TIDOMAT smartONE
version 2

- User manual -

TIDOMAT

Copyright information

www.tidomat.se
info@tidomat.se
doc.no. 01080010-0844

Content

Introduction

The **security system smartONE** controls up to sixteen Access Points. The settings for the Access Points and the system are configured in the user interface, which is implemented in two different layers, the **System-layer** and the **Admin-layer**.

The Access Points can be unlocked by using the Card Reader, the Exit button or via the Web or the Telephone. The Card Reader will grant access according to a Door code or an access Card/tag which is used with or without a PIN being requested. The logic which controls the Card Reader is situated at another location. It is thus impossible to unlock the Access Points by altering the Card Reader. The Access Point can be controlled to be locked or unlocked for specified hours by using Time Channels and Schedules. The user interface is dynamic and adapts to every individual User's rights, as well as responding to dynamic system designations, languages and help files.

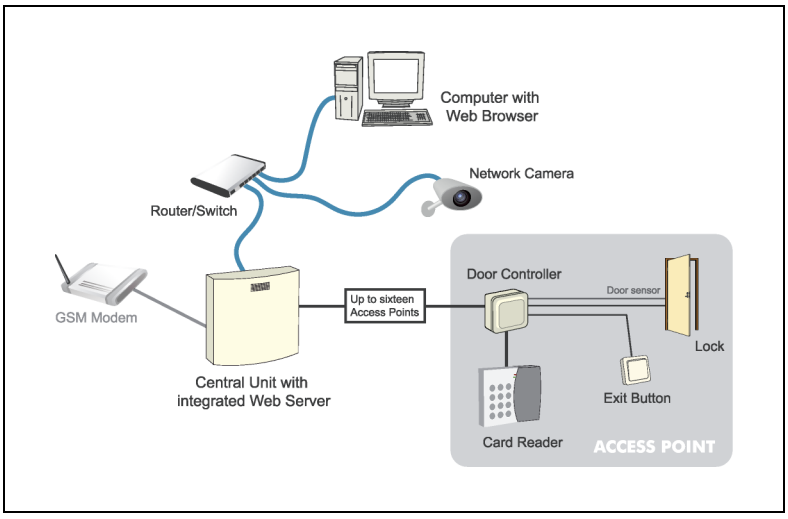
The System-layer is used for the configuration of the system and the connections between the Access Points and the hardware. The Admin-layer is used for the everyday maintenance of the system.

Once the hardware has been configured, smartONE is ready to be adapted to your personal preferences. In order to maintain the system, there is one pre-requisite:

- The Access Points must be configured in the user interface.

Instructions on how to configure the hardware of smartONE are found in the ***Startguide for smartONE***. For instructions on how to set the functions for the Access Points, please read ***Access Points, Appendix I*** of this user manual.

Overview of smartONE



The System and the Admin-layer

The user interface of smartONE is implemented in two different layers. The **System-layer** initiates the settings. This is where the Access Points are configured. The **Admin-layer** is used for the everyday maintenance of the system, such as granting Access Cards and Access Plans, creating Time Channels, Schedules and compiling Log and Reports over the events of the system. You can use the **System-** and **Admin-layer** simultaneously. In order to do so, you login to the **System-layer** from the **Admin-layer**.

The list below gives an overview of the different functions of the **System-** and **Admin-layer**, as it is structured in the user interface:

The System-layer:	**The Admin-layer:**
• Time Channel • Trigger • Access Points • Network Camera • Users • System • Tools • Log/Report.	• Cardholders • Schedule • Time Channel • Trigger • My Access Points • Users • System • Tools • Log/Report.
In the top of the user interface, it is indicated whether you are operating as a System-user, an Admin-user or System+Admin user.	

The following functions can be controlled from both the **System-** and **Admin-layer**:

- Time Channel
- Trigger.

The following functions can be controlled from both the **System-** and **Admin-layer**, but the functions vary in the different layers:

- Access Points
- Users
- System
- Tools
- Log/Report.

The following functions can be controlled from the **System- layer** only:

- Configuration of the Access Points
- Network Camera.

The following functions can be controlled from the **Admin- layer** only:

- Cardholders
- My Access Points.

Several Users can access and maintain the system simultaneously. They can operate the **System-** and the **Admin-layer**, or have limited rights to use certain functions. The user interface is dynamic and adapts to very User's individual rights.

Installation of hardware

The *Start Guide for smartONE* will take you through the installation of the hardware for the system. The different components and all the technical data are described. When smartONE is installed, make sure that you read about how to configure the Access Points thoroughly. It is of great importance that the hardware is correctly connected to the Access Points. Information about the control the Access Points is included in *Access Points, Appendix I.*

Facts about smartONE

The security system smartONE has a user friendly user interface, which integrates a host of functions. The program creates lists which provide you with a comprehensive overview of the choices and functions you choose to activate. There are nevertheless a number of things worth bearing in mind when using smartONE:

- Several options in the system contribute to the dynamic user interface, which adapts to your individual choices. An example is the use of **Time Channels** and **Triggers**. If you have created **Schedules**, they can be connected to these functions by being selected in the windows for each function. However, if you have not created any **Schedules**, the options to connect them to the functions are not offered.

- The user interface is adapted to every User's right.

- This manual is written in accordance to the default values of smartONE. Should you decide to change the **object Cardholder** to a designation of your choice, for example **Flat owner**, this manual will still refer to **Cardholder**. The help files will register your choices and display the designation of your choice.

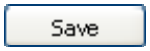
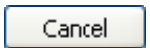
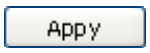
- When the different headers are followed by a plus sign (+), there is more information in that window. Should you wish to view the information, please click on the plus sign. When all information is displayed, the header is followed by a minus sign (-).

- ***Do not forget your password***. You can change your password when you are logged in to the system but you cannot get a new one. Should you forget your password, the system must be restored and all data will be lost. If you have made backups, all data on the system settings and the database is conveniently restored and your system will be re-established.

- You should therefore **save a back up of the database and settings** regularly.

- The system is delivered with two default passwords: for the **System-layer**, the default password is ***smart***, and for the **Admin-layer**, the default password is ***admin***. If you restore a backup copy of the settings and the data, those default passwords are applicable.

List of symbols and buttons

	Edit, Test Schedule
	Delete/Cancel filter
	Access Plan (displays an overview in a separate window)
	Delete, block
	Activate filter
	List new Cards/tags, View calendar
	Update
	Activate
	Attention required
✔	The function is active
	Saves the settings
	Return to previous settings
	Undo changes and return to overview
	Apply settings and changes
	Add new
	Go to the starting page of the system
	View the help files
	Logout from the system

Getting started with smartONE

1. Open **smartONE** via your Web browser.
2. Bookmark the page and save it in your favourites.

Login to the System-layer

On the initiating page, you will be prompted to state you **User name** and **Password**.

1. Type **User:** ***System*** and login with the **Password:** ***smart***. This is the default password of the system.
2. Select the connection, **Normal** or **Secured (SSL)**[1].

The window which appears is the overview of smartONE in the **System-layer**. You can navigate in the system by using the links in the menu to the left. Every link will display an overview for the functions of each header. Should you wish to return to the starting page, click on the button **Home** in the top right corner. To view the help files of the page which is currently open, click on the button **Help**. The information box at the top of the page displays important information, such as if an Access Point is off-line or if any settings are incorrect. This information enables you to conveniently follow up and correct any errors of the settings.

Changing the Password in the System-layer

The first thing you should do when using smartONE is to change the default Password to a personal one. It is recommended to have a password of at least six characters of which at least two are numbers.

1. Click on **User>Password**.
2. Type the **Password** you used to login.
3. Type your **New Password**.
4. Confirm you **New Password** and click on **Save**.

[1] When the option SSL is selected, your web browser will inform you that this is a not trusted certificat. It is however safe to continue.

Checking the Date and Time (the System- and Admin-layer)

Please check that the settings for Date and Time are correct.

1. Go to **System>Date/time**.
2. Check the **Date** and **Time** to ensure that the settings are accurate. Date and Time can be filled out **manually** or click on **Synchronize with PC-clock**.

The Date and Time is displayed in the right hand corner of the system. The Date and Time can also use Network Time Protocol. Daylight-saving time is automatically adjusted by the system, but can be edited. *For further information, read the section Using Network Time Protocol on page 40 and Changing Daylight-saving time on page 41.*

Configuring the E-mail account

By using an E-mail account, you can receive messages from smartONE and thereby find out if anything unusual occurs by the Access Points. The system can notify you when it starts up and if an Access Point or a Card Reader is off-line. The E-mail account is also used for the function Trigger, which sends information via E-mail to one or several receivers.

1. Go to **System>E-mail**.
2. State the host or IP address for the **SMTP-server** which you are using.
3. Fill out the **User** and **Password** of the E-mail account, if this is required.
4. State **E-mail from**, this being smartONE@ followed by the domain which smartONE is connected to[2].
5. Type the name of the **Receiver**, in this case the **E-mail address** to the person whom the mail should be sent to.
6. Click on **Send an e-mail as a test** to check the setting.
7. Click on **Save**.

