
  
Door controllers and readers can of course be mounted and connected to SR34i when setup is performed.
- 6 Finished.

### **Connect PC and other equipment**

- 1 Connect the ordinary PC and verify that communications are working.
- 2 As soon as the Installer program communicates with all SR34i, all door controllers will be displayed on the screen. Carry on and programme these according to the manuals.  
  
Because the PC software knows every SR34i, it discovers immediately if some SR34i do not communicate.
- 3 If the reservation terminal **InfoPoint IP810** shall be used – this must also be setup according to its manual. E g you select that it will use DHCP and will get its IP-Address automatically.
- 4 Programme all necessary settings for the Entro system according the ordinary manual. Do not forget to change the encryption key.
- 5 Now also the **End Users must be informed** about the IP-address (alternatively the www-address) to where the web browser should search for – to make reservations.
- 6 Finished

## Apartment building – example 2

In this example the ISP allows for one (1) **static IP** for one SR34i whilst the rest will be allotted dynamic IP (DHCP). This might also be the case in a company where the number of "internal" IP-addresses is limited.

We also assume the login is not necessary to use the network.

Because the IP-address in one SR34i will not be changing, we can let other controllers dynamically report any changes to this dedicated SR34i. I.e. this SR34i contains the name directory (with IP-addresses).

The network IDs (names) for the different SR34i's will be dependant of the ISP (house1.telia.com, house1.swipnet.se or similar).

Proceed as follows:

- 1 Install the software in the PC according to chapter *Basic setup of database (for DHCP)*. Enter *House1.dyndns.net* as network ID for the first controller (that the PC will use for communication) and select COM-port.
- 2 Select the SR34i to be used and enter the IP-address. This SR34i will store names and IP for other controllers
- 3 Configure according to chapter *Customise the database for DHCP* and select **Login** and **Use DHCP for one or more controllers**.
- 4 Programme all SR34i manually with the **New** button and enter name etc.
- 5 Carry on with the tab **Network** and enter (for the first SR34i) the static IP-address, Netmask and Gateway. (This information you should have obtained from the ISP or IT-manager).
- 6 Whether the controller has a static IP or not you have to enter the address to the domain name server (DNS). This is necessary to get e-mail confirmations in reservation to work. Note that also this IP-address should be obtained from ISP/IT-manager).
- 7 Enter the **Identity** according to table above. I.e. *House1.dynalias.net* etc.
- 8 Enter the name of the ISPs e-mail server (e.g. *mail1.telia.com*) to prepare the controller to send confirmations
- 9 Finally perform action according to preceding chapters *Download database to SR34i* and *Connect PC and other equipment*.
- 10 Finished.

# Programming - User

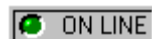
## Start the system

This is how to start Bewator Entro:

- 1 In **Windows**, go to the Start menu; choose **Program, Bewator Entro** and then **Entro**. The login window is displayed.
- 6 Enter <user name> (bewa) in the **User name** field and press TAB.
- 2 Enter <password> (pass) in the **Password** field.
- 3 Select **System** to use (if several exists).
- 4 Click **OK**. Now you are logged on. Bewator Entro's main window is displayed.

## On-line, off-line and database information

In the bottom right of the box there are two indicators:



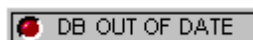
If the text ON LINE and a green indicator are displayed, the PC and the Bewator Entro programme are connected to the access control system.



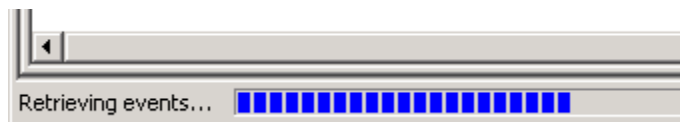
If the text OFF LINE and a red indicator are displayed, Entro has no contact with readers and controllers. This means that the information registered in the PC does not reach the segment controllers.



If the text DB UP TO DATE (DB = database) and a green indicator are displayed, all segment controllers have the same information as the PC.



If the text DB OUT OF DATE and a red indicator are displayed, the segment controllers do not have the same information as the PC. Note that a certain amount of time may pass before the information has reached all segment controllers and that the system has to be ON LINE for this to be possible.



You can also look at the status bar to see how far the transferring of data to the PC has gone.

**Note!** The default setting is that you will automatically be logged out of the system if no task is performed within 15 minutes. In the *Entro* program you may set the desired number of minutes or disable auto log-off (described on page 64).

## Entro serial communication (Entroser)

In the bottom right of the window task bar the following symbol is displayed:



Regardless of using network or direct cable to the PC the following information applies.

When displayed, Entroser (Entro serial communication) is running, this is a required condition for events to be displayed on the PC's screen. Entroser will be running even if you exit Entro. Click the right mouse button on the symbol to display a menu, from where you may start Entro (if it is not running) and the Door control programme. You can also exit Entroser from here. Shutting off the PC will also exit Entroser.

The indicators (green or red "LEDs") function as explained above.

## Shortcuts

The *Entro* software consists of five main tabs:

- Time schedules
- Doors
- Zones
- Access groups
- Persons

We recommend that you follow the above order when you set up the system according to your specifications. In the following sections we will follow this order.

However – there are two nice shortcuts sometimes available in the software, to help creating, editing or deleting information.



Shortcut to Access groups



Shortcut to Time schedule

E.g. when you create a new person, click on the shortcut *Access group* if you have not yet created a suitable one. In the same manner you can click further to *Time schedule* if you want to create or edit a time schedule. In all cases you will come back to the previous step when you exit the menus.

## Time schedules – general



Bewator Entro uses three types of time schedules:

- Access Control (used for doors setting and access groups)
- Intruder alarm zones (automatic activation of intruder alarms)
- Reservation intervals (see more in the chapter *Reservation*)

## Time schedules – access control

The first thing to do is to identify the different types of working hours or other time divisions in the premises. Then decide what time schedules are to be used. Finally, decide what time zones are to be used within each time schedule.

- 1 Start the *Entro* program.
- 2 Click the **Time schedules** tab.
- 3 Click **New**.

For new time schedules a wizard is invoked which will help you programme the required functions. For existing time schedules the tabs are shown (displaying the same information).

The wizard also allows for directly programming the Half days, Holidays and holiday periods. See *Enter specific half days, public holidays and holiday periods* section.

- 4 In the **Name** field, enter the name of the time schedule e.g. Office Hours, and press TAB.
- 5 In the **Name** field of **Time zone 1** square, enter the name of the first time zone, e.g. Work Hours, and press TAB.
- 6 In the **Name** field of **Time zone 2** square, enter the name of the second time zone, e.g. Lunch Time, and press TAB.
- 7 **The** cursor is placed in the **From** field far left, next to the **Mon.** (Monday) text in the **Time zone 1** square.
- 8 **Enter** the first time interval for Mondays. Enter the time by typing four digits in succession, e.g. 0800 for 8.00. Continue with the next time interval, if any.
- 9 Press TAB until the cursor is placed in the first **From** field in the **Time zone 2** square.
- 10 Enter the time intervals defined for **Time zone 2**.

**Note 1!** The time intervals must not overlap. If one interval in Time zone 1 ends with 1200, the following time interval in Time zone 2 must start with 1201.

The unspecified hours i e the remaining time, are always called **Other time**. This time zone is the third time zone.

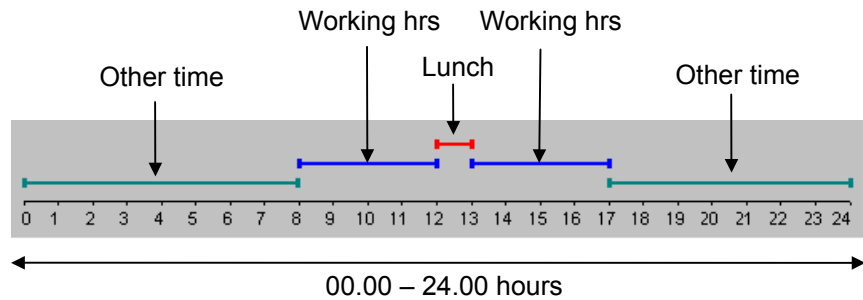
**Tip!** If you create separate time schedules for Doors and Access groups, you can easily change times for the security level of the door – or change times for only the authorities of different access groups

## Copy time intervals

You will probably want to use the same time intervals for Tuesday's and the other weekday's working hours. This is how to copy the time intervals defined for Monday.

- 1 Place the pointer above the Mon. text and click the right mouse button. A menu is displayed.
- 2 Choose **Copy times** using any mouse button.
- 3 Place the pointer above the Tue text and click the right mouse button. The menu is displayed again.
- 4 Choose **Paste times**. The time intervals are pasted – the ones you have defined for Time zone 2 as well.
- 5 Follow steps 3–4 for the remaining weekdays using the same time intervals. Should the working hours be shorter on Friday, it is easy to change that interval.

The time intervals you have defined are illustrated graphically at the bottom of the window for you to check that you have programmed the times correctly (see the example below).



- 6 If you want to use the same half days, public holidays and holiday periods for all time schedules, i.e. you have only completed one Holidays chart, click OK. The Time schedules tab is redisplayed.

If you want to define specific half days, public holidays, or holiday periods for this time schedule, go to the Enter specific half days, public holidays and holiday periods section below.

- 7 Set up information for the next time schedule in the same way. Start by clicking New.

**Hint 1!** Instead of clicking New you can click **Duplicate**. If the information is similar, you need only change a few pieces of information, e.g. the name of the time schedules.

**Hint 2!** You can select a time schedule and right-click to invoke the same commands as the buttons.



## Time schedules - Intruder Alarm zones

If the installer has installed an intruder alarm system (controlled by the Bewator Entro) you can make use of special time schedules for automatically activating it). You can programme these schedules separately, or when you create the Alarm zones. Note that the intervals can cover the midnight hour.

- 1 Start the *Entro* program.
- 2 Click the **Time schedules** tab.
- 3 Click **New**.

For new time schedules a wizard is invoked which will help you programme the required functions. For existing time schedules the tabs are shown (displaying the same information).

- 4 Enter the name of the time schedule under **Name**.
- 5 Click on **New** to create the first interval. E g Monday evening.
- 6 In the list box **Start** enter the weekday and time. E g Monday 18:00.
- 7 In the list box **Stop** enter the weekday and time. E g Tuesday 07:00.
- 8 Then chose how often the intruder alarm will be activated. E g every 60 minutes.
- 9 Click **OK**.
- 10 Repeat step 3 – 7 for every interval. E g Tuesday evening, Wednesday evening etc.

## Enter specific half days, public holidays and holiday periods

The most common working hours in an office are Monday to Friday with Saturdays, Sundays and holidays off. Certain days, e.g. the day before a holiday, you might only work a half-day. Perhaps the company applies a fixed holiday period in July.

To make the system understand that holidays, half days and holiday periods should not be treated as ordinary working days, this information must be programmed. Holidays and holiday periods are automatically given the time zone **Other time**.

Proceed as follows:

- 1 Click the **Time schedule** tab and mark the time schedule and click **Edit**.
- 2 Click the **Half-day** tab and **New**. A window is displayed.
- 3 Enter the desired information. In the *General half-days, public holidays and holiday periods* section. Later in this manual you will find instructions on how to enter the information.
- 4 If you want, you can mark the tick in the **Use Global half-day** table box. Then the days programmed in the *Global Settings* menu in the Time schedule tab will be displayed - and used by this time schedule.
- 5 Enter the desired information about other **holidays** and **holiday periods** in the same way.

## General half-days, public holidays and holiday periods

The next step is to programme half days, public holidays and holiday periods to be used generally in the premises. Remember that you can combine both general and unique settings (in each time schedule).

### Half days



Proceed as follows:

- 1 Start the *Entro* program.
  - 2 Click on **Global Settings** in the **Time schedule** tab.
  - 3 On the **Half days** tab.
  - 4 Click **New**. The window Half days is displayed.
  - 5 Enter the date of the first half-day in the yymmdd format, e.g. 000430, or click the **Calendar** button (in the *Calendar* section on page 62 you will find instructions on how to use the calendar).
  - 6 Place the cursor in the leftmost **From** field under the **Time zone 1** heading.
  - 7 Enter the working hours to apply for the first time interval during **Time zone 1**. Type four digits in succession, e.g. 0800 for 8.00.
  - 8 Enter the working hours to apply for the second time interval during **Time zone 1**.
  - 9 Enter time intervals for **Time zone 2**, if any, in the same way.
- Note!** The time intervals must not overlap. If an interval in **Time zone 1** ends with 1200, the following time interval in **Time zone 2** must start with 1201.
- 10 Click **OK**. The **Half days** tab is redisplayed with the new half day registered.
  - 11 Proceed the same way to register the next half-day according to the chart.

## Public holidays



Below you will find instructions on how to programme public holidays for the year. Holidays belong to the **Other time** zone.

- 1 Click the **Public holidays** tab.
- 2 Click **New**.
- 3 In the **Date** field, enter the date of the first holiday in the yymmdd format, e.g. 000501, or click the **Calendar** button (in the *Calendar* section on page 62 you will find instructions on how to use the calendar).
- 4 Click **OK**. The Public holidays tab is redisplayed with the date filled in.
- 5 Click **New** and programme the next holiday accordingly.

## Holiday periods



- 1 In this section you will find instructions on how to enter holiday periods, if any. Holiday periods belong to the time zone **Other time**.
- 2 Click the **Holidays** tab.
- 3 On the **Holidays** tab, click **New**.
- 4 Enter the start date of the holiday period in the yymmdd format, e.g. 000630, or click the **Calendar** button (in the *Calendar* section on page 62 you will find instructions on how to use the calendar).
- 5 Enter the end date of the holiday period in the yymmdd format, e.g. 000831, or use the calendar.
- 6 Check that the information is correct, and then click **OK**. The **Holidays** tab is redisplayed with the holiday period filled in.
- 7 Click OK to close the **Holidays** tab.

## Doors



The next step is to programme information about doors. Depending on what the doorcentrals/readers are used for, different parameters can appear in the menus.

- 1 Start the *Entro* program and click the **Doors** tab.

Since the installer has already allocated addresses for the doors they are also registered with a name in the system.

- 2 Select the name (by clicking it) of the door whose information you want to enter.

- 3 Click **Edit**.

The name of the door is displayed in the Name field.

- 4 Enter the desired opening time in the **Opening time** field. Click the up- or down arrow respectively to increase or decrease the value, or enter the desired value in the field directly.

The time available to open the door after a valid card has been swiped and/or a valid PIN code has been entered. If the door is not opened during this time, it is locked again. Recommended opening time is 7 seconds. You can choose an opening time between 1 and 99 seconds.

- 5 Enter the door held warning time in the **Door held open warning time** field. Click the up- or down arrow respectively to increase or decrease the value, or enter the desired value in the field directly.

If the door is still open when the opening time is over, a buzzer sounds at the door for the time set as door held warning time. The buzzer reminds the person entering to close the door immediately as an alarm is about to go off. Recommended door held warning time is 20 seconds. You can choose a time between 1 and 99 seconds.

- 6 In the **Time schedule** field, choose the time schedule applying to the door. Click the down arrow to display a list of available time schedules (the time schedules you registered earlier). You can also click on the clock icon to *Create*, *Edit* or *Copy* a time schedule. Then choose the desired time schedule by clicking the name.

- 7 Choose **security levels** for the different time zones in the time schedule. Click the down arrow to display a list of available security levels. Then choose the desired security level by clicking the name.

- 8 Choose the suitable security level to apply to the reader in off-line condition (e.g. during a communications breakdown) in the same way. Persons belonging to the **Priority group** are the only ones that can open doors in an off-line condition. This is only true of doors where the DC22 or DC12 door controllers with additional readers are installed. For doors connected to DT05 door terminals, you can only choose whether the door should be locked or unlocked.

- 9 Click the **Advanced** tab.

- 10 Enter the choices you have made for the door concerning **access registration**, **remote opening** (exit request) and **background lighting**.

- 11 If you are using a motor lock, select which time zones the **motor lock** should be unlocked.

- 12 Select the **Motor lock stays locked...** check box if the motor lock should remain locked until the first person unlocks the door, e.g. in the morning.
- 13 Enter whether the internal buzzer should sound on key presses or not.
- 14 Select the Allow remote control of this door check box if the door will be operated from a PC, e.g. opened, via the Door and event monitor program.
- 15 You can select how the exit request input will act (pulsed):
  - **Marked** means that the door is unlocked for the maximum *opening time* from the moment the input is activated.
  - **Unmarked** results in the opening time starting from the moment the input becomes inactive. I.e. the door can be externally controlled and the lock relay can be activated longer than the opening time.
- 16 Select if this door allows for a temporary changing of security levels to Unlocked or Group code by a caretaker. See chapter *Caretaker* function on page 68 on how this is managed at the door.
- 17 If lift control is applied, you may go to the **IOR6 Relays** tab and activate the desired relays during certain time zones. By activating the relay for a specific floor during a specific time zone, the floor will be accessible without the use of cards or code.
- 18 Click **OK**.
- 19 Enter information about the next door in the same way.

**Hint!** If you select a door and right-click you are able to *Edit* settings – or *Show persons* to see people authorised at this door.

## Access groups



Before you decide on access groups, you should identify the departments or sections in the premises, what staff groups should have access to these departments and during which time zones they should have access.

For example, the office staff may consist of people working in a number of different departments. If you do not want the reception staff to have access to the research department's doors you can programme this.

- 1 Click the **Access groups** tab.
- 2 Click **New**.
- 3 Enter the name of the access group in the **Name** field.
- 4 If a common group code is to be used, enter the code in the **Group code** field.

**Note!** Group code cannot be entered if *PIN without card* is allowed (this can be set in the Bewator Entro Installer).

- 5 Choose the time schedule for the group by clicking the desired alternative in the list next to the Time schedule prompt.  
You can also click on the clock icon to *Create*, *Edit* or *Copy* a time schedule.
- 6 Mark the tick box **Caretaker** if this group is allowed to temporarily change security levels for certain doors.

**Note!** This will also give access to all doors in a Reservation system (without reservation).

- 7 Select the doors that the persons in this access group should have access to and during which time zones they should have access.

For example, if you want the group to have access to the entrance 24 hours a day, select all check boxes for that door.

If lift control is applied, the floor numbers will be displayed under the name of the reader controlling the lift. Select the floors to which the group should have access.

- 8 Click the **Alarm and entrance limitations** tab (if this is displayed).
- 9 Select the suitable alarm by-pass rights for this access group.
- 10 If needed, select the desired entrance limitations for the group and the doors the group has access to. This can only be done if an entrance limitation zone has been created in Bewator Installer.
  - **Counter.** Used if access should be limited to a certain number of entries. Later you may, for each individual people, specify the number of allowed entries (double-click the desired person on the **Persons** tab and click the **Duration** tab. Can be combined with limited access.
  - **Limited access.** Used if access should be limited to a certain number of entries per day (can be limited further to certain time intervals during the day). Limited access is specified in Bewator Installer on the **Zones** tab, **Entrance limitation**). Can be combined with the counter.
- 11 If the access group should also have access to a reservation object, click on the **Reservation object** tab and select the object(s). See Reservation on page 80.
- 12 Click **OK**.
- 13 Set up information about the next access group in the same way. Start by clicking **New**.

**Hint 1!** Instead of clicking **New**, click **Duplicate**. If the information is similar for the next access group, you need only change a few pieces of information, e.g. name and group code.

**Hint 2!** You can select an access group and right-click to invoke the same commands as the buttons.

## Persons

The next step in the programming is to register the persons to have access to the premises and to divide them into access groups. First however, you must make a few common settings.

Remember that there are commands in the software for importing information from external files (e.g. Excel). Read more on page 70.

### General settings

Two settings affect the **Person properties** window where you enter information about persons. To make the settings, proceed as follows:

- 1 Choose **System settings** on the **System** menu.
- 2 In the two fields, **Title for free data field**, in “Persons” screen field, you can enter a text of your own choice. This text will be displayed as a field title in the **Person properties** window. For example, enter **E-mail**: (there is only room for 10 characters) if you want to be able to enter an e-mail address for each person you register.
- 3 There are two alternatives for setting the individual PIN codes:
  - Make sure the button next to **At PC** is selected if you want to set the person’s PIN code on the PC.
  - Make sure the button next to **At Door terminal** is selected if each person should be able to choose his own PIN code at a door terminal (how this is done is described in the *Setting/changing the PIN code* section in the *Using Bewator Entro* chapter).

**Note!** You can not change the method of entering the PIN-code during operation. In case all PIN-codes have to be re-entered again. Therefore you should carefully consider the method.

- 4 Click **OK**.

### Information about persons



To enter information about the people who should have access to the premises, take the **Persons** chart and follow the instructions below.

- 1 Click the **Persons** tab and Click **New**.
- 2 Enter the name of the first person in the **Name** field. If you enter the last name first, the names can be sorted in alphabetical order according to last name when you programme the information.
- 3 Enter the desired information in the free fields (see the previous section). Maximum 40 characters.  
**Note!** If confirmation of a reservation is to be sent, the first field must be used for holding the persons **e-mail address**.
- 4 The field **Member Group no** is mainly intended for setting the authorities in the *Reservation system* but can be used as a free field for numerical information. Maximum six digits. You have the choice of a letter prefix.
- 5 Enter the person’s eight-digit card number in the **Card No** field. If you have a keyboard with a built-in card reader you can swipe the card through the reader instead.

**Note!** If personal code without card is allowed (this can be set in Bewator Entro Installer) and the person desires this alternative, click the **Personal code without card** check box. Then enter the desired code in the PIN Code field. Do not enter any card number.

- 6 If you have chosen the option to set the person's PIN code at the PC, enter the desired four-digit code in the **PIN code** field. Next time you edit this persons' properties you will see stars \*\*\*\* in the field.  
  
If you have chosen the option enabling each person to choose his PIN code at a door terminal, the field is greyed out.
- 7 In the **Access groups** square, the access groups you have defined are displayed. Choose which access groups the person should belong to, by clicking the box to the left of the desired access group. You can choose up to six access groups per person. You can also click on the group icon to *Create*, *Edit* or *Copy* an access group.
- 8 A tick is shown in front of chosen groups. The group's name is displayed in the **Selected Access groups** square. If you want to remove a group, double click the name in the **Selected Access groups** square. The name disappears. You can also click the tick in the box.
- 9 Beside the card number there is a tickbox which shows if the the card (person) is **Active** (valid) in the system. This means it is possible to keep settings for a card that is not yet authorised for use. This can also be changed by right-clicking a name in the card list.
- 10 Click the **Duration** tab.
- 11 In the Start at field, enter from which date the person should be authorised in the system. Today's date is automatically displayed.
- 12 If you want to choose another date, enter the date directly, using the yymmdd format, e.g. 000521, or click the Calendar button (in the *Calendar* section on page 62 you will find instructions on how to use the calendar).
- 13 The **Until further notice** alternative is pre-set, which means that the person is authorised in the system until you or another system user registers an end date. You can however enter an end date straight away. Click the button next to **End at** and enter the desired date.
- 14 Select **Restrict** and enter the maximum number of entries allowed, if the person's access rights to certain doors should be limited. Use this alternative if the person belongs to an access group with entrance limitations.
- 15 Click **OK**. The **Persons** tab is re-displayed with the name of the person you registered.
- 16 Register the next person in the same way. Start by clicking **New**.

**Hint!** You can select one (or more) persons and right-click – and you can choose among several commands. E.g. to make the card inactive, show authorised doors, export information etc.

### **Register unknown cards from the Door monitor program**

Sometimes there will be "unknown cards" displayed in the event log window of the Door Monitor program. You can easily make a card valid for a new user by right-clicking on the card number. A new window will be shown where you enter information (as above section).