[2] You can also use a sender name of your choice before @, such as myfirstname.mysurname@mycompany.com.

Explanations, E-mail

Server, SMTP-server
The address of the server which is being used.

User (if not applicable, please leave the field blank)
The User of the E-mail account.

Password (if not applicable, please leave the field blank)
E-mail from (E-mail address)

E-mail from (E-mail address)
The E-mail is sent from smartONE. After @, please state the address of your domain, such as smartONE@mycompany.com. You can also use a sender name of your choice, such as myfirstname.mysurname@mycompany.com, or if you have given the system a personal designation, your address can be mysecuritysystem@mycompany.com.

Receiver
The e-mail address of the receiver. If you choose to have more than one receiver, the addresses are separated by a semicolon (;).

Test
In order to test the E-mail address you have stated, press the button.

Should the system not be able to reach the SMTP-server, the messages are placed in the outbox. The outbox will save 50 messages from the system for five days. The security system smartONE also sends Text-messages. If you want to use the Text-messages, please read on page 54 how to ***Configuring a GSM modem*** *to the system.*

The Access Points

The Access Points which are configured to smartONE can be controlled in a number of ways. The Access Points can be opened:

- Via the web.
- With the Exit-button.
- With a Door code; a Card/tag; a Card/tag and PIN.
- With a Card/tag and PIN, and by using the function PIN-code timer, the Card Reader memorises the PIN and grants access for a set time when the same that Card/tag is displayed.
- Via the telephone.
- By using Input EXTIN, a function which unlocks the Access Point from an external source.
- Via a Time Channel.

The Access Points can also be controlled to:

- Be locked and unlocked for specific times during the day, according to Time Channels connected to each Access Point.
- Be unlocked for a set time when a Card/tag has been displayed to the Card Reader twice during a span of 20 seconds, the so called Show-card-twice function.
- Keep a Log over the granted accesses, with optional extent of the details.

Connecting the Access Points (the System-layer)

Information on how to connect the hardware to the Access Points to the system is found in the **TIDOMAT smartONE 2 Start guide**. *The different settings for the Access Points are stated into detail in **Access Points, Appendix I.***

The settings for the Access Points can be edited under the heading Access Points in the **System-layer**.

Setting and updating the Door codes

The Door codes can be updated in both the **System-** and **Admin-layer**.
Go to the header **Access Points>List>New/Edit>Door codes**.

1. If you are logged in to the **System-layer**, type the four digits for **Door code 1** and **Door code 2**.
2. Click on **Save**.
3. In the **Admin-layer**, type the four digits for **Door code 1** and **Door code 2**.
4. Click on **Update**.

The Time Channels

The Time Channels enable you to control various functions during set time spans. In order to create a Time Channel:

1. Go to **Time Channel** in the menu.
2. Click on **New**.
3. Give the Time Channel a **Name**.
4. To decide how the Access Point should be controlled for the stated time, click on the dropdown menu **Type**. Select a function.
5. Click on the dropdown menu **Access Point** and select which Access Point the Time Channel should be connected to.
6. Select the Authority Level which is to be applicable in the header **Activate by Authorized Level**, should this function be active. If the function is to be inactive, leave the field blank.
7. State the **Time**[3] manually in the fields by selecting the radio button **Enter from/until time**. If you have created Schedules, tick the radio button **Or use Schedule**, and select the one of your choice in the dropdown menu. Select whether the **Schedule function** should be the **Actual Schedule** or the **Reverse Schedule**. *To read about **Creating a new Schedule**, go to page 33.*
8. Select the **Days of the week**.
9. Click on **Overview Info/Schedule** to see an overview of your selected **Time** or the **Schedule**.
10. Click on **Save**.

When the Time Channels have been created, they are saved in a list. Every Time Channel can be edited when you click on the green button, **Edit**. The Time Channel is deleted when you press on the red button, **Delete**. *Read the **Explanations, Time Channel**, on page 16.*

[3] For a Time Channel which is to be active during the day, please state 08.00-17.00. For a Time Channel which is to be active during the evening and night, please state 17.00-08.00.

Explanations, Time Channel

Name
The name of the Time Channel.

Type
Decide what the Time Channel should do during the specified hours, if the Access Point connected to it should:

Activate relay (AUX)
This option activates the relay.
Unlock door (DOOR)
Sets the Access Point to be unlocked.
Request PIN
Increases the security for access granted with Card/tag by also requesting PIN. Access by other means is granted.
Block Door code 2
Blocks Door code 2, access by other means is granted.
Block Door code 1
Blocks Door code 1, access by other means is granted.
Request PIN + block Door code 2
Blocks Door code 2 and increases the security for access granted with Card/tag by also requesting PIN. Access by other means is granted.
Request PIN + block Door code 1
Blocks Door code 1 and increases the security for access granted with Card/tag by also requesting PIN. Access by other means is granted.
Block Access Point
Blocks the Access Point and all means of access are denied. The Door bell and the manual Relay Functions can still be used.

Access Point
Select the Access Point which is to be connected to the Time Channel.

Activate by Authorized Level
Authorized level is a function which can be connected to a Time Channel. When a person of the Authorized level or above enters the Access Point, the Time Channel is consequently activated. Authorized level global 1-4 is a variety of the above function. However, the person of the Authorized level or above must now enter any Access Point in the system for the Time Channel to be activated.

There are two prerequisites for the Time Channel to respond accordingly:

- A Time Channel which includes Time and Weekdays or a Schedule must be connected to the Access Point.
- A person of the stated Authorized level or above must access this Access Point during the day.

It does not matter what time of the day the Cardholder displays the Card/tag for the function to be activated. The function is re-set at midnight. *If the function is not to be used, leave the field blank.*

Time
The times which are to be applicable for the Time Channel.

Enter from/until time manually, alternatively select **Or use Schedule.**

From hh:mm
From what time of the day...
Until hh:mm
...until the time of the day.

Exempel, Time Channel
For a Time Channel which is to be active during the day, please state 08.00-17.00. For a Time Channel which is to be active during the evening and night, please state 17.00-08.00.

Schedule
Select the Schedule which is to be connected to the Time Channel.

Schedule function
Decide whether this Schedule should be an **Actual Schedule** or a **Reverse Schedule**.

The **Actual Schedule** for a Schedule set to 08.00-17.00 includes the times stated, in this case 08.00-17.00. The **Reverse Schedule** when applied to the same Schedule will be active at 17.00-08.00.

Days of the week

Days
Select the Days during which the Time Channel should be active.

Exampel
Should the function be used in a reception, where the Access Point is to be locked until the receptionist is there, these are the requirements:

1. Create a **Time Channel**.
2. Select the **Access Point** which this Time Channel should be connected to and select **Unlock door (DOOR)**.
3. Select the **Authorized level** and the **Time** or the **Schedule** during which the function should be active.
4. Under the header **Time Channel**, select **Activate by Authorized Level 1- 4**.
5. Under the header **Cardholder**, select the equivalent **Authorized level 1-4** for the receptionist.

When the receptionist enters the Access Point, the Time Channel is activated. When the selected Time or Schedule includes 08.00-17.00, the Access Point is unlocked at 08.00 and locked at 17.00, even if the receptionist entered the Access Point earlier. If the receptionist should display the Card/tag later, the Time Channel is immediately activated, however not before 08.00. If the receptionist should fail to enter the Access Point during a day when this Time Channel is active, the Access Point remains locked. When Authorized Level global 1-4 is in use, the receptionist can any Access Point connected to the system, and the Time Channel will be activated.

The security system smartONE supports up to four different Authorized Levels:

1 Authorized level 1	1 Global level 1
2 Authorized level 2	2 Global level 2
3 Authorized level 3	3 Global level 3
4 Authorized level 4	4 Global level 4

The system creates four extra fields prefixed **Global**, which are based on the four original levels. To define the **Authorized Levels** in the system, please go to **System>System designations.** *Further information on how to **Changing the System designations** is found at page 36.*

*To read about how to **Temporarily locking an unlocked Access Point**, go to page 25.*

Trigger (the System- and Admin-layer)

The Trigger performs actions when specified events occur at selected Access Points. The Trigger informs you by E-mail, Text-message, IP notify or HTTP request. You select the events which are to be included in the Trigger.