### **Duplicate a card**

Instead of clicking **New**, click **Duplicate**. If the information is similar you need only change a few pieces of information, e.g. name and card number. You may only need to change a few digits in the card number.

**Hint!** You can also select a card and then right-click to Duplicate the card.

### **Duplicate to several cards**

In a new system the card numbers are often in a series. You can easily programme these into Entro by using the extended duplicate function. Proceed as follows:

- 1 Enter the first card as usual.
- 2 Select the card to duplicate, if not marked, and click on the **double arrows** to the right of the Duplicate button.
- 3 In the field **Number of copies** enter the amount of duplicates you need.
- 4 Enter the **first card number** – or use the suggested (which is one higher than the selected card).
- 5 In the **Name field** there are two choices:
  - Click the actual name and decide what **number to add** to it. The card number is then incremented with one and the name will get a suffix (added with one for each).  
E g if a name Visitor is marked in the above – the next name will be Visitor – **x** (where **x** is the entered number).
  - Click **Same as card number** - and the card number is incremented and copied to the Name field.
- 6 Click **OK**.

The same access group settings etc will apply to these duplicates.

### **One person – multiple cards**

It is possible for a person to have multiple cards. E g when using one type of card in the office and another for parking.

You enter in the tab **Extra cards** the *names* and *card numbers* to be valid. Theses names will be shown in the event log. Normally the card is valid immediately, but you can deactivate it and make it invalid.

The PIN-code and access groups will be the same for all cards.

### **Show persons authorities for doors**

In the list of persons it is easy to get information about the authorised doors of a specific person. Proceed as follows:

- 1 Start *Entro* and the list of persons are displayed.
- 2 Select a person.
- 3 Right-click and choose **Show doors** and a list of the doors is shown.
- 4 Click on Close (or Print).

## Register System Users



In Bewator Entro you can register several system users, i.e. several people with authorisation to programme the system.

**Note!** The people appointed as system users can also be registered in the system as persons. In the *Information about persons* section on page 55 you will find instructions on how to do this.

This is how to register system users:

- 1 Start the *Entro* program and choose **System users** on the **System** menu. The names of existing system users are displayed in this window. If you have not registered any system users yet, the window is empty.
- 2 Click **New**. The **System users** window is displayed.
- 3 Enter a suitable name in the **User name** field.
- 4 Optionally you can tie a card to this User by clicking the down arrow in the next field to display a list of registered persons. This may be used in applications using a physical card for login.
- 5 Select the desired name.
- 6 Choose a password and enter it in the **Password** field (16 characters at the most).
- 7 Enter the password once again in the **Verify** password field.
- 8 Choose the desired user level for the system user you have registered.

**Note!** The first time you register a system user you can only choose the **All rights** level. The reason for this is that there has to be at least one system user with authorisation to perform all tasks in the system. Also note that the user name **bewa** and the password **pass** will disappear as you register a system user for the first time.

- If the person should have authorisation to make all types of changes in the system, choose **All rights**.
  - If the person should have authorisation to all functions except the ones reached from the **System** menu, choose **All rights except system properties**.
  - If the person should only have authorisation to register, change and delete information about persons, choose **Person properties only**.
  - If the person should have authorisation to remotely open doors with the PC in the *Door monitor* program.
  - If the person is an **Installer**.
- 9 Select the **door& event filter** to use, enter the **computer** and the **folder** to store events on for this System User. You can read more about filters on page 60.
  - 10 Click **OK**. The List of system users window is redisplayed with the name of the new system user.
  - 11 Click **Close**. If you exit Bewator Entro now you can log in with the user name and password you just registered.

If you want more people to have authorisation to programme Bewator Entro, proceed the same way to register the information

## Access registration

Every SR34i is striving to receive *all* events in the system storing them in its event buffer. I.e events occurring in any part of the Entro system is mirrored between the segment controllers.

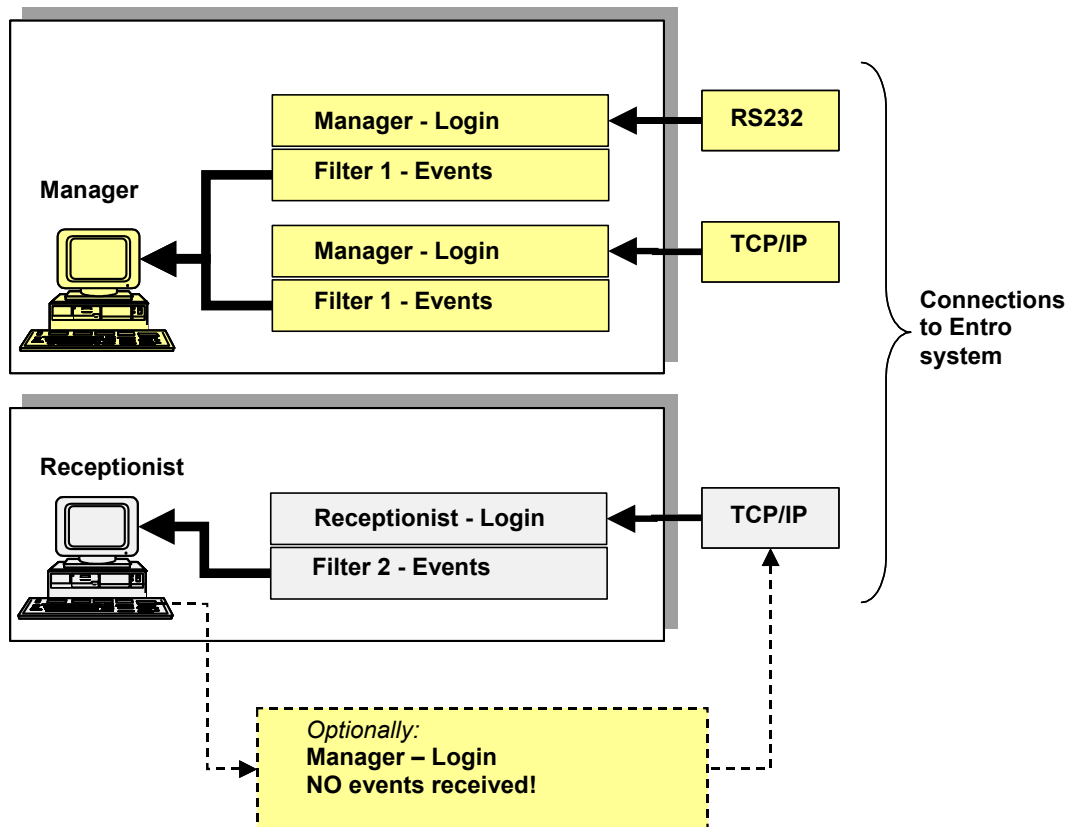
Depending of how the set up is done for each System users, the registering, alarm reporting and graphical symbols will now be displayed according to the selected filter. See the illustration below where two separate filters send information to connected PCs.

Remember that all controllers will attempt to get all events for making further decisions (filtering, alarm reports etc.)

### Decide on PCs to retrieve events

When you create a System user, you must choose which PC to be his/hers 'primary' PC, where events only are stored for this System User. Also you have to select which event filter and door filter to be used for this System User.

This means that if the same person using his/her level of authorisation logs onto **another connection (PC)** the events will **NOT** be stored on that computer.



In the *Door and event monitor* chapter on page 73 you will find instructions on how to start the monitoring programme on your PC.

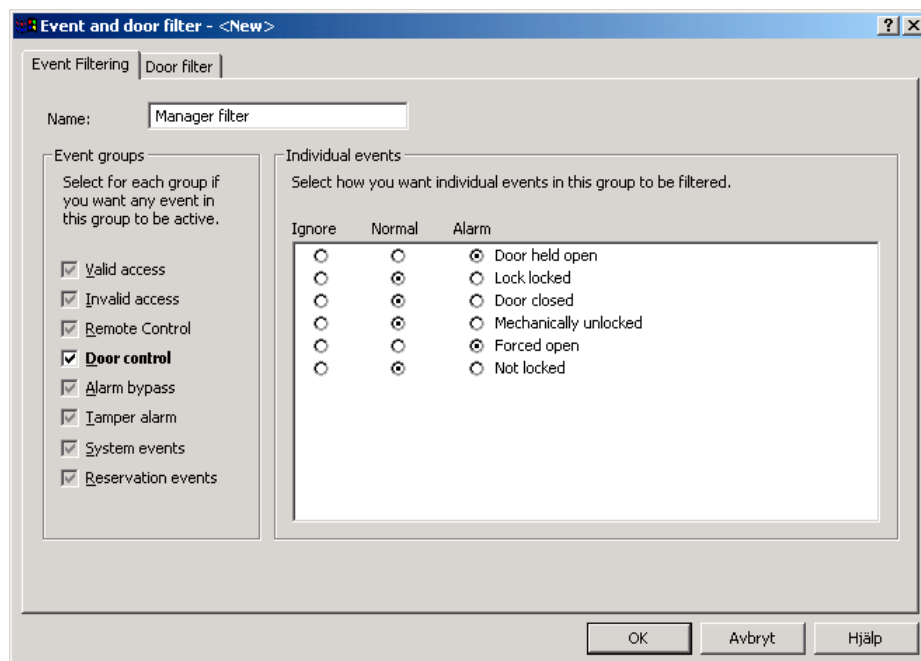
## Event and door filters

Event and door filters are used in different ways in the Entro environment:

- To control **common alarm** outputs in the IOR6 (and pop-ups on the screen)
- Reduce the amount of events stored on hard disk.
- Control which events and door symbols to be displayed on the screen for a particular System user.
- Searching in the event archive.

Normally the system uses a standard event filter with recommended settings and displays all doors graphically on the connected PC. You do not need to change anything.

The screen shot below shows a typical setting for the door monitor type of events.



## Decide on name for new event filter

In every place in the software where you can/should select a filter you can **create**, **edit** and **store** your filter settings (to be able to re-use them). You can create a maximum of **32 event different filters**.

You can change filter settings – and then name it and save it. As follows:

- 1 Click on the icon beside the list box. Then choose **New filter**.
- 2 The **Event filtering** window is displayed. Enter the name for the new filter.
- 3 For each **Event group**, choose which events are to be reported.

Click the text, e.g. Valid access, to view the events belonging to this Event group. Then filter the events.



<b>Ignore</b>	The event is not registered and cannot be retrieved later.
<b>Normal</b>	The event is shown in the Door and event monitor and on printouts.
<b>Alarm</b>	The event is defined as an alarm event, i.e. is displayed in red in the Event window.

To ignore all events in an event group, simply deselect the check box in front of the event group's name.

**Note 1:** The events **Exit request** and **Group code** are by default set to ignore and are not registered.

**Note 2:** Events marked **Alarm** are always printed, (only to the printers) even if you have requested nightly printouts only for this particular door.

**Note 3:** Events marked **Alarm** will also activate any Common alarm relay in any of the IOR6 (if activated). In addition, alarm-marked events are displayed as pop-ups on the PC's screen. The pop-ups are displayed even though the **Door monitor** programme is not running, on condition that *Entroser* is running (see page 46).

- 4 Click **Door filter**. Decide on which doors are to be displayed graphically on the screen.
- 5 Click **OK**. The Controllers window is redisplayed. Choose another segment controller (tab) and enter information about this segment controller in the same way.

## Managing Event filters

You can also edit, copy or delete event filter settings. Mark the filter and click the button - but choose *Edit filter*, *Copy filter* or *Delete filter*.

You will get a warning message if you try to delete a filter that is in use.