Activating Triggers

In order to activate a Trigger, please follow these instructions:

1. Click on **Trigger** in the menu.
2. Select **New** to create a Trigger.
3. Give your Trigger a **Name**.
4. Select the **Action** in the dropdown menu. This option refers to *how* smartONE should inform the receiver, should the selected event/s occur. Send **E-mail**, **Text-message**, **IP notify**[4] or **HTTP request**[5].
5. If the message is to be sent to a **Contact list**, please select which one in the dropdown menu.
6. State the address of the **Receiver** in the field. If the field is left blank, the message will be sent to the configured E-Mail address and/or mobile number.
7. If you select **Text-message**, **IP notify** or **HTTP request**, a field called **Message** will appear. Write the message you want the receiver to get in this field.
8. Select the events which are to be included in the Trigger, **Events related to Cardholder Yes/No**, **Events related to Access Points Yes/No** and **Divergences Yes/No**.
9. State the times the Trigger should include. If you state the times manually, select the radio button **Enter from/until time**. State **From** which hour and **Until** which hour.
10. If you have created Schedules and wish to apply them, the option **Or use Schedule** will appear. The Schedules are displayed in the dropdown menu. Select the Schedule you wish to connect to the Trigger.
11. Select the **Days** you want the Trigger to be active. Click on **Overview Info/Schedule** to get an overview of the Times or Schedule.
12. Select the **Access Points** you wish to the Trigger to cover by ticking the boxes.
13. Click on **Save**.

When the Triggers have been created, they are saved in a list. Edit each Trigger according to the instructions above by clicking on the green button, **Edit**. Delete a Trigger by clicking on the red button, **Delete**.

[4] IP notify is sent by URL-style, for example tcp://exampel.com:80 or udp://192.168.0.10:1234.

[5] HTTP request is sent by the method POST.

Explanations, Triggers

E-mail
The information is sent to the E-mail address stated after the field in Receiver, or to the E-mail address of each person in the Contact list. Should this field be empty, the message is sent to the E-mail address configured in the system. *For further information on how to **Configuring the E-mail account**, go to page 12.*

Text-message
The information is sent as a Text-message to the mobile number stated after the Receiver and/or the mobile number of each person in the Contact list. Should this field be empty, the message is sent to the mobile number configured in the system. If the field for Message is left empty, a message is automatically created, including information about the event such as date and time; what sort of event which has occurred; the Cardholder; the Access Point.

IP notify
The IP notify is used to integrate with external systems. If this function is applied, the text box for Message must be filled out. You can type a message of your choice and use the predefined Variables. *The list of **Variables for smartONE** is compiled in **Appendix III**.*

HTTP request
The HTTP request is used to integrate with external systems. If this function is applied, the text box for Message must be filled out. You can type a message of your choice and use the predefined Variables. *The list of **Variables for smartONE** is compiled in **Appendix III**.*

Contact list
The Contact list stores your contacts and enables you to reach more than one person at the time. The Contact list is stored in the dropdown menu. *For further information on **Creating Contact lists**, please go to page 36.*

Explanations, Events

Events related to Cardholder
Access granted by using Card/tag and manual relay controls.

Events related to Access Points
Access granted using Card/tag or Unlocked from My Access Points.

Divergences
Incorrect PIN; invalid Card/tag; Access Denied and Access Point forced.

The Admin-layer – maintaining the system

The system is maintained in the **Admin-layer**. This is where you issue access Cards/tags, create Schedules, Time Channels, Triggers and Contact lists. You can also open the Access Points via the user interface, add further Users to administer the system, view the Log and Reports of the events of the system, edit the System designations and upload Language Files and save backups of the database and settings.

Login to the Admin-layer

Open **smartONE** in your Web browser. If you are logged in as a **System-user**, please click on the button **Logout** in the right hand top corner. On the initiating page, you will be prompted to state you User name and Password.

1. Type **User** ***admin*** and login with the **Password** ***admin***. This is the default password of the system.

The window which appears is the overview of smartONE in the **Admin-layer**. You can navigate in the system by using the links in the menu to the left. Every link will display an overview of each header. Should you wish to return to the starting page, click on the button **Home** in the top right corner. To view the **Help Files** of the page which is currently open, click on the button **Help**. In order to close the user interface or change the User, click on **Logout**. The information box in the top of the page displays important information, such as if an Access Point is off-line or if any settings are incorrect. This information enables you to conveniently follow up and correct any errors of the settings.

Changing the Password in the Admin-layer

The first thing you should do when using smartONE is to change the default Password to a personal one. It is recommended to have a password of at least six digits of which at least two are numbers.

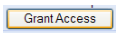
1. Click on **User>Password**.
2. Type the **Password** you used to login.
3. Type your **New Password**.
4. Confirm you **New Password** and click on **Save**.

*To read more about **Access Points**, please go to page 14. Should you wish to read more about **Time Channels**, go to page 15, and for further information about **Triggers**, go to page 20.*

My Access Points – to control Access Points in the user interface (the Admin-layer)

My Access Points provides you with an overview of every Access Point connected to smartONE. The Access Points can be unlocked to grant access and several functions can be altered. The traffic in the Access Points is displayed in real-time. [6]

List of symbols, My Access Points

	Opens the Access Point.		Access Point opened.
	Access Point off-line.		Access Point forced.
	Access Point Blocked.		Access Point Locked.
	Displays Events related to Card user: access granted using Card/tag and PIN as well as PIN code timer.		
	Displays Events related to Access Points: access granted using Door code; Access Point Unlocked/locked by Exit button; Show-card-twice function and Unlocked from My Access Points.		
	Displays Divergences: incorrect PIN; invalid Card/tag and Access Point forced.		
✔	The function is Active.	 Activate the function.	 Inactivate the function.
	Doorbell - by pressing the button ⊛ (star key) on the Card Reader, a signal is sent to the computer. This signal indicates that somebody has pressed the button. A pop up window shows from which Access Point the signal comes. Simply unlock Access Point by pressing the button Grant Access.		
	View images from the Network Camera.		

[6] In order for the events to be displayed in real time, Java™ platform must be installed. For further information, please go to www.java.com.

You can also change the **Authorized Level**, should this function be connected to the Trigger or a Cardholder. Click on the padlock, select the **Current Authorized Level** in the dropdown menu and click on **Edit**. You can also edit and activate different functions for locking and unlocking the Access Points.

Temporarily locking an unlocked Access Point

1. Go to **My Access Points**. The padlock symbol indicates that the Access Point is **unlocked**.
2. Click on the padlock symbol. A pop-up window appears.
3. Click on the green symbol, **Block unlocked** in order to lock the Access Point.
4. A pop-up window prompts you to click on **Ok**.

The temporarily locking of the Access Point remains until it is removed manually.

Remove **Block unlock**:

1. Go to **My Access Points**. The padlock symbol indicates that the Access Point is **locked**.
2. Click on the padlock symbol. A pop-up window appears.
3. Click on the red symbol, **Block unlocked**.
4. A pop-up window prompts you to click on **Ok**.

*To view the **List of symbol and buttons**, please to page 10. To view the **List of symbols, My Access Points**, go to page 24.*

The Cards and the Cardholders (the Admin-layer)

This is where the **Cards/tags** and **Cardholders** are administrated. The Cards/tags are connected to the system and given to the Cardholders whom Access Plans are granted to. The Cardholders can enter an Access Point by using the Card/tag only or, at request, the Card/tag and PIN.

Should the functions **PIN code timer** and/or **Show-card-twice function** be activated at an Access Point, please bear in mind that every Cardholder which is granted access to this Access Point can use the function. *For further information on the function **PIN code timer** and the **Show-card-twice function**, please read **Miscellaneous, Appendix I**.*

> Please note that the designations of the objects[7] can be changed to personal preferences. *Read more about **Changing the System designations** on page 36.* Should the designations for the object Cardholder be changed, it is advisable to do so before the Cards/tags are issued, since you get a more accurate overview.
>
> If you have connected a GSM modem to the system, your Cardholders can use the phone to open the Access Point. The phone number is stated as Card data in the system, and when the Cardholder calls the modem, his/hers number is identified as a valid Card/tag and the Access Point is thus opened. *For further information, go to page 30.*

Creating Cardholders and issuing Cards

Once the Access Points are connected to smartONE, you can specify the functions which should interact between the Access Points and the Cards/tags. *To read about **Connecting a new Card/tag**, please go to page 30.*

[7] The designations of the system refer to the default names which the system calls the Cardholders, such as First name and Surname. Should, for example, the system be used for a block of flats, the name Cardholder could be changed to Flat and First name could be changed to Flat owner and so on. This manual will still refer to First name, but the User interface and the help files will change to your personal settings.

Specifying Departments

By specifying the Departments, you are provided with a comprehensive overview when the Cardholders are saved in a list. If you will not use Departments, please continue with *Creating Cardholders on page 27.* In order to specify Departments, please follow these instructions:

1. Click on **Department** in the menu.
2. Give the Department a **name** in the field.
3. Click on **Apply**. A new, empty field will appear. Continue until you have all the Departments you need.

Edit the Department in the field and click on **Apply**. Should you wish to delete a Department, click on the red button, **Delete**.

Creating Cardholders

In order to add a Cardholder to the system, please follow these instructions:

1. Click on **New**.
2. Type the Cardholder's **First name**.
3. Type the Cardholder's **Surname**.
4. State the **Employee number**.
5. Select the **Department** the Cardholder belongs to. The Departments are stored in the dropdown menu, should they be used.
6. Type the **PIN**, four digits. If the Card/tag should be used without PIN, leave the field blank. However, do note that if the Access Point is programmed to request PIN, the Cardholder will be denied access.
7. If the Card/tag should grant access, please ensure that the option **Blocked No** is selected. Should the Card/tag *not* grant access, the option is to be **Blocked Yes**.
8. State **Number of allowed access**, should this function be activated. The function limits the Card/tag to grant a certain number of accesses, or give unlimited access if the field is left blank. *To read about how to **Display Access Counter**, please go to page 36.*
9. Decide from which date the Card/tag is **Valid from** and **Valid until**. For a Card/tag which should leave unlimited access, please leave the field blank.
10. If an **Authorized Level** should be connected to the Card/tag, please select which one in the dropdown menu. The Authorized Levels are displayed if the function is activated. *For further information on how to activate the Authorized Levels, please go to **Changing the System designations** on page 37, and on the other functions where Authorized Level is used, go to **Time Channels** on page 15 and for general information, read **Miscellaneous , Appendix I**.*
11. Select which **Days** the Card/tag should grant access. You can state this manually by ticking the box for each day, and/or select a **Schedule** in the dropdown menu. The Schedules are displayed if they have been created. *Read about **Creating a new Schedule** on page 33.*
12. Select the **Access Points** which the Card/tag should grant access to.
13. Select the **Functions**[8] which are to be connected to the Card/tag.

*Read the **Explanations, Cardholders** on page 28.*

[8] The Functions can be for example to control a Relay via the Card Reader. The functions are set when the Access Points are configured and are displayed in the dropdown menu. *Read more about how to create functions in **Relay output (AUX), Appendix I**.*

Explanations, Cardholder

Personal data

First name
Fill out the First name of the Cardholder or what you have chosen to call this field according to your personal settings in the System designations.

Surname
Fill out the Surname of the Cardholder or what you have chosen to call this field according to your personal settings in the System designations.

Employee number
Fill out the Employee number of the Cardholder or what you have chosen to call this field according to your personal settings in the System designations. The data in this field should be unique for each Cardholder, in order to avoid duplications if the data is imported via CSV-files.

PIN
State the PIN which should be connected to the Card/tag, four digits.[9]

Department
State which Department, or what you have chosen to call this field according to your personal settings in the System designations, the Cardholder belongs to. When the Departments have been created, they are stored in the dropdown menu.

Blocked
When **Yes** is selected, ***access is denied***. When **No** is selected, ***access is granted***.

Number of allowed accesses
This function is used in for an Access Point to for example a sun bed, or any room where it is convenient for the administrator go use an Access Counter. The Card/tag will allow the set number of accesses only. This function must be activated to be displayed in the user interface. *To find out how*

[9] The Functions can be for example to control a Relay via the Card Reader. The functions are set when the Access Points are configured and displayed in the dropdown menu. *Read more about how to create functions in* ***Relay output (AUX), Appendix I.***

*to activate the function, go to **Changing the System designations** on page 37. Please note that if this function is activated, it is applicable for every Access Point connected to the system.*

Days

Valid from
This is from the date which the Cardholder should be granted access. If the Cardholder should be granted unlimited access leave the field empty. To View the calendar, please click on the orange button.

Valid until
This is until the date which the Cardholder should be granted access. If the Cardholder should be granted unlimited access, leave the field blank. To View the calendar, please click on the orange button.

Authorized Level
This is where you decide which Authorized Level the Cardholder should belong to. The Access Point controlled by an Authorized Level will only be opened when a Cardholder of the selected Authorized Level has entered the Access Point. The Authorized Levels are set in the window for System designations. *For further information, go to **Changing the System designations** on page 37. For further information on how to use the **Authorized Levels**, go to **Time Channels** on page 15 and **Miscellaneous, Appendix I.***

Schedule
When a Schedule has been created, it is stored in the dropdown menu. Select the Schedule you wish to connect to the Cardholder.

Days
Select the Days the Card/tag should grant access.

Access Point
Select the Access Points which the Cardholder is granted access to.

Functions
If any Functions are connected to the Access Point, select the Functions the Cardholder should be allowed to control.

Card/tag
This is where the data for the Card/tag is displayed. If a Cardholder is to open the Access Points via the mobile telephone, please type his/hers mobile number in this field. When the Cardholder calls the GSM-modem, the system recognises the mobile number and unlocks the Access Point during the hours the Cardholder is granted access. *For further information on **Opening Access Points via the telephone**, please go to page 55.*

Connecting a new Card/tag

The Cards/tags can be connected to the system via the Card Reader or via the USB Reader. In order to connect a Card/tag to the system and issue it to a Cardholder, please follow these instructions:

Via the Card Reader:

1. Hold the **Card/tag** in proximity to the Card Reader.
2. When the Card Reader has registered the **Card/tag**, a red light will flash. Return to the user interface.
3. Click on the button **List new Card/tag**.
4. Click on the orange button, **Update card/tag**.
5. Wait for the **data** of the **Card/tag** to be displayed in the field.
6. Select the **Card/tag**.
7. The field to the right behind the header **New Card/tag** displays the Card/tag data. The field to the left of the Card/tag data is for your personal choice of the **Card identification**. You can use letters and/or digits. If you do not wish to use the Card identification, please leave the field blank.
8. Click on **Save**.

Via the USB Reader:

1. By the header **New Card/tag**, place the cursor in the field on the right.
2. Hold the **Card/tag** in proximity to the **USB-reader**. The Card data will appear in the field.
3. Click on **Save** to return to the list or click on **List new Cards/tags** to connect this and further Cards/tags to the system.

Every Cardholder is saved in a **List.** You can **Block**, **Delete**, view **Access Plan** and **Edit** the Cardholder by clicking on each button.

Connecting several Cards/tags to the same Cardholder

Via the Card Reader

When a Cardholder is to have more than one Card/tag, those can be registered all at once.

1. Open the header **Card/tag** by clicking on the plus (+) sign.
2. Click on the orange button, **List new cards**.
3. Hold the new Cards/tags in proximity to the **Card Reader**.
4. When the Card Reader has registered the **Card/tag**, a red light will flash. Return to the user interface.
5. Click on the orange button **List new Card/tag**.
6. Wait for the **data** of the **Card/tag** to be displayed in the field.
7. The field behind the Card/tag is grey and displays the **Card/tag data**. The white field in front of the Card/tag data is for your personal choice of the **Card identification**. You can use letters and/or digits. If you do not wish to use the Card identification, please leave the field blank.
8. Click on **Save** and return to the list or click on **Add card/tag** should further Cards/tags be registered.

Via the USB Reader

1. By the header **New Card/tag**, place the cursor in the field on the right.
2. Hold the **Card/tag** in proximity to the **USB-reader**. The Card data will appear in the field.
3. Click on **Save** to return to the list or click on **List new Cards/tags** to connect further Cards/tags to the system.

Cardholders – List

Every Cardholder is saved in a **List**. You can **Block**, **Delete**, view **Access Plan** and **Edit** the Cardholder by clicking on each button.

Block/delete

In order to **Block** or **Delete** a Cardholder, please tick the boxes. Click on **Apply**.

Access Plan

If you click on Access Plan in the menu, you can view a compilation of the Cardholder's Access Plan. The Schedules, Days and Access Points can be edited in the list.

Searching for data by using the Filter

Data related to the object **Cardholde**r under the headers Cardholder – **List**, **List of Cards/tags**, **Delete/block** and **Access Plan** may be found and compiled with a **Filter**. All objects which match the search are displayed in a list[10].

You can also use the **USB-Reader** to identify Cards/tags.

1. Highlight **Filter.**
2. Hold the Card/tag in proximity to the **USB Reader.**
3. Select the **Card/tag** in the dropdown menu.
4. Click on **Activate filter**.
5. The **Cardholder** connected to the **Card/tag** will be displayed in the list.

Sorting order of the object Cardholder

The list is sorted by clicking on each header for **Card data**, **Card/tag**, **Employee number**, **First name**, **Surname** and **Department**. The list is sorted in ascending and descending order.

[10] Should you carry out a search stating the word John as a First name the filter will include all words with John, such as John and Johnson. A* will search for all objects commencing with a. Numbers may be searched for with limits, such as 1 - 10.

Using Schedules (the Admin-layer)

The Schedules enables you to specify time spans. The Schedules can be connected to the following functions:

- Time Channels
- Cardholders
- Triggers.

The Schedules save time when these functions are utilised. They are stored in dropdown menus and displayed in the dynamic user interface when applicable. The security system smartONE is distributed with a **Calendar**. You can add your own **Special days** to the Calendar, such as public holidays and education days.

Adding Special days to the Calendar

When you are using the Schedules, you can tailor them by adding your **Special days**. *If you do not wish to add any Special days, please and continue to read about Creating a new Schedule, page 33.*

1. Click on **Schedule** in the menu.
2. Click on **Kind of day**.
3. Add the **Special days**, for example Public holiday.
4. Click on **Save**.