## Use event filters

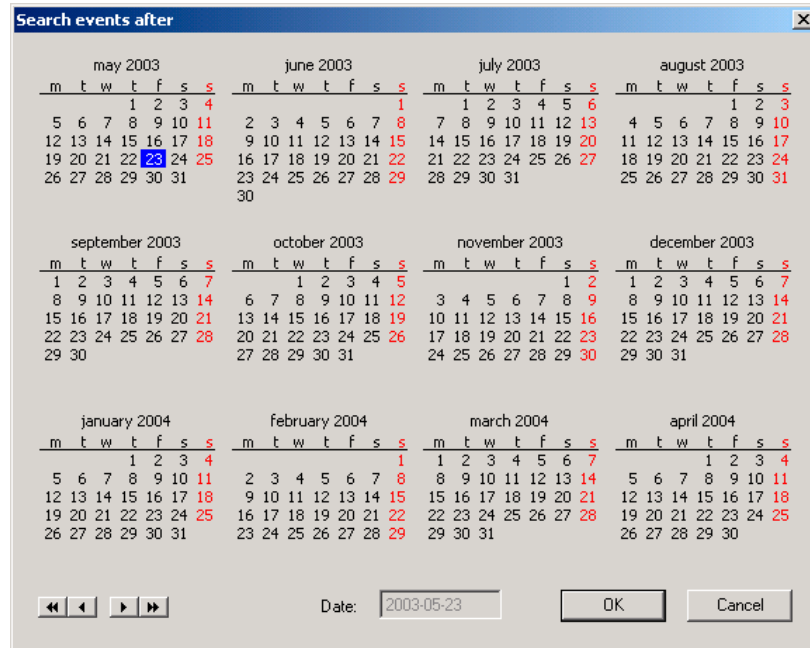
You can reload already stored event filters, to simplify setting up, if you for instance have several common alarm or System Users (which should perform event control).

## The calendar

By using the calendar you can enter a date quickly and easily, with only one mouse click e.g. when you are programming holidays or holiday periods. The calendar can be reached from all windows where you are requested to enter a date.

Proceed as follows:

- 1 Click the Calendar button. This is what the calendar might look like if you clicked on the button in the Holidays window:



- 2 Choose the desired start date (applies to holiday periods) by clicking it. The date is displayed in the **Starting date** field.
- 3 Choose the desired end date by clicking it. The date is displayed in the **Ending date** field.
- 4 Click **OK**. The dates are displayed in the window from which you activated the calendar.

By clicking the double arrows you can browse one year backwards and forwards respectively. Click the single arrows to browse the calendar one month backwards and forwards respectively.



## Encryption functions in Local Area Network

Bewator Entro uses integral encryption software when communicating in network environments. This higher security level is necessary - especially when Entro is installed in Internet applications.

The user of Bewator Entro should regularly change the crypto key needed by the encryption algorithm. The crypto key will always be stored in the database. The algorithm uses 128-bit level.

**Note!** The crypto key must be written down and kept in a safe place!

**If the crypto key is not correct the communication is not established – and the system must be completely reset and re-programmed.**

### Encryption gives higher security

Because of the fact that network use needs an encryption algorithm the security aspects of a system are improved. At the same time this raises some important points:

- Always write down the crypto key as soon as it is changed from the standard!
- There are no back-doors into the system. I.e. there is no work-around if the crypto key is lost.
- The only way to re-create a system - is to reset it and re-programme the entire information.

**Note!** A good idea is to use the default crypto key (used at delivery) until the system is completely set-up – and then change it.

### Change the crypto key

- 1 Start the *Entro* program.
- 2 Click on System and select **Change crypto key**. A wizard is invoked to guide you further.
- 3 Select in which way the crypto key should be created:
  - The System creates the crypto key **automatically**.
  - You enter the crypto key **manually** – at least 32 characters. Valid characters are 0-9, A-F (hexadecimal, upper case).
  - Use a **default** (which also is used in the SR34i at power-up – if no database is loaded).
- 4 Click Next.
- 5 If you have chosen to enter the crypto key manually – a field appears where you enter the 32 characters.
- 6 The entered/generated crypto key is shown. **Do not forget to write it down and keep it in safe place!**
- 7 Click Next – and the new crypto key is sent to all SR34i.

**Note!** All SR34i must be on-line to make the encryption work.

- 8 Click OK.

## Special computer setting in Entro

Some settings can be done to optimise or change the way the PC treats the Entro information. This can be set for each individual System user. You can find these settings in the *Entro* menu **System/System Users** (in the properties for the System User).

### Auto log-off

If the Auto log-off function is enabled, Bewator Entro, Installer and Door and event monitor will automatically be logged off if any of these programs have been idle (not used) for a certain time.

This is how to set the desired settings:

- 1 Click the **Advanced** tab.
- 2 In the top box, select whether or not automatic log-off should be applied and for how long the programs have to be idle before they are logged off (pull the indicator to the desired number of minutes).
- 3 Click OK.

### Automatic deletion of events

In Bewator Entro, information about events in the system, e.g. entries, are stored daily. To free disk space, event files can be deleted automatically after a certain time or when a certain file size is obtained.

Proceed as follows:

- 1 Click the **Advanced** tab.
- 2 Select when events should be deleted:
  - **By time.** Select the check box and set the desired number of days. Event files where the latest event is this old will automatically be deleted.
  - **By size.** Select the check box and set the desired file size in Megabytes. The entire event file is deleted when this file size is reached.
- 3 Select if event files should be moved to the waste paper basket when they are deleted or if they should disappear at once.
- 4 Click OK.



## Supplementary information

This section describes a couple of additional settings that you can make in the system.

### Priority group

Using this function you can determine which people should be able to open a door in case of a communications breakdown in the system. Note that this only applies for doors controlled by the DC22/DC12 door controllers.

This is how to decide which people should have this authorisation:

- 1 Choose **System settings** on the **System** menu.
- 2 Click the check box to the left of the person to be included in the group. A tick is shown in the box and the name is copied to the Priority persons square.

**Note!** To withdraw the authorisation, double click the name in the **Priority persons** square or click the tick.

- 3 Click **OK**.

### Duress code on/off

With the Duress function activated, a person entering the building is able to enter a specific code if forced to open the door under threat. Doing so, an alarm signal is sent to a connected alarm transmitter. When Bewator Entro is delivered the duress function is deactivated.

This is how to activate the function:

- 1 Choose **System settings** on the **System** menu.
- 2 Click the **Enable duress** button. A warning message is displayed.
- 3 Click **Yes** to activate the duress function.

### Anti-pass back violation

If a person violates anti-pass back, i.e. does not use his card to leave a zone and then tries to enter the same zone or another zone, the card will be blacklisted. This function is used to specify for how long the card should be blacklisted.

- 1 Start the *Entro* program and choose the **Zone** tab and **Settings**.
- 2 Click the **Anti-pass back** tab.
- 3 Choose the desired alternative

## Using Bewator Entro

In this chapter, Bewator Entro's functions are described from the viewpoint of a person entering the building. How do you get in? How do you set an intruder alarm? The following sections give answers to these questions and a few others.

### Entrance

People entering the building can open a door in several different ways, depending on the security level:

- By using their card through the door terminals card reader.
- By entering a group code
- By using their card and entering his PIN code

If the card/code is accepted, the green LED is lit and the lock is opened.

If the person entering the door enters the wrong PIN code three times in succession, the card will be blacklisted and must be re-validated at the PC. To indicate that a card is blacklisted for this reason, two asterisks (\*\*) are displayed in front of the person's name on the **Persons** tab in Bewator Entro. Double click the person's name to withdraw the cancellation.

### Switching on and off alarm systems

To be able to activate and deactivate an intruder alarm system, the person must be a member of an access group with authorisation to activate and deactivate alarms. Note that certain access groups can have authorisation to activate an alarm only, while other access groups may only be allowed to deactivate alarms.

#### Activating an alarm system – with card

- 1 Press **B** on the door terminal.
- 2 Use the card through the reader and enter your PIN code (depends on the current security level). The alarm is activated.

The door is given the security level chosen in the *Installer* program (often **Card+PIN** security level), irrespective of the security level applying when the alarm was activated. This security level applies until the alarm is deactivated.

#### Deactivating an alarm system – with card

- 1 Read the card at the door terminal's card reader.
- 2 Then enter your PIN code (decided by the current security level). When the alarm is deactivated the door is given the security level according to the defined time zones.

### **Abort an automatic alarm activation cycle**

If the system is set up so that alarm activation is done automatically by a time schedule – people remaining in the facility are still able to abort an *on-going* alarm activating cycle. A warning signal sounds during this time. However - once the warning time ends there are no possibility to “buy time”. Instead the alarm is activated immediately.

Proceed as follows:

- 1 When you hear the warning signal (the alarm will soon be turned on) – find the nearest door (in the same zone).
- 2 Use your card – or push the exit button (if allowed).
- 3 Entro will go back to the normal state – until the next automatic activation is started.

You can remain in the facility until you hear the warning signal again – and repeat the steps above.

### **Entering the duress code**

This is what the person entering the building should do if forced to open the door under threat.

- 1 Use the card.
- 2 Enter the ordinary PIN code; only add 1 to the last digit in the code.

**Example 1:** If the PIN code is 1234, press 1235 instead.

**Example 2:** If the PIN code is 1239, press 1230 instead.

When a duress code is entered, the door is opened at the same time as the common alarm output in IOR6 can be activated (duress has to be defined as an alarm event for this to happen).

**Note!** Duress works only during the Card + PIN security level.

### **Setting/changing the PIN code**

This is how a user sets/changes their PIN code. (If “Personal Setting” has been activated.)

- 1 Press the **A** button on the door terminal. The yellow LED is lit.
- 2 Use the access card through the card reader. The yellow LED is lit.
- 3 Enter the old code. If you have no previous code, enter 0000. The yellow LED blinks twice.
- 4 Enter a new code (four digits). The yellow LED blinks twice.

**Note!** The code 0000 cannot be used.

- 5 Enter the new code once again.

## Caretaker functions

Some doors can be set up to allow for a temporary change of security level. The door can be set *Unlocked* for certain times - or set to *Group code* (4 digits). The command is invoked at - and applies only to – a selected door.

The prerequisite is that the person doing this must belong to an access group with the **Caretaker** tick box selected.

### Unlocked

Proceed as follows:

- 1 Press **A20** and the yellow LED flashes three times. If you press **A19** instead, only a Caretaker is able to reset the door.
- 2 Use the **card** (+ PIN). The yellow LED is lit.
- 3 Enter the **time** when the door is to be locked again. E g 1600 for 4 PM.
- 4 The reader sets the door unlocked until the requested time (or a time zone change)

### Group code

Proceed as follows:

- 1 Press **A21** and the yellow LED flashes three times.
- 2 Use the **card** (+ PIN). The yellow LED is lit.
- 3 Enter the **time** when the door is to be locked again. E g 1600 for 4 PM.
- 4 Enter the group code with four digits (not 0000). The yellow LED flashes once and the group code will work until the requested time (or a time zone change). Remote opening from PC will still work.

### Reset door to normal

To put the door into normal mode again before the requested time - proceed as follows:

#### When unlocked

- 1 Use the **same card (+ PIN)** in the same reader **or** use the *Toggle reset* from PC in the Door monitor program.
- 2 The door is **locked** and set to normal mode.

#### When group code

- 1 Press A21 and use the **same card (+ PIN)** in the same reader
- 2 Press 0000.
- 3 Press 0000 once again
- 4 The door is **locked** and set to normal mode.

## Searching registered persons

Using this function you can search for all the persons granted access in the system.

- 1 Choose **Person** on the **Search** menu. The **Search persons** window is displayed.

In the **Search persons** window you can use a number of different search criteria in order to search for a person. For example, you can use the name, part of the name, the card number, the optional field or one of the access groups. You can also combine the search concepts and use "wildcards" and "jokers" ("\*" and "?"). See the examples on the next page.

- 2 Enter the desired search criteria.
- 3 Choose whether the search should be case sensitive. If the check box is selected and the search criterion is "smith" the system will not find "Smith".
- 4 If the **Match all criteria** check box is selected, all entered search criteria must be matched for the person to be found. This alternative is best when the search consists of a combination of search criteria. If the check box is empty, only one of the criteria needs to be matched.
- 5 Click **Search**. The name you searched for is displayed on a new, temporary tab called **Search result**.
- 6 You may now, using the **Search result** tab, change the database information for this person. Just select the name and click **Edit**. To remove the person from the database, click **Delete**.

If you are not satisfied with the search result, click the **Change criteria** button. The **Search persons** window is redisplayed. The original search criteria are saved for you to make the necessary changes.

When you are finished you can remove the **Search result** tab by clicking the **Remove tab** button.

### Search, example



To find all persons belonging to a certain access group, simply select the desired access group. In addition it is also possible to select one or more doors in the lower frame.

To find all persons by the name of Smith, enter the last name and an asterisk (\*), i.e. Smith\*. The asterisk (or wildcard) implies that any character and any number of characters may be found after the asterisk, the system will find them whatsoever. If you have registered the persons with the christian name first, enter the asterisk first, i.e. \*Smith.



To find all card numbers beginning with 1234, enter 1234 and an asterisk, i.e. 1234\*.

Apart from asterisks, question marks (jokers) can be used in the search criteria, e.g. if you are not sure how the person spells his or her name. The question mark represents one character, any character.

### Search with right-click on person – or door.

You can mark one person in the list, right-click and select to show **authorised doors**.

In the same way you can mark one door and all **authorised persons** will be shown.

## ***Import and export information about persons***

It is easy to import information about persons to Bewator Entro, from e.g. Excel. You may also export files to other applications from Bewator Entro.

### ***Import information***

You can import all information about cards (persons). In the table on the next page you can see the format.

**Note!** If any person uses *extra cards*, you cannot import this information from a file. Instead you must enter this via the standard menus.

- 1 In the *Entro* program, choose **Import persons** on the **File menu**.
- 2 Find the file to import.
- 3 Click **Open**.

### ***Export information***

You can also export all information about cards (persons) into a file. Note that the PIN-code is encrypted and cannot be understood. However - it can still be imported from the same file.

- 1 In the *Entro* program, choose **Export persons** on the **File menu**. The Export persons to file window is displayed.
- 2 Find a folder where the file can be stored.
- 3 Type a name for the file in the **File name** field.
- 4 Click **Save**.

**Note!** The name of a group must be identical. Both spelling and lower/upper case must be correct. If not – a complete new group will be imported without any authorities at all.

### Create an import file in Excel

- 1 Create one empty spreadsheet. E g Remove any Sheet 2, Sheet 3 etc.
- 2 Be sure that actual cells are in **Text format** before you enter any information and store it in a file.
- 3 The file should be of the format below for each person (row).

Column	Field	Comments
A	<b>Name</b> (e g Surname)	Text
B	<b>Name</b> (e g first name)	Note! Field A and B together maximum 32 characters.
C	<b>Free field</b>	Text ( <b>maximum 40 characters</b> ). E g E-mail address.
D	<b>Card number</b>	Text value ( <b>00000000-99999999</b> ) If Bewator standard card parameters are used, padding zeroes will be imported to get eight digits.
E	<b>PIN code</b>	Text value ( <b>0001-9999</b> )
F	<b>Valid</b>	Text Alt 1 <b>YY-MM-DD</b> Alt 2 <b>YY-MM-DD - YY-MM-DD</b>
G	<b>Group 1</b>	Text ( <b>16 characters</b> ) – or empty
H	<b>Group 2</b>	Text ( <b>16 characters</b> ) – or empty
I	<b>Group 3</b>	Text ( <b>16 characters</b> ) – or empty
J	<b>Group 4</b>	Text ( <b>16 characters</b> ) – or empty
K	<b>Group 5</b>	Text ( <b>16 characters</b> ) – or empty
L	<b>Group 6</b>	Text ( <b>16 characters</b> ) – or empty
M	<b>Priority person</b>	Not imported – Leave empty
N	<b>Counter</b>	Text value ( <b>00-99</b> )
O	<b>Member group no</b>	Text value ( <b>0-999999</b> )
P	<b>Card inactive</b>	Text <b>Yes/No</b>

- 4 Choose **Save as** on the File menu.
- 5 In the **File format** list box, select the desired delimiter, e.g. semicolon.
- 6 Type a name for the file in the **File name** field and click **OK**.

**Note 1!** The name for a group must be identical regarding spelling and case. Otherwise a new group **without** any permission at all will be imported. For other software than Excel be sure that a delimiter character (e g semi-colon) is included for every access group not used.

**Note 2!** Numerical fields in Excel cannot accept leading zeroes. Instead change the cell format to *text* in these cases – before entering the digits. That would be the case for card number 00340100.

## Backup of event files

In cases where you want to archive events files (stored on the PC hard disk) on some other backup media, this can be copied separately. Remember to coordinate these operations with the automatic deletion of event files.

Proceed as follows:

- 1 Start *Windows Explorer*.
- 2 Find the program folder where the actual system user has specified to store the events.
- 3 Select which users **event files** to archive.

Dependant of the PC environment itself, there maybe many methods of doing this automatically. Consult the IT-manager.

## Backup of the database

Normally it is sufficient to let the database (with all the settings, persons etc) be stored in every SR34i (and in the PC) to ensure the safety and integrity of the system. The more segment controllers there are – the more backup copies there are.

However – it is possible to save a PC-file copy of the entire information on a backup media. Proceed as follows:

- 1 Start *Windows Explorer*.
- 2 Find the folder where Bewator Entro is installed.  
Normally *C:/Program/Bewator/Bewator Entro*.
- 3 Go to the database folder. The first system is stored in **System 1**.
- 4 Copy the file **entro.db** to a suitable backup disk.

There are also methods of doing this automatically, dependant of the PC environment. Consult the IT-manager.

## View system resources

You can see how many doors, cards, time schedules there are that are used in the system. Proceed as follows:

- 1 Start the *Entro* program and click on menu **View**.
- 2 Select **View system resources**.
- 3 A graphic bar diagram displays the capacity of the system.
- 4 Click **OK**.



## Door and event monitor

The *Access registration* section on page 59 described how to choose which doors will be monitored on your PC. Below you will find instructions on how to use the **Door and event monitor** programme.

- 1 Start the *Door and event monitor*. Note that you can also start the program from Entro/File menu.
- 2 Choose **Event log** on the **File** menu (if the Events window is not already displayed).

Each event defined as **Normal** or **Alarm** is displayed (see the *Access registration* section on page 59). Alarm events are displayed in red. The events will appear on the screen as they occur.

Even though the **Door and event monitor** is not running, alarm events can be displayed as pop-ups on the PC's screen. This requires however that Entroser is running and that the SR32I Common alarm output is activated in the segment controller connected to the PC.

## Multiple windows with different monitoring focus

By opening multiple event windows you can monitor different doors, persons, events etc in different windows.

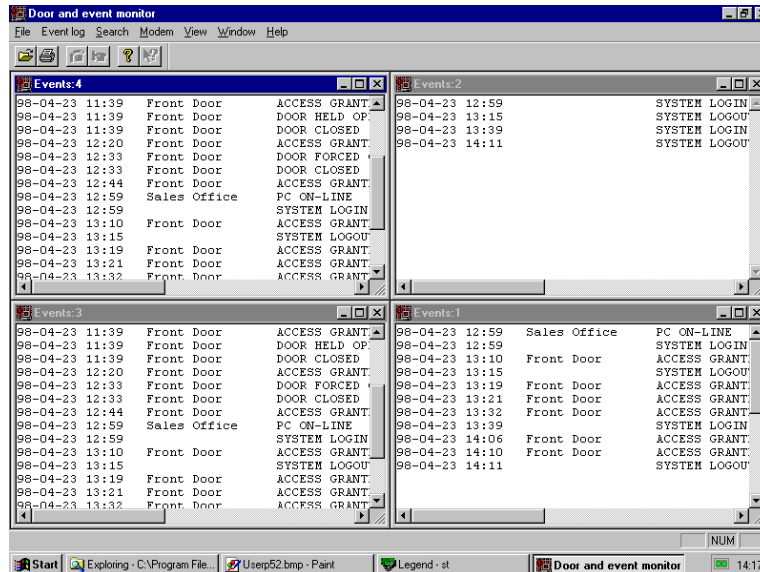
Proceed as follows:

- 1 Choose **New Event log** on the **Event log** menu. A new event window named **Events:2** is displayed. The first event window is renamed **Events:1**.
- 2 Choose **Tile windows** on the **Window** menu. The windows are arranged side by side. Both windows display the same events.
- 3 Click the right mouse button on the **Events:2** window. A menu is displayed.
- 4 Choose **Change filter**. The **Change filter** window is displayed.

Now you can choose whatever you want to monitor in this window. For example, you can monitor a specific person and/or a specific door. You can also customise the event filter, e.g. to limit monitoring to certain types of events.

- 5 To customise the event filter, click **Custom filter**.
- 6 Click **Set filter**. The **Event filter** window is displayed.
- 7 Select which event types to monitor in the **Events:2** window, and then click **OK**. The **Change filter** window is redisplayed.
- 8 Click **OK**. Now you have two event windows monitoring different movements.
- 9 To add **more** event windows, choose **New Event log** on the **Event log** menu and then **Tile windows** on the **Window** menu.

This is what the screen might look like when you are using four event windows:



To simplify monitoring, the event windows can be named.

Right-click the desired window and choose **Name view**. The **Set name of view** window is displayed. Name the view and click OK. Filtered and named views will reappear even if the program is shut off and restarted.

## Search events

To search for old events in the archive, proceed as follows:

- 1 Choose **Search events in archive** on the **Search** menu. The **Event search** window is displayed.
- 2 As in when you are choosing what to display in a monitoring window, you may search for events relating to specific persons and doors. Using the custom filter you can choose what event types to search for.
- 3 Choose the desired settings.
- 4 To limit the search to specific dates and times, select the **Events after** and **Events before** check boxes and state the desired date and time intervals.
- 5 Click **Search**. Events corresponding to your search concept are displayed.
- 6 You now have the option to export this information by using the command **Save events** in the **System** menu and select file format.

This can be used for searching for example reservation events and for further administration in external software such as Excel or similar.

## Door operation from PC

The **Door and event monitor** also includes graphical door status display. This is where you can operate the door directly from the PC, e.g. open the door. To make this possible you have to enable this function for each door to be operated from the PC. The option is found on the **Doors/Advanced** tab.

- 1 Choose **Door status** on the **File** menu.

The following symbols exist:



The door is locked.



The door is unlocked.



Alarm event on locked door. Example: The card reader has been vandalised.



Alarm event on unlocked door. Example: The door held warning time has expired.



Unknown status. Displayed when the system is off-line, e.g. when you are working with a modem connected system (see the *Working with multiple systems* chapter).



Alarm activated. Shows that Entro understands that an intruder alarm is turned on and that the door is blocked.



Alarm event on a door where the alarm is turned on. E.g. if the door is forced.

- 2 Right-click a door symbol to display a menu where several options for door operation are available, e.g. Remote open, Toggle open etc. You can also display the door's event log and open a window displaying the door's current status.

**Note!** To be able to operate a door from the PC you have to be logged on and be a level 1 or 2 system user, i.e. with all rights or all rights except system settings. There is however a special level of system user that permits remote control of doors.

You can log on by starting Bewator Entro and log on, or choose **Login** on the **File** menu in the **Door and event monitor**.

## Open/close all doors

In case of fire or in other circumstances when all doors need to be opened at once, choose **All Doors Open** on the **Door** menu. To close the doors, choose **All Doors Reset**.

**Note 1!** This command will not fully work over TCP/IP communication. In this case only the doors that are on the same local area network connected to the SR34i and the PC communicates with, will open.

**Note 2!** To be able to open/close all doors from a PC, you have to be logged on and be a Level-1 System user, i.e. with all rights.

You can log on by starting Bewator Entro and log on, or choose **Login** on the **File** menu in the **Door and event monitor**.