Day 1-7 are default values and are thus grey. You cannot change these days. You can add days from day 8, such as public holidays and educational days.

Connecting the days to the Calendar

The **Special days** can be connected to the Calendar. Click on **Calendar** in the menu. Click on each day you wish to call a **Special day**. Should you for example wish to designate **New Year's Day** a **Public holiday,** please follow these instructions:

1. Click on **the1of January**.
2. In the dropdown menu, select **Public holiday**.
3. If the day is to be **Annually**, please tick the box. If not, leave the box empty.
4. Click on **Apply**.
5. The **Calendar** will appear again. Continue accordingly until all your **Special days** have been designated and added to the system.

Creating a new Schedule

In order to create a new **Schedule**, click on **New** in the menu. Fill out the details of **Name**, **Time** and **Days**.

Example, Schedule

Should you wish to create a Schedule which is going to leave an Access Point open for free access during the following hours: office hours during weekdays; until lunch every Friday; every Wednesday evening, please follow these instructions:

1. Click on **Schedule>New**.
2. Give your Schedule a **Name**, for example **Opening hours for Main entrance**.
3. Fill out the **Time** hh. mm. which is applicable, in this case from 08.00-17.00.
4. Select the **Days** which the Schedule includes, in this case Monday, Tuesday, Wednesday and Thursday.
5. Click on **Save**.
6. Add a **New Schedule item** for the day during which the Access Point is to be open until lunch.
7. Fill out the **Time**, in this case 08.00-12.00. Select Friday.
8. Click on **Save**.
9. Add a **New Schedule item** for the evening which is to be active within this Schedule. Fill out the time, in this case 19.00-22.00. Tick the box for Wednesday.
10. Click on **Save**.
11. Add a **New Schedule item** for the other days which are to be active within this Schedule. Since the Main entrance is to be locked during weekends, select Saturday and Sunday and click on **Denied all day**.
12. Click on **Save**.

A Schedule according to the above settings is now saved in the system. In order for the Access Point to be open, the Schedule needs to be activated. In the menu, go to **Time Channel**.

1. Select **New** and give the Time Channel a **Name**. Select **Type>Unlock door (DOOR)**. Select the **Schedule Main entrance** (the name of the Schedule) in the dropdown menu **Or use Schedule**.
2. Fill out the further information which is required and click on **Save**.

The Schedule is now connected to the Access Point.

Delete a Schedule item by pressing the red button, **Delete**. The Schedule is edited in the window when you click on the green button, **Edit**. Click on **Save** when you have edited the Schedule according to your choices. The Schedule will be stored in dropdown menus in the windows of the functions **Time Channel**, **Cardholder** and **Trigger**.

In order to create another **Schedule**, click on **New** and repeat the instructions.

The Schedules you have created are saved in a **List**. You can check the settings of the Schedule by selecting it in the dropdown menu and clicking on the green button, **Test Schedule**. Edit each Schedule by pressing the green button, **Edit**. Delete a Schedule by pressing the red button, **Delete**.

Using the functions in System

This is where you create **Contact lists**, change the **Date** and **Time** and edit the **System designations**. In the **System-layer**, there are also function for editing the **Network settings**, configuring **E-mail** and **GSM modem**. The **System log** displays the administrative events of the system.

Creating Contact lists (the System- and Admin-layer)

The **Contact lists** are used to administrate receivers of **E-mail**, **Text messages** and **IP notify**.

1. Click on **Contact list**.
2. Give the Contact list a **Name**, for example the **Security group**.
3. State the **E-mail addresses** of the group members.
4. State the **Mobile numbers** of the group members.
5. State the **IP notify address** of the group members.
6. Click on **Save**.

Your contacts are saved in a **List.** You can edit the list by clicking the green button, **Edit**. The list is deleted when you press the red button, **Delete**. The Contact list can be activated in the function **Trigger**. *For further information on **Triggers**, please go to page 20.*

Changing the System designations (the System- and Admin-layer)

The default settings for the **System designations** can be edited to your personal preferences. The changes are registered by the system and will be displayed in the user interface. You can change the designation of the system, and call smartONE a name of your choice. The designation of the **object Cardholder** can be given a name you find suitable for your cardholders, as can the designation of the **object Group**. This is also where you decide what the different **Authorized Levels** should be called. The designations of the system tailor the system and adapt it to your personal needs. In order to change the designations, please follow these instructions:

1. In the menu, go to **System>System designations**.
2. To change the **Designation of the system**, please type what you wish to call your system in the text box.
3. To change the **Designations of the object Cardholder**, please state your preference of:

    - the **Object Cardholder**
    - **Cardholder field 1-5**
    - **Cardholder field 6 (unique for each)**.

4. To change the name of your **Group** from the default value **Department**, fill out the field following:

    - the **Designation of the object Group**.

5. To designate the **Authorized levels**, fill out the field following:

    - **Authorised level 1-4.** When the Authorised levels have been set, the system will automatically create a further four settings, prefixed **Global.**

6. Click on **Save**.

In order to see your personal designations, please go to **Cardholder>Cardholder-List**. The system designations are changed. *Read the **Explanations, System designations** on page 38.*

Explanations, System designations

Identification

Designation of the system
This is the **Designation of the system**, which can be changed to a personal preference. The function is much appreciated when more than one system is in use, since it reduces the risk of getting the systems mixed up.

Designation of the object Cardholder

Object designation
This is the designation of the person whom an access Card/tag is issued to. The system has a default value, **Cardholder**. Should you change this designation to for example **Flat owner** or **Employee**, your personal designations will be displayed in the system and in the help files.

Cardholder field 1-6
These designations are liaised to the object **Cardholder**. The fields 1-5 are for your personal choice, and refer to the information which is displayed with the object Cardholder. **First name** and **Surname** are default values, but can be changed to for example **Flat number** or **Project Manager**. The other fields are for information relevant to the object Cardholder, such as e-mail address, telephone number and address. Field 6 has the default value **Employee number**. This value can be edited, but it is recommended that the data is unique for each Cardholder. Should you have to import data for the object Cardholder from the database, the system uses the data in this field to ensure that the data is not duplicated. If the fields are blank, they will not appear in the user interface.

Group

Designation of the object Group
This is the **Designation of the object Group**. It is displayed under the header Cardholder. The default value is Department.

Authorized level

Authorized level, field 1-4

This function is used when the Cardholders should be granted different **Authorized levels**. This is where you decide what the different Authorized levels should be called. Once the Authorized levels have been designated, the system will automatically create four extra fields prefixed **Global**. The fields for Global are displayed under each function where the Authorized level is applicable.

The **Authorised levels** are connected to an **Access Point**. The function calls for a Cardholder of the selected Authorized level or above to be granted access before access is granted for the Cardholders of the lower Authorized levels. It is thus ensured that a person of the selected Authorized level is at the premises of this Access Point before the Cardholders of a lower Authorized level.

The function **Authorized level Global** is a variety of the above function. It is not limited to a specific Access Point, but will grant access to Cardholders of a lower function to the premises once a Cardholder of the selected Authorized level or above enters *any* Access Point connected to the system.

The **Authorized level** can also be connected to the function Time Channel, which is activated when a Cardholder of the selected Authorized level or above enters the Access Point. The Authorized level is restored at midnight or can be inactivated in the user interface **My Access Points**.

Miscellaneous

Display Access Counter

This function is used when a **Cardholder** is to be allowed a limited number of accesses. The Access Counter counts the access down to zero, after which the status of the Cardholder will be blocked. If **Yes** is selected, the header **Number of allowed accesses** is displayed under the header **Cardholder>Cardholder - New/edit**. This is where you state how many accesses the Cardholder should be granted.

System log (the System- and Admin-layer)

Shows the **System log**.

Changing the settings for Date and time (the System- and Admin-layer)

In order to change the settings for **Date** and **time**, *go to page 12 and read about Checking the Date and Time*.

Using Network Time Protocol

The clock can also be synchronized with an Internet server by using **Network Time Protocol**. Should you wish to use Network Time Protocol, go to **System>Date/time**:

1. Tick the radio button **Use Network Time Protocol**.
2. Type the name of the **Server** you wish to use.
3. Select the **Time Zone** either by stating it manually in the text box or select one of the Time Zones displayed when you click the orange button.
4. Click on **Save**.

Changing Daylight-saving time (the System- and Admin-layer)

The system will automatically adjust the clock to **Daylight-saving time**. Should you however, wish to change the date and time for Daylight-saving time, go to **System>Date/time**:

1. Deselect the box **Automatically adjust clock for daylight-saving time**.
2. Select the **Month** and at what **Time** the Daylight-saving time should begin.
3. Select the **Month** and at what **Time** the Daylight-saving time should end.
4. Click on **Save**.

*Please note that the function **Automatically adjust clock for daylight-saving** time is active when the box is ticked.*

E-mail (the System-layer)

To read about how to configure the E-mail address, please to go page 12.