## Roll call

If you have created roll call or anti-pass back zones, the **Roll call** view shows the whereabouts of different persons in the premises.

- 1 Choose **Roll call** on the **File** menu. The **Roll call** view is displayed with names of persons and the zones they are currently visiting.
- 2 The view can be filtered further if needed. Right-click and choose **Change filter**.
- 3 To monitor several zones or persons at the same time, right-click and choose **New roll call view**. A new window is displayed. Arrange the windows on the screen by choosing **Tile windows** on the **Window** menu. Then filter each view as desired.

## Reset blacklisted card

Persons who have violated anti-pass back, i.e. not used their card to leave a zone they have previously entered, and persons that have entered three incorrect PIN codes in succession, get their cards blacklisted. This is displayed in the **Roll call** view and in Entro's **Person's** tab with two asterisks (\*\*) in front of the name. To reset the card, double-click the name. Note that you have to be logged on in Entro or the Door and event monitor to be able to do this.

## Printouts

Bewator Entro provides you with two types of printouts:

- **Programmed information.** At any time you can print the information you have programmed about time schedules, doors, access groups and persons. Print the information by choosing **Print** on the **File** menu. This type of information can only be printed to printers directly connected to your PC.
- **Events.** This type of information can be printed to a printer connected to the PC or automatically to a printer directly connected to a segment controller.

### Programmed information

- 1 Choose **Print** on the **File** menu.
- 2 Choose what information to print. In the above example the **Persons** option is pre-set. Bewator Entro automatically suggests the option corresponding to the tab being active when you chose **Print**.

The **Selected persons**, **Selected doors** etc. options mean that only information about the person, door etc. selected on the tab is printed (make your selections before you choose **Print**). By clicking **Preview** you can view the printout on your PC's screen.

### Events

Events can be printed from the **Door and event monitor**.

Proceed as follows:

- 1 Open an event log by choosing **Event log** on the **File** menu (if it is not already displayed).
- 2 Right-click somewhere in the event window. A menu is displayed.
- 3 Choose **Change filter**.
- 4 Select the types of events to be displayed.
- 5 Click **OK**.
- 6 Choose **Print** on the **File** menu.

## Working with multiple systems

This chapter describes how to provide a modem-connected system with information about time schedules, persons, access groups, doors etc.

### Logging in

As you log in you can choose which system to work with.

- 1 Start *Bewator Entro*. The log on window is displayed.
- 2 Enter user name, password and connection.
- 3 In the **System** list box, choose the system you want to programme.
- 4 Click **OK**.

The system's site name is displayed in the title bar of the window. Otherwise the window is empty. The red indicator next to the OFF-LINE text tells you that you have no contact with the modem-connected system.

### Dialling the modem connected system

This is how to establish modem connection with the system you logged in to:

- 1 Click the lifted handset symbol or choose **Dial** on the **Modem** menu. A message is displayed while the system tries to establish a connection.
- 2 When the connection is established, the ON LINE indicator is lit green to indicate that you have direct contact with the dialled-up system the following message is displayed.
- 3 Wait until the DB UP TO DATE indicator turns green. This may take a couple of minutes since information has to be transferred.

When the DB UP TO DATE indicator is lit green, your PC contains the same information as the dialled-up system.

### Programming information

Now programme the information the same way as described earlier in this manual.

**Note!** Bewator Entro should always be ONLINE (dialled-up) when you programme a modem-connected system. This makes information transfer quicker and safer.

When you have finished programming, wait until the green indicator and the DB UP TO DATE text is displayed bottom right in the **Entro** window. Then click the replaced handset symbol or choose **Hang up** on the **Modem** menu.

### **Starting Door monitor without interrupting the modem connection**

The following symbol is displayed bottom right on the PC's screen:



Click the right mouse button on the two indicators to display a menu where **Door monitor** is one of the alternatives. In the same way, you can switch from **Door monitor** back to **Entro**. The modem connection will not be interrupted.

### **Logging in to another system**

On the **File** menu you will find an alternative named **Login to another system**. Choosing this alternative you do not have to exit **Entro** to programme another system. Instead, the login window is displayed for you to log in to the desired system. If the modem connection is open when you choose **Login to another system** the current connection will automatically be closed.

## Bewator Entro Reservation

Bewator Entro includes reservation functions (e.g. in sports arenas, tennis courts, conference rooms etc) and works together with the integrated access control system.

The System Administrator sets which objects (like card readers/doors) are to be included and chooses the relevant reservation time schedules.

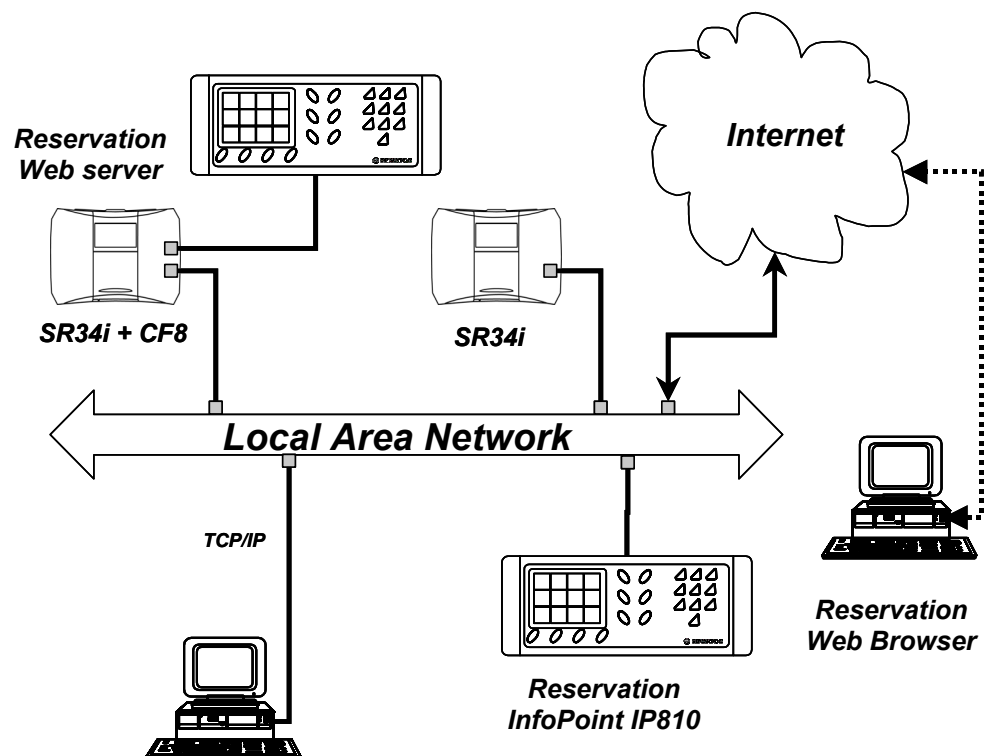
The users wanting to reserve times can use an ordinary web-browser (like Explorer or Netscape) and login to the SR34i containing the reservation system. Alternatively use his/her card in a card reader together with a touch-screen – depending on how the system is configured.

**Note!** The Reservation requires that all controllers be of model SR34i (or later).

### Integrated Web server

The SR34i has an integrated (embedded) web server function, which is used for reservation applications. It requires that the dedicated SR34i have a static IP-address and a permanent connection to the Internet (when Internet is used).

**Note!** One of the SR34i must be equipped with a **Memory card for web reservation**, which will contain the reservation information.





## Set the Reservation options (System User)

In the *Installer* program a reservation object is created which can be a tennis court, conference room – or similar.

You then choose which card readers (from a table of all installed) to be included in the object/zone.

There are also possibilities for machine control and door control in reservation applications.

After that you, in *Entro*, create one or more reservation time schedules, which states possible times and days to reserve e.g. a tennis court. The time schedules are then named to simplify their use.

The reservations objects are then configured further to fit different needs. E.g. how many reservations to book forward – or how many tennis courts there are etc.

In the main Bewator Entro program you decide which objects different access groups can reserve.

Finally, you decide which **access groups** and **member groups** every **person** belongs to.

Technically the entire reservation information is stored in an integrated web page (in a SR34i) with its own IP-address on a network.

The address to this website is **<IP-address>/login.html** which should be notified to the users of the Reservation system.

## Reservation operation (User)

When all settings are done, reservation can be done in two ways:

- Login from a **web browser** in a computer – where the card number and the PIN code is used as a password and identification.
- Login at an InfoPoint IP810 where the card number is used for identification.

You then choose the relevant object and enter the times to reserve.

## Confirmation of reservation

In the software there are functions to generate an e-mail message to confirm the reservation to the user. This requires that the Users' e-mail address is known and entered into the person's properties (free field).

## Using the reservation object (User)

When you have booked your reservation you just use your card in the normal way.

Depending of the configuration of the system, different levels of access and possibilities are available. E.g. you can pass through a door some minutes after the reserved time (to pick up forgotten items or similar).

## Important concepts - Reservation

To be able to programme the system you have to be familiar with the following concepts:

- Reservation Time schedules
- Reservation objects
- Security levels
- Access Groups
- Persons and Member groups

### Time schedules

Here you programme different schedules for different objects.

The intention is that different access groups can reserve one or more objects during one or more times – depending on the configuration.

E g two tennis courts have four separate sessions with exactly the same times during Monday to Friday – but first and last sessions are not available on Saturday and Sunday.

#### Example

**Tennis court 1:** Time schedule: Training session

09:00 - 12:00	12:00 - 15:00	15:00 - 18:00	18:00 - 21:00
Mo - Fr	Mo - Su	Mo - Su	Mo - Fr

**Tennis court 2:** Time schedule: Training session

09:00 - 12:00	12:00 - 15:00	15:00 - 18:00	18:00 - 21:00
Mo - Fr	Mo - Su	Mo - Su	Mo - Fr

### Flexible reservation in same interval

The Reservation system also allows for reserving the whole or part of a longer time interval. E g if you have created an interval for a conference room between 8 AM and 6 PM, the User can reserve the whole interval – or only 8 AM to 10 AM alternatively 8 AM to 2 PM. This is called “flexible interval reservation” in the Bewator Entro.

## **Reservation objects (single)**

Reservation objects can consist of facilities with doors, e.g. sports arenas, conference rooms - but also other items such as coffee machines. I.e. something that can be electrically controlled and have a locking function. These can then be reserved by different kinds of users (sportsmen, employees etc).

In a reservation object you can also include doors that must be passed before you reach the reserved object. Note that these doors cannot be used for normal access.

## **Reservation objects (grouped)**

This concept is used when a random allocation of objects is required. You can also group several reservation objects together with similar possibilities.

An example of this might be a laundry room with a couple of washing machines, where each is an object, which will be controlled by a relay in an IOR6 (machine control). These individual objects are then grouped together and can be treated as one common, grouped object. The users are then allocated one of these individual machines when a reservation is done and subsequent use of it.

## **Machine and door control**

In a reservation object, up to 10 **IOR6 relays** can be included as well as a traditional card reader at a door –.

For example, a relay can control a machine in such a way that when a person uses his card, not only the door will be unlocked; but also the machine is enabled to be started and used during the reserved time – but no longer.

At the same time other relays in the IOR6 may be used to control other reserved doors (like a drying room), which can be open for access (with defined opening time) and locks again.

In fact even more relays can be controlled with a time schedule (e.g. light is on for a certain time).

## **Security levels**

The security level determines what action is needed to open a door. Because the reservation function has to know which person is using the objects, only the following alternatives are possible:

- **Card only.** A personal card is to be used in the reader to be able to open the door. If the card is lost or stolen it is easy to cancel the card.
- **Card + PIN.** The door is opened when the access card is used and a personal code belonging to this particular card has been entered.

In other card readers in the Entro-system other levels can be used – see the Users Manual.