GSM modem (the System-layer)

To read about how to configure a GSM modem, please to go page 54.

The Users of the system

The security system smartONE can be administrated by several users simultaneously. Every **User** has individual rights, and the user interface is adapted to these rights. This is also where the Users change his/her password.

Changing the User password (the System- and the Admin-layer)

*To read about **Changing the password in the System-layer**, please go to page 11. To read about **Changing the password in the Admin-layer**, please go to page 23.*

Adding new Users to the system (the Admin-layer)

In the **Admin-layer**, you can add several Users and give them individual rights. The user interface adapts to every User's rights. In the menu, click on **User**:

1. Click on **New**.
2. State the User's **Name**.
3. Select which **Rights** the User should have in the dropdown menu.
4. If the User should be entitled to see the **PIN** codes of the Cardholders, tick the box following **Show PIN code**.
5. Select the **Access Points** which the User has the right to administer.
6. Type a **New password** for the User.
7. Type the new password again in order to **Confirm new password**.
8. Click on **Save**.

Explanations, Users

Rights

Every User is granted one of the Rights below. The Rights are stored in the dropdown menu.

Administrator

The User works on the same level as the Admin-user with access to all function in the Admin-layer.

Read and write

By this choice, the User can:

- Add and edit Cardholder.
- Edit Department.
- Change his/her Password.
- Edit and open Access Points in the user interface, My Access Points.
- Create Reports.

Read only

By this choice, the User can:

- View information regarding Cardholder, Access Points and Department.
- Change his/her Password.
- Use Reports.
- Open Access Points in the user interface, My Access Points.

The new **User** can login to the system using his/her own user name and password. The user interface adapts to the different Rights the user is given, and can thereby take part of the information which is relevant to him/her. All the Users are saved in a list. You can change the Rights by clicking on the choices in the dropdown menu, followed by Apply. Edit the Users by clicking on the green button, **Edit**, and delete a User by clicking on the red button, **Delete**.

Viewing the Log and compiling Reports

The Log and Reports provides you with a comprehensive overview of the events in the Access Points and the administrative events of the system.

Creating a new Report (the Admin-layer)

1. Go to **Log/report** in the menu.
2. Click on **New report**.
3. Under the header **Report layout**, give the report a **Name**.
4. Under the header **Orientation**, select if the report is to be printed out in **portrait** or **landscape**, A4 paper format.
5. Select the **Column** where you wish your headers to be. You may change the headers in the dropdown menu or simply use the default values.
6. Fill out whether a specific **Cardholder** should be included in the report. You can narrow the report down by specifying **First name**, **Surname** and **Employee number**. Select the Department in the dropdown menu. To include every Cardholder, leave the field blank.
7. By choosing **Yes** or **No** in the dropdown menu, select the **Events** which are to be included in the report.
8. Select the **Access Points** you wish to include in the report.
9. Under the header **Time span**, select the **From date** and **To date** which the report should include. Delete a date by clicking on the red button, and to **View calendar**, click on the orange button.
10. Fill out the **Time**, hours and minutes which the report should include.
11. Click on **Apply**.

Explanations, Events

Events related to Cardholder
Access granted by using Card/tag and manual relay controls.
Events related to Access Points
Access granted using Card/tag or Unlocked from My Access Points.
Divergences
Incorrect PIN; invalid Card/tag; Access Denied and Access Point forced.

Select how many rows the **Report** should include and if you want to **Print out** a hard copy or **Save** a copy in your computer. You can navigate the pages by using the arrows or select a page by clicking on the page number. The **Report** can be sorted according to the headers. **Totally x of pages** refer to the number of A4-pages. Print a hard copy of the Report or Save a CSV-file[11] for documentation.

[11] CSV is an abbreviation for the file format comma-separated value. It is a file format which stores tabular data and is commonly used on all computer platforms.

Using Report templates (the Admin-layer)

The settings for a **Report** can be saved as a template in order to be re-used. Click on **Report templates** in the menu, follow the instructions for **Creating a new Report** and click on **Save**. The Report templates are saved in a list. Click on the green button **Edit** to edit the list and **Apply** to compile a Report. Before the Report is compiled, you can carry out temporary changes. Click on **Apply** again to view a copy of the Report.

View a Report in calendar (the Admin-layer)

You can view a **Report** in the layout of a calendar. Go to **Log/Report>Report in calendar:**

1. Select the **Year** and **Month** which are to be displayed.
2. Select what the **Report** should include; **Events related to Cardholder**, **Events related to Access Points** and **Divergences**. *Read about the **Explanations, Events** in the text box on page 44.*
3. **Exclude times** accordingly to limit the Report, or leave the field blank should both day and night be included.
4. Select the **Access Points** which the Report should include.
5. Click on **Apply**.

The **Report** in calendar shows an overview of the events in the layout of a calendar. Every event is linked to a list of details. Click on each event to view the details. The settings for the Report can be edited in the dropdown menu underneath the calendar. Choose which **Year** and **Month** you wish to include. State **Events related to Cardholder**, **Events related to Access Points** and **Divergences**, **Yes** or **No** and whether you wish to **Exclude times** accordingly. Tick the boxes for the **Access Points** to be included. Click on **Apply** to view the **Report in calendar**.

The Log

The Log stores and displays all the events of the system in chronological order. *To tailor the **Log**, please read about **The settings for the Log** on page 46.* To view the **Log**, click on the header in the menu. The settings can be edited in the dropdown menu. Click on **Apply** to see the changes in the user interface.

List of symboles, the Log

	Displays Events related to Card user: access granted using Card/tag and PIN and PIN code timer.
	Displays Events related to Access Points: access granted using Door code; Access Point Unlocked/locked by Exit button; Show-card-twice function and Unlocked from My Access Points.
	Displays Divergences: incorrect PIN; invalid Card/tag and Access Point forced.

If you select the event in the box, it will disappear from the list in the user interface. It will nevertheless be saved in the database of the system. The **Log** can be edited in the box at the top of the window. Select the **Access Points** you wish to log, and select the **Events related to Cardholder**, **Events related to Access Points** and **Divergences**, **Yes** or **No** in the dropdown menu. When you have made your choices, please click on **Apply**.

Journal (the System- and Admin-layer)

The **Journal** displays all the administrative events of smartONE. Should you wish to save a copy of the Journal for documentation, click on **Save** and follow the instructions.

The Settings for Log (the System- and Admin-layer)

The **Log Settings** specify the Log. Should you wish to do so, go **to Log/Report>Settings** in the menu:

1. Select whether you wish to **Send log by e-mail before erasing**, **Yes** or **No**.
2. State the number of seconds you wish to **Update the log list after**.
3. Select the **Number of events to view on screen**.
4. Select the sort order of the Log should be displayed, in **Ascending** or **Descending** order.
5. Should you wish to **Limit the number of days in the log**, state the number here. If this setting equals 0 the log is unlimited.
6. State how much information for each **Access Point** the Log should include.
7. Select whether it should **Exclude log**, **Log continuously or Exclude log** during specified hours.
8. If the Log should exclude specific **Time**, please fill out the hours and minutes.

Explanations, General settings of the Log

Maximum number of events in log
Displays the number of events which can be saved in the Log. This is a default value which cannot be edited. The values in the brackets stand for: (Number of events saved in the log / the average number of events per day / the latest event). If the log should include more than 9 500 events by midnight, the earliest events are erased (the number of erased logs will be approximately the events of seven days, calculated as the average events per day x 7). Should the log reach the maximum number of events before midnight (00.00), the earliest 100 events registered will be erased.

Send log by e-mail before erasing
This function sends a copy of the Log by E-mail to the configured E-mail address before it is erased. The file can be saved for documentation. Should you wish to receive a copy of the Log, select **Yes**. Do you not wish to receive a copy of the Log, select **No**. *For further information on how to **Configuring the E-mail account** to the system, please go to page 12.*

Number of events to view on screen
The number of old events displayed in the Log.

Sort order – log
How the Log should be displayed, in Ascending order or Descending order. Ascending order shows the latest event at the top and following in chronological order, the earliest event furthest down. Descending order shows the earliest event at the top and following in chronological order, the latest event furthest down.

Erase events until
Any events backdating further than the given date will be erased.

Access Points connected to the system (log granted accesses)

Once you have selected the settings for the log, please state how extensive it should be regarding each Access Point. Select whether it should register accesses at 24-7 or during limited hours.

Select of the below:

Exclude log
No granted accesses will be logged.
Log continuously
Every granted access will be logged.
Exclude log during specified hours
The Log will not record granted accesses during the specified hours. Please state the hours which are to be excluded.

Time hh. mm.
States the hours which are to be excluded from the Log. This option is applicable should **Exclude log during specified hours** be selected.

To delete Logs manually

1. State the dates you wish to **Erase** events until, fill out the date or select a date in the Calendar.
2. Click on **Erase**.
3. The system automatically compiles a CSV file[12] which you can **Save**. Click on **Cancel** to erase the Log without saving a copy.