## **Access Groups**

In a large company with several different departments, you may have to divide the staff into different access groups. This way you can decide which doors the different groups should have access to – and during which hours they should have access to these doors. For example, you can programme that the reception staff should not have access to the research department during lunch; at the same time as both the reception staff and the research staff should have access to common doors during all time zones. Each person may belong to up to six access groups.

In this part you also choose which **Reservation object** a certain access group can book.

Persons who always have access to a reservation object – e.g. caretakers – can belong to an access group with this functionality.

## **Persons and Member groups**

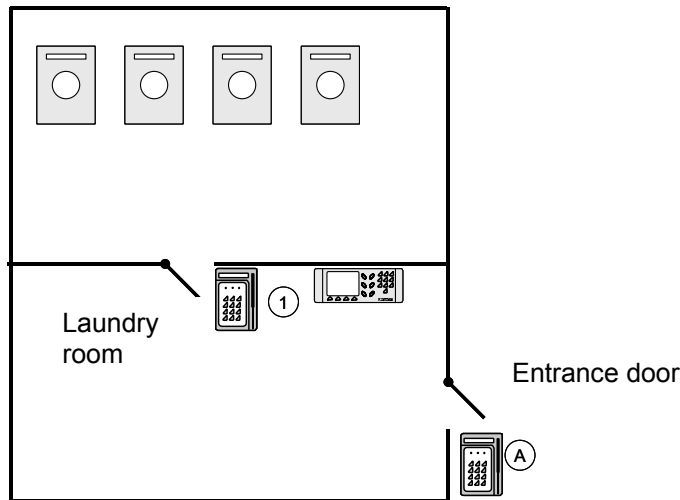
In addition to every person having his/her own personal card and belonging to at least one access group, you can also decide on a member group for each person. Every member group will be considered as equivalent and have the same access for reserving/changing the same object.

E.g. in sports club different teams can form a member group who could book, change or cancel times for each other.

## Example 1 of Reservation

To illustrate how a reservation object can be set up, we show an example of washing machines on a laundry room with one door, where reservation applies only to the Laundry room door (#1). Outside this door a Bewator InfoPoint IP810 booking terminal is mounted for reservation.

Note that door A does not have to be reserved. This door will be under normal access control from the Entro system.



In the example there is a site with a Laundry room door (card reader #1).

All washing machines can be freely used, but the access to the machines themselves will be seen as one object. A maximum of two reservations (two member groups) for two machines can be reserved on this door. The aim is that only two machines should be used - but nothing prevents someone using both.

**Table 1- Example of parameters for a laundry room**

Parameter	Value	Comments
<b>Reservations per Member group:</b>	10	Total amount of reservation allowed for each member group. Max 60.
<b>Number of concurrent reservations:</b>	2	Two member groups can reserve at the same time. Max 99.
<b>Max number: *)</b>	2	Two reservations. Max 6.
<b>Calendar period: *)</b>	Week	Day, week or month.
<b>Forward reservation time:</b>	32	Reservation allowed only one month forward at a time. Max 365 days.
<b>Overlap time:</b>	10 min	Extra time to collect forgotten things. Max 99 minutes.
<b>Automatic cancel time:</b>	15 min	Somebody can book after certain time Max 60 minutes
<b>Minimum remaining time to book:</b>	2 h, 30 m	Minimum left to allow for a new reservation. Max 23 hours, 45 min.

\*) Optionally parameters.

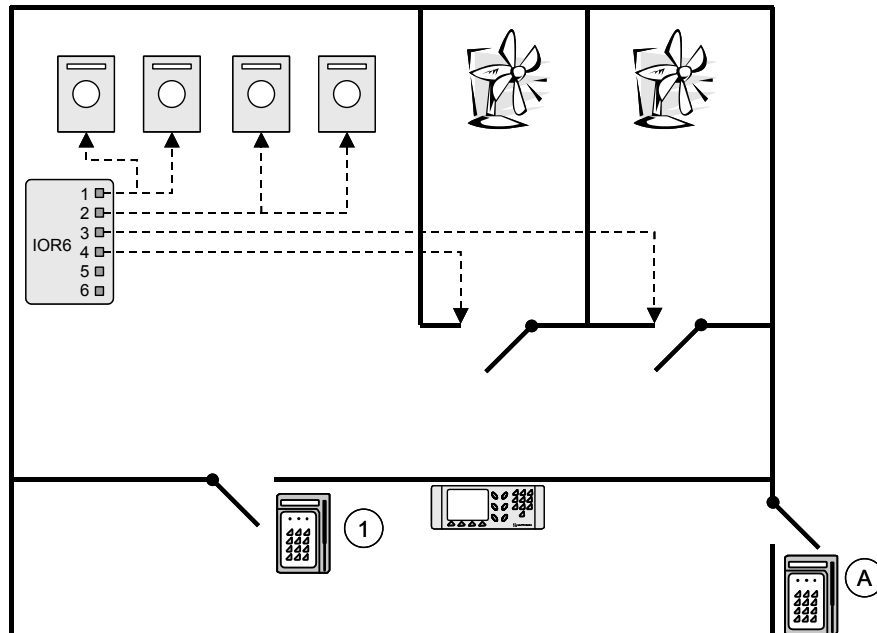
## Example 2 of Reservation

The example below illustrates some other features included in the reservation system. Once again we refer to a laundry room. But the washing machines are grouped in pairs, and are controlled by relays in an IOR6. They are randomly allotted to users so that only one pair of machines will be activated. This might be done to distribute the wear and tear of the washing machines.

In this case you create **two separate objects** each with a dedicated relay (defined as machine control in the IOR6) – but using the same main reader. Then you group these together as a superior object, which then is allotted to the users.

Outside the door there is a Bewator InfoPoint IP810 booking terminal allowing for making new reservations local to the laundry room. I.e reservation will be possible either via a web browser (PC) - or at this terminal.

Note that door A does not have to be reserved. This door will be under normal access control from the Entro system.



## Programming - Reservation

In the *Installer* program you create zones (forming reservation objects) where a specific card reader is used for reservation (known as “Main reader”). In addition you include the readers “on the way” to the object.

In the following section we describe how the System User programme settings and conditions for different reservation objects (time schedules, access authorities etc) are set up.

### Time schedules

The first thing to do is to identify the times for reserving. In a tennis court there may be three-hour sessions, which can be booked all the week around – or some other object only available on weekdays.

In the system there can be 32 time schedules with each 24 intervals for reservation.

- 1 Start the *Entro* program and click the **Time schedules** tab.
- 2 Click **New**.

For new time schedules a wizard is invoked which will help you programme the required functions. For existing time schedules the tabs are shown (displaying the same information).

The wizard also directly allows for programming of Half days, Holidays and Holiday periods. See *Enter public holidays and holiday periods in Reservation* section.

- 3 In the **Name** field, enter the name of the time schedule e.g. Training sessions.
- 4 Click **New** to create a new **Interval**. A row with suggested fields with From, To and Weekdays is displayed.
- 5 Click on the arrow at **From** and choose time. Press TAB.
- 6 Click on the arrow at **To** and choose time. Press TAB.
- 7 Select the **Days** when the interval should be valid.
- 8 Repeat step 4-7 for every new interval.

You can click on **Sort** to get the intervals sorted.

- 9 Click **OK** to save the time schedules.

Set up information for the next time schedule in the same way.

## Reservation object

Next step is to programme the Reservation object itself.

- 1 Start the *Entro* program and click the tab **Zones**.
- 2 Mark the zone and click **Edit**.
- 3 Select the **Time schedules** from the list. Click on the arrow to list available time schedules.  
  
You can also click on the clock icon to *Create*, *Edit* or *Copy* a reservation time schedule. Then choose the desired time schedule by clicking the name.
- 4 Mark if flexible reservation within an interval should be possible. Read more in the *Flexible reservation in same interval* section.
- 5 Click the tab **Max nr limits**.
- 6 Decide the **Maximum reservations per member group** for a certain advance period. E g to book four training sessions in a month in the same object. Max value is 60.
- 7 Enter how many **Maximum no of concurrent reservations** on the same object will be allowed. E g if a tennis park has two separate courts but only one door, two different member groups must still be able to book the same time. Max value is 99.
- 8 Choose if even more restrictions should apply. Enter in the field **Max nr** and **Calendar period** the number of reservations (maximum 6) a member group can make in a certain period (day, week or month).
- 9 Click the **Time related restrictions** tab.
- 10 Enter in the field **Max forward reservation time** for how long a period booking is available. E g 31 days. Max value is 365 days.
- 11 Decide on how many minutes the system waits until an automatic cancel is done. Enter in the field **Automatic cancel time**. This gives a delay before some other Member group can book the same time. Max value is 60 minutes.
- 12 Enter the allowed **Overlap time** for accessing the object after the reserved time. This makes it possible to enter a booked tennis court some minutes later (due to a traffic jam or similar). Max value is 99 minutes.
- 13 Enter how long, in hours and minutes must **remain of an interval** to allow for a new reservation. Maximum value is 23 hours, 45 minutes.
- 14 Click **OK**.

Repeat necessary steps for each reservation object.



## Enter public holidays and holiday periods in Reservation

Certain day's reservations might not be available. E.g. if tennis court is used for a tournament – or if a golf court has closed for the season.

**Note!** See also paragraph *Service mode* for another type of exception.

In the ordinary Entro system there are *Public Holidays and Holiday periods*, which allow exceptions from an ordinary week. These can also be used in the reservation system to inhibit reservation at these times.

In most cases they will not coincide and must be specified for each separate time schedule – in the Reservation.

To make the system understand that holidays and holiday periods should not be treated as ordinary working days, this information must be programmed.

Proceed as follows:

- 1 Start the *Entro* program. Then click **Time Schedules** tab.
- 2 Select the time schedule; click **Edit** and then the **Public Holidays** tab.
- 3 Mark the tick in the **Use Global Public holidays** – if you prefer to use the same dates as specified in the main Bewator Entro program.
- 4 Click **New**. The **Public holidays** window is displayed.
- 5 In the **Date** field, enter the date of the first holiday, or click the **Calendar** button and choose the date. You can have up to 14 days in each time schedule.
- 6 Click **OK**. The **Public holidays** tab is redisplayed with the date filled in.
- 7 Click **New** and programme the next holiday accordingly. .
- 8 Create the **Holidays** in the same way – but enter both **Start** and **End** date. You can have up to 4 periods in each time schedule.
- 9 Repeat steps 4-8 for every separate time schedule in the reservation system.

## Decide on reservation authorities for access groups

- 1 Start the *Entro* program.
- 2 Click on the tab **Access groups**
- 3 Create or select an access group and go to the tab **Reservation objects**.  
If you also select the tick box **Caretaker** this group will be able to access (and use) this object 24 hours a day – without any reservation. (Normally you create a separate access group with this functionality).
- 4 Select one or more of the available **objects** to be accessible for this group.
- 5 Click **OK**.

## Give persons reservation authorities

In a reservation system it is important that every person has a Member group no even if it is the same for all persons. Otherwise the person cannot reserve any times.

**Note!** We only describe additional information regarding Reservation.

Every person must belong to one or more access groups simultaneously. These may already been given reservation rights.

If not - you first create a new access group and proceed as follows:

- 1 Start the *Entro* program
- 2 The **Person** tab is displayed.
- 3 Mark a person and click on **Edit**.
- 4 If you enter a persons' e-mail address in the **Free field**, Bewator Entro can confirm a reservation by sending an e-mail message (if the software is set up for this). See paragraph *Prerequisites for reservation confirmation*.
- 5 Check that the field **Member group no** is correct. All persons belonging to the same member group number will automatically have the same rights in the reservation system. These may be e.g training groups, families etc
- 6 Check or choose correct **access group**.

**Note!** Check that the **access group** allocated to a person has the correct reservation object associated (see access groups).

- 7 Click **OK**.
- 8 Repeat necessary steps for every person.

**Hint!** You can simplify the programming of cards/persons even for the reservation by using the duplicate function described on page 57

## Flexible reservation in same interval

In many cases, such as conference rooms, you do not want to be restricted to reserving one or more short intervals – you would rather have a more flexible way to reserve times.