For example
If it is of less interest to log the granted accesses in a main entrance during office hours weekdays, but of greater interest to log the granted accesses during evenings, nights and weekends, fill out the Log as follows:

Access Point (connected to smartONE) (log granted accesses)

1. **Monday - Friday**, select **Exclude log during specified hours** in the dropdown menu.
2. **Saturday - Sunday** select **Log continuously**.
3. Fill out the **Time** you wish to exclude, in this example since the Log is to be kept evenings and nights for weekdays, 07-00 - 18.00 (refers to office hours Monday - Friday).

This Log will include accesses during evenings and nights (18.00 - 07.00) as well as day and night weekends. Granted accesses during office hours weekdays will be excluded.

Every Access Point which is connected to smartONE is displayed in the user interface. Continue according to the instructions above until the Log is set according to your choices. When it is, click on **Save**.

[12] CSV is an abbreviation for the file format comma-separated value. It is a file format which stores tabular data and is commonly used on all computer platforms.

Using the functions in Tools (the System- and Admin-layer)

By using the functions in Tools, you can upload different language files, save a back up of the database and save the settings of the system. You can also export data on Cardholders and save them as CSV-files[13], which conveniently can be imported to the system.

The System-layer has functions for:

- Saving a backup copy of the database and saving the settings of the system.
- Importing and exporting data for Cardholders.

The Admin-layer has functions for:

- Importing and exporting data for Cardholders.
- Uploading a new Language file. Saving a backup copy of the database.
- Login from the Admin-layer to the System-layer and administer both the layers simultaneously.

The database of the system

The Cardholders, Schedules, Time Channels, Triggers, Access Points and system designations as well as the log is saved in the database of the system.
The configurations for E-mail, GSM modem, Report templates and the Log are saved as settings.

> *Please ensure that you make regular backups of your database and settings! Should you forget your password and be forced to reset the system, you must login with the default password. When doing so, all data will be lost and must be restored. If you have made backups, all data on the system settings and the database is conveniently restored and your system will be re-established.*

[13] CSV is an abbreviation for the file format comma-separated value. It is a file format which stores tabular data and is commonly used on all computer platforms.

Creating a new database (the System-layer)

In order to create a new database, please follow these instructions:

1. Go to **Tools>Database**.
2. Click on **Erase**.
3. A pop-up window will ask you to confirm, **Yes** or **No**.

> *Please note that when you accept to create the new database by confirming Yes, the old database will be erased.*

Saving a backup copy of the database (the System- and Admin-layer)

To **Save a backup copy of the database**, please do as follows:

1. Go to **Tools>Database>Save a backup copy of the database**.
2. Click on **Save** and follow the instructions to save a copy on your computer.

Saving a backup of the settings (the System- and Admin-layer)

In order to **Save a backup of the settings**, please follow these instructions:

1. Go to **Tools>Database>Save a backup of the settings**.
2. Click on **Save** and follow the instructions to save a copy on your computer.

Restoring a copy of the database (the System-layer)

If data has been lost from the system, or if the system is upgraded, the database can be restored. In order to do this, please follow these instructions:

1. Go to **Tools>Database>Restore backup of database**.
2. Click on **Browse**.
3. Select the **file** where the backup has been saved.
4. Click on **Load**.

Restoring a backup of the system settings (the System-layer)

If the settings have been lost from the system, or if the system is upgraded, the settings can be restored. To Restore backup of the settings, please follow the instructions below:

1. Go to **Tools>Database> Restore backup of the settings**.
2. Click on **Browse**.
3. Select the **file** where the settings have been saved.
4. Click on **Load**.

The configuration files of the system (the System-layer)

The Configuration files (**Edit key**) displays and edits the files of the Web server. Please note that a key is required.

Exporting and importing CSV-files – Cardholder data (the Admin-layer)

The data of the Cardholders is saved in a format called CSV[14]. In order to **Export the data of the Cardholders**:

1. Go to **Tools>Cardholders>Export**.
2. Click on **Save** and follow the instructions in order to save the data on your computer.

In order to **Import the data of the Cardholders**, please do as follows:

1. Go to **Tools>Cardholders>Import**.
2. Click on **Browse**.
3. Select the **file** where the data of the Cardholders is saved.
4. Click on **Load** to save the data in smartONE.
5. Select the **columns** you wish to import. The columns are displayed on the top of the window in dropdown menus. If the data for a specific column is not to be imported, please leave the field blank. Please note that you can only have one choice for each designation.
6. Tick the **boxes** on the left for the Cardholders whose data you wish to import.
7. Click on **Apply**.
8. When the import is complete, a pop-up window will confirm so. Click on **Ok**.

The data of your Cardholders is saved in the system[15].

[14] CSV is an abbreviation for the file format comma-separated value. It is a file format which stores tabular data and is commonly used on all computer platforms.

[15] Please bear in mind that when you import the data of the Cardholders, if the data is already saved in smartONE, it cannot be imported again. Should you attempt to import the data again, it will be recognised by the system and an error message will inform you that the data has been identified, thus avoiding duplication.

Changing the language (the System- and Admin-layer)

Should you wish to use another language than English, you can upload one of the Language Files which smartONE supports. Go to **www.smartONE.info** and download the Language File you wish to use. In the System-layer, you can create a new database when the Language File is uploaded. Should you create a new dataase, all previous data will be erased and replaced with data for the new language.

> *Please note that you must have the Language Files for smartONE version 2!*

1. Go to **Tools>Language**.
2. Click on **Browse**.
3. Select the **Language File** of your choice by **double clicking** on the file or highlight it and click on **Open**.
4. Your choice will be displayed in the field **Upload language**.
5. Click on **Load** to execute.

The language of your choice is being uploaded to smartONE.

Using the System- and the Admin-layer simultaneously (the Admin-layer)

Should you wish to, you can use the System- and the Admin-layer simultaneously.

1. **Login** to the **Admin-layer**.
2. Go to **Tools>System login**.
3. Type the **Password** for the **System-layer**.
4. Click on **Login**.

You are now logged into both the **System-** and the **Admin-layer** and have access to every function of the system. Should you wish to return to one layer only, click on **Logout** and login to either the **System**- or the **Admin- layer**.

Configuring a GSM-modem (the System-layer)

By connecting a GSM Modem, Text-messages may be sent from the system to mobile telephones. A Text-message is automatically sent to the receiver, notifying when the system starts up, if there is an Access Point off-line or if divergences should occur by an Access Point, such as Access Point forced or if an incorrect PIN has been repeatedly entered. The Text-messages are charged at the current rates of the operator.

In order to connect a GSM Modem to the system, please ensure that the cable of the Modem model is connected to the door central RJ12. Thereafter, follow the instructions below:

1. Go to **System>GSM modem**.
2. Select the **Modem model** which has been connected to the system. The Modem model is displayed in the dropdown menu.
3. Type the **PIN code** for the **SIM card**.
4. Type the **PUK code**.
5. Type the **Telephone number of the administrator**, to whom the information should be sent.
6. In order to **Test the modem configuration**, click on **Send a text message as a test**.
7. In the dropdown menu, select the **Access Point** which is to register the events and to be opened by using a mobile telephone.
8. If you are using a **Pre-paid phone card**, use this field to **Refill phone card** and **Check phone card balance**. To charge the pre-paid phone card, type the code and click on **Refill**.
9. Type the code to **Check phone card balance**.
10. **Statistics** regarding sent and received messages, type of Modem and Modem RING are displayed in the text box furthest down in the window.

The Modem model is now configured and the system will be able to send Text-messages to the receiver. You will be instantly notified about events for each Access Point which is connected to the Modem.

Opening Access Points via the telephone

You can also unlock the Access Point by simply making a phone call[16]. In order to do so, the phone number must be connected as card data to the Cardholder who is to be granted access. The Access Point is opened when the Cardholder calls the modem.

1. Go to **Cardholder>List**.
2. Select the **Cardholder>Edit** and go to the header for **New Card/tag**.
3. Type the telephone number of the phone which is to open the Access Point in the field following **New Card/tag**.
4. Click on **Save**.

The telephone now acts as an access Card/tag. When the Cardholder calls the telephone number of the modem, the telephone number is identified as valid Card/tag data and the Access Point is thus unlocked. This function is free of charge.

Setting the IP-address manually (the System-layer)

The security system smartONE uses either a static or automatic IP-address. In order to set the IP-address manually, please go to **System>Network**. The **IP-address DHCP** is the connection which is automatically configured via the network. Should you wish to set the IP-address manually, please contact your network administrator to retrieve the information required for the manual IP settings and the DNS-server.

[16] This function requires number presentation.

Explanations, Network

Connection

IP address from
How the IP Address of the system is configured, whether the system uses an IP address from DHCP or Manual IP settings.

Manual IP settings
The system uses the settings stated under the header Manual IP settings.