The software allows for defining a longer interval (e.g 8 AM to 6 PM) where the user then can reserve a flexible time within this interval. I.e you first restrict the total outer limits (start and stop) but the user can reserve the whole or part of it.

Proceed as follows:

- 1 Start *Entro* and click the tab **Zones**
- 2 Mark the actual reservation object and click on **Edit**.
- 3 Create or Edit the time schedule to be used. Normally this results in fewer - but longer intervals.
- 4 Mark the tick box **Accept flexible reservation periods on this object**.
- 5 Click **OK**.

## Special Set-up – Reservation

### Show reservation information to the user

When reserving times the software can display different levels of information to the user. E.g. names of other member groups and users can be displayed in plain language. This could be useful if you want to shift each other's bookings etc. You set up these functions as follows:

- 1 Start *Entro* and click the tab **Zones**.
- 2 Click on **Settings** and then click the **Web Settings** tab.
- 3 Select appropriate alternatives – Show Name of Person, Show Member Group Numbers and Show all reservations.
- 4 Click **OK**.

### Service mode

If some kind of maintenance or service is scheduled, it is possible for personnel to set this up in the software. Proceed as follows:

- 1 Start *Entro* and click the tab **Zones**.
- 2 Mark the object and click **Edit**.
- 3 Click on **Set Service mode** and select date (by picking in the calendar) and time for start and stop in the list boxes – or mark the tick-box **Until further notice**.
- 4 Click **OK** and you will see the chosen time. To edit the time just click the same icon again.

If you want to delete the chosen time just click Clear service mode.

- 5 Click **OK**.

## Using confirmations in Reservation

Bewator Entro can automatically generate an e-mail message to the person making a reservation (or a cancellation). The texts in these messages are stored in two files in the CF8 (compact flash) memory card and may be edited but this is normally not necessary.

The messages also include the IP-address to the web server (SR34i) that sent the message. This gives an easy way to log in again (for editing reservations).

**Note!** The name of the SR34i, sending a confirmation, allows only characters accepted in e-mail addresses. Special, national characters cannot normally be handled by the e-mail server (ISP).

### Prerequisites for confirmations

The Reservation system uses Internet connections that allow for making reservations on any PC. The prerequisite for this is that the SR34i controller has an available Internet connection with fixed IP-address.

In addition to this you can set up some parameters, which allow for sending a confirmation by e-mail to the person doing the reservation.

**Note!** The following parameters are defined in consultation with the IT-manager.

Proceed as follows:

- 1 Start the *Installer* and click the **Controllers** tab.
- 2 Mark the controllers, which contains the CF8 and will send the e-mail message – and click on **Edit**.
- 3 Click the TCP/IP Settings tab and check/enter the IP-address to the **Domain Name Server (DNS)**. This is in fact a server converting the domain name (e.g. *bewator.com*) into a valid IP-address. The DNS often resides with the contracted Internet Service Provider (ISP) – or in the local area network.
- 4 Click the **E-mail settings** tab.
- 5 Enter the **SMTP Server** which is the e-mail server handling the *outgoing* mails. This often resides with the contracted Internet Service Provider (ISP). The name may look like *smtpserver.swip.net* - or similar.
- 6 Enter the **Domain Name** that SR34i uses to create a valid sender address. May be e.g. *bewator.com* and is often used by the ISP to further validate the sender.
- 7 Click **OK**.
- 8 Finally check that each person has a **valid e-mail address** entered in the free field of the person's properties (in *Entro*).

If you have named the SR34i "Reservation" and enter "bewator.com" as domain name – the message is sent from the sender address *reservation@bewator.com* to the e-mail address entered in the free field on each person's properties.

## Editing text in the confirmations

The actual texts sent are stored in files CF8 memory card and are named:

- **reservation.txt** (Message sent when reserving)
- **cancelreservation.txt** (Message sent when cancelling)

To change these you make use of a suitable PC-adapter for retrieving and storing the contents of the CF8 memory card. As follows:

- 1 Place the CF8 in the adapter. (Be careful when connecting the card to avoid destroying the data). Use the Windows Explorer or similar to find the files.
- 2 In the folder "LANG" there are a number of language folders (0, 1, 2 etc.). Locate the file to change.
- 3 Edit the file and write the text you want to display to the User. You then include some optional field tags that (at run-time) will get information from the system (like object, date, time etc.)

If you include e.g. the tag %pfnm the first name of the person will be displayed. See example in next section.

- 4 Store the edited files and place the CF8 in the SR34i Controller.

## Example of confirmation

E.g. write the following text in the file *reservation.txt* and store the file in the CF8.

**%sbn**<Reservation confirmation>

Hello **%pfnm**,

This is an automatic e-mail message that confirms your reservation of

**%robn, %rhur:%rmin – %ehur:%emin on %rdat/%rmon.**

To change any reservation, log on to **%ipme/login.html**

If the person's first name is Thomas and they have reserved the Tennis court 1 on the 14<sup>th</sup> of July at 2 – 4 PM, the e-mail message will look like this:

**Subject: Reservation confirmation.**

Hello **Thomas**,

This is an automatic e-mail message that confirms your reservation of

Tennis court 1 **14:00 – 16:00** on **14/06.**

To change any reservation, log on to **http:xxx.xxx.xxx.xxx/login.html.**

In a similar way the file *cancelreservation.txt* can be changed. The table in the next section gives more types of information you can include.

### Table of e-mail fields in reservation confirmations

The table below shows different types of fields, which can be included in e-mail messages. It is the text in the left column that may be included.

Field	Function
%pfnm	Persons first name
%plnm	Persons last name
%pfrf	Persons free field 1 (normally email-address)
%pmno	Persons family/member group
%dnam	Door name
%rwkd	Weekday of reservation - Start
%ryer	Year of reservation - Start
%rmon	Month of reservation - Start
%rdat	Date of reservation - Start
%rhur	Hour of reservation - Start
%rmin	Minute of reservation - Start
%robn	Reservation object name
%ewkd	Weekday of reservation - End
%eyer	Year of reservation - End
%emon	Month of reservation -End
%edat	Date of reservation - End
%ehur	Hour of reservation - End
%emin	Minute of reservation - End
%ipme	IP-address to web server (me) <b>Note!</b> This parameter does not work in DHCP environments. Please write the web address in plain text.

### Special e-mail fields

The following fields can also be included if other people need a copy of the e-mailed confirmation.

%sbj<x>	Mail subject, x= Subject text
%bcc<y>	BCC recipient, y= e-mail address for secret copy
%rcc<z>	CC recipient, z= e-mail address for copy

## View and make reservations as Administrator

The System Administrator of Bewator Entro has the possibility to see all reservations made. Even new reservations for persons can be done. The ordinary PC used for administration is also used in this case.

Remember that it is possible to make reservations in all objects which means the objects that a user normally does not have access to. E.g. if an object is out of order another similar object may be reserved instead.

### View reservations in general

Proceed as follows:

- 1 Start *Entro* and select **Manage Reservations** in the **System** menu.
- 2 A list is displayed with every reserved object and corresponding member group.
- 3 You will be able to make new reservations by clicking the **Make reservations** icon. Doing this – there is also a choice for sending an e-mail confirmation message.

In a similar way you can cancel reservations by clicking **Cancel reservations**

- 4 Exit the window.

### Make reservations for person

It is possible to make reservations in the person list directly. Proceed as follows:

- 1 Start *Entro* and mark a person in the list.
- 2 Right-click and select **Make reservations**.
- 3 Select in the list box **Reservation object**.
- 4 Select **date** (by picking in calendar).
- 5 Choose one of the times written in black text. Any green text is earlier reservations made for the member group. Any red times displayed are reservations made by another member group.
- 6 Click on **Make reservations**.
- 7 Exit window.

### Cancel reservations for person

If want to cancel any reservation – follow as above and mark a green text but instead click on **Cancel Reservation** icon.

## **Reserve and use objects**

### **Prerequisite**

To be able to reserve times in the Bewator Entro Reservation system you need a standard web browser in a PC - or a card reader together with a touch screen. The method depends on the type of installation.

When you have made your reservation you may receive a **confirmation by e-mail**. You should already have been notified if this method is in operation. If in doubt consult your System Administrator.

### **Reserve with a web browser (User)**

You need access to a standard PC with a browser (like Microsoft Explorer or Netscape). In addition you need an IP-address (Internet) tied to a website (running in one of the Entro segment controllers).

- 1 Start your browser and enter the IP-address to the website.
- 2 You will see a **login page** for the reservation.
- 3 Enter your **card number** and your **personal code** (PIN). The first time you will also have the choice of a suitable language.
- 4 Select object and reserve times.
- 5 Confirm your choices. (You can of course edit your choices).
- 6 Log out.
- 7 You can now wait for the reserved time and use your card in the reader at the reserved objects (e g the tennis court).

### **Reserve at booking terminal (User)**

In this case usually a Bewator InfoPoint IP810 is mounted local to the object. Together with this there is a card reader used for identification.

- 1 You will see the **Home page** for the Reservation system
- 2 Use your card at the **card reader**. The first time you will also have the choice of a suitable language.
- 3 Select (by using arrows) the objects and times you want to reserve.
- 4 Confirm your choices. (You can of course edit your choices).
- 5 Log out.

You can now wait for the reserved time and use your card in the reader at the reserved objects (e g the tennis court).

### **Reserve at touch screen (User)**

Function is similar to the InfoPoint IP810 but you select objects and times by touching the screen.



# Integrating with external applications (BAPSI)

## General

Normally access control system software is quite proprietary to its system components and is seldom open for customised applications. This is quite natural because it is also a security system to be used for controlling e.g access to doors in different kind of facilities.

Bewator Entro can use a well-defined programming interface to communicate with other, external software packages (like Time & Attendance, Alarm control or similar). E.g to import/export cards, get time stamps or events.

An ordinary **TCP/IP** link is used for transferring the data between the different software components.

The external software must be modified/completed according to the specification we call *Bewator All Purpose Socket Interface* (BAPSI). Remember, this not a program just guidelines to the programming interface.

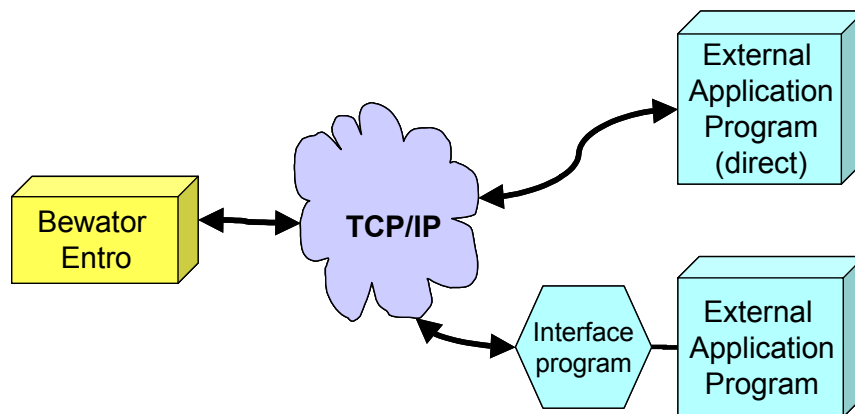
With BAPSI this is done in a specified and safe (encrypted) way that still keeps the access control system on a secure and integral level.

The specification can be requested from Bewator.

## What is BAPSI used for?

Normally the User interface in access control software allows for functions like card registering, time schedule programming and standard event logging (and searching).

Using BAPSI, custom application software can take advantage of sending/receiving messages to/from the access control system – and easily add new functions to the overall system. This could be Time& Attendance, Reservation systems etc.



## Field applications

At the moment there are already systems running in the reservation applications area – using the BAPSI software interface. In this case the supplier of the external reservation software made a modification to their software module, which writes data into a file – and Bewator developed a special module that reads this file and forwards this information to the access control system.

Please contact Bewator for more information