DHCP
The IP Address and any other Network settings are configured automatically by a DHCP-server.

Media
States the kind of Network media being used. Should Auto be selected, the system recognises the Network media automatically.

Manual IP settings

IP Address
This field states the IP Address of the system.

Subnet mask
This field states the Subnet mask of the Network.

Broadcast
This field states the Broadcast of the Network.

Default gateway
States the Default gateway of the Network.

DNS-server

Primary DNS
States the IP Address of the DNS server to be used.

Host
States the Host of the Network.

Surveillance with a Network camera

The Network camera is used for increased security. The still images are displayed in the user interface, in the window of the Access Point, My Access Points.

Connecting the Network camera (the System-layer)

In order to connect a Network Camera to the system, please follow the instructions:

1. Assemble the **Network Camera** to the **Access Point** which is to be supervised.
2. Return to the user interface and click on **Network Camera>New**.
3. Give the Network Camera a **Name**.
4. Fill out the **Host/Internet address** of the Network Camera.
5. Fill out the **Homepage of Network Camera** to establish a connection to the Network Camera.
6. Fill out the **Path for still image** to create a connection to the still images of the Network Camera.
7. Fill out the **User name** and **Password** if the Network Camera is protected by a password. When the Network Camera is connected to **Method>Through smartONE** directly from the Network Camera, the user name and password must be filled out manually. If the Network Camera is not protected by a password, leave the fields for User name and Password blank.
8. Click on **Test image**. A window will show a still image from the Network Camera.
9. Click on **Save**.

Every Network Camera which is connected to the system is saved in a list. Edit each Network Camera by clicking on the green button, **Edit**. Delete a Network Camera by clicking on the red button, **Delete**.

The Network Camera is connected to smartONE and can be linked to the Access Point in the user interface:

1. In the menu, click on **Access Points**.
2. Go to **List** and select the **Access Point** which the camera should survey.
3. Click on **Edit**. Under the header **Miscellaneous>Network Camera**, the name of the Network Camera is stored in the dropdown menu.
4. Select the **Network Camera** and click on **Save**.

Go to **My Access Points** in the **Admin-layer**. Still images from the Network Camera are displayed in the window of the Access Point it is linked to. The still images are automatically updated every time an event occurs at the Access Point, or if you click on the button **Update**. You can zoom in by clicking on the image. The Access Point is unlocked if you click on the symbol **Open**. When somebody presses the Door bell (the symbol star key ⊛) on the Card Reader of the Access Point, as well as sending a signal, a separate window with an image from the Access Point appears. If you wish to not see the images, click on **Close**. Some Network Cameras show moving images, depending on the specification of the camera.

Performance of smartONE	
Access Points	Up to 16 Access Points, 8 connected to the Door Central SO-3008 and 8 additional to the expansion card SO-3016. The expansion card is connected to the Central Unit.
Door codes	2 Door codes for each Access Point.
Cardholders	Up to 2 500.
Cards	Up to 2 500.
Time Channels	Up to 50.
Triggers	Up to 50.
Schedules	Up to 50.
Schedule items	Up to 200 items, spanning over all the created Schedules.
Special days in the Calendar	Up to 50.
Contact lists	Up to 10.
Users	Up to 10.
Departements	Up to 100.
Network Cameras	Up to 16, one for each Access Point.
Log	Up to 10 000 events.

Accessories	
GSM modem	In order to send text-messages and open the Access Points using the telephone, a separate GSM modem is required.

TIDOMAT smartONE
version 2

- User manual -

Appendix

I – IV

TIDOMAT

Content

Appendix I

The Access Points

The Access Point is to be attached to a connector and given a name. The Access Points which have been connected to the system but not been configured in the user interface are found in the dropdown menu under the header **Access Point>New>Connector**. The Access Point can be edited in the **System-layer**. The Door codes may be updated in the **Admin-layer**, but no other editing of the hardware configuration may be carried out. Select the Access Point and configure it according to your choices.

Each Access Point connected to the system is displayed under the header **My Access Points**. For further information, please read the ***Start Guide for smartONE***.

Configuring the hardware of the Access Points in the system

Connector
P1-P8 and P1-P16. Select the Access Point which is to be configured. P1-P8 is for a system with eight Access Points and P1-P16 is for a system supporting sixteen Access Points. For a system supporting sixteen doors, an Expansion Card with connectors for P9-P16 is attached to the Central Unit.
P = Access Point.

Name
The name of the Access Point.

Type of Card Reader

The system supports two different kind of Card Readers:

- the smartONE Reader
- OEM-Reader (clock & data, ABA, track 2).

Input EXTIN

Is used when the Access Point is configured. This option controls the functions of the Input EXTIN.

Empty field

No function is activated.

Egress (exit) button

This function is used when the Access Point is to be unlocked according to an external control.

- Input EXTIN output open = the Access Point is locked.
- Input EXTIN output closed = the Access Point is unlocked.

Block Door code 2

This function is used when the Access Point is to block Door code 2 according to an external control.

- Input EXTIN output open = Door code 2 is blocked.
- Input EXTIN output closed = Door code 2 is in operating mode.

Block Door code 1 and 2

This function is used when the Access Point is to block Door code 1 and 2 according to an external control.

- Input EXTIN output open = Door code 1 and Door code 2 are both blocked.
- Input EXTIN output closed = Door code 1 and Door code 2 are both in operating mode.

Request PIN

- Input EXTIN output open = PIN is requested with the Card/tag.
- Input EXTIN output closed = Card/tag without PIN is used.

Request PIN + block Door code 1

- Input EXTIN output open = PIN is requested with the Card/tag. Door code 2 is blocked.
- Input EXTIN output closed = Card/tag without PIN is used. Door code 2 is in operating mode.

Request PIN + block Door code 2

- Input EXTIN output open = PIN is requested with the Card/tag. Door code 1 and Door code 2 are both blocked.
- Input EXTIN output closed = Card/tag without PIN is used. Door code 1 and Door code 2 are both in operating mode.

Door Contact

The feedback from for example the bolt contact of the Electric Door Strike, (DOOR).

- Input EXTIN output open = indicates to the system that the Access Point is open.
- Input EXTIN output closed = indicates to the system that the Access Point is closed.

Block Access Point

- Input EXTIN output open = the Access Point is blocked. The manual relay control and the Doorbell are in operating mode.
- Input EXTIN output closed = normal function.

Electric Door Strike, (DOOR)

The Electric Door Strike, (DOOR) is supplied with the same voltage as the Central Unit, 24 VDC or 12 VDC. *Please note that the current consumption of the Electric Door Strike, (DOOR) must not exceed 500 mA.*

- Normally open (N/O) = voltage when activating.
- Normally closed (N/C) = voltage when resting.

Relay output (AUX)

The Relay output (AUX) is mainly used for controlling the external units of for example motor operated locks, external alarms or lights. *Please note that the charge of the Relay output (AUX) must not exceed 1 A/VD, or the units may be permanently damaged*.

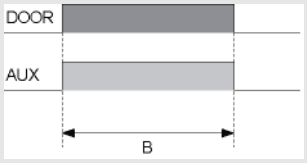
Relay function (AUX)

Controlled via Time Channel

The Relay output (AUX) is controlled via a Time Channel.

Parallel with DOOR output

The Relay output (AUX) is activated throughout the time the Access Point is unlocked.

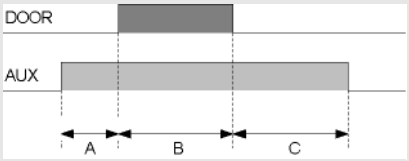


B = Unlocked for a maximum of (the time is active until the Access Point is closed).

Alarm by pass

The Relay output (AUX) is activated before the Access Point is unlocked. The Relay output A is continuously active after the time the Access Point has been unlocked, C.

- The time for A is set under the header **Delay between Door Strike (DOOR) and relay (AUX)**.
- The time for B is set under the header **Unlocked for a maximum of**.
- The time for C is set under the header **Relay (AUX) delay after released Door Strike (DOOR)**.

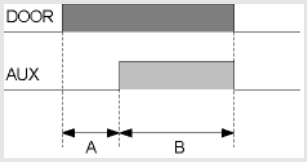


A = Delay between Door Strike (DOOR) and relay (AUX).
B = Unlocked for a maximum of (the time is active until the Access Point is closed).
C = Relay (AUX) delay after released Door Strike (DOOR).

Automatic door

The Relay output (AUX) is activated after the Access Point has been unlocked. The Automatic door should be connected to the Relay output (AUX).

- The time for A is set under the header **Delay between Door Strike (DOOR) and relay (AUX)**.
- The time for B is set under the header **Unlocked for a maximum of**.

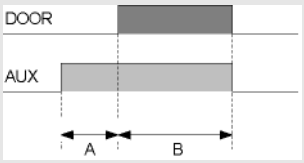


A = Delay between Door Strike (DOOR) and relay (AUX).
B = Unlocked for a maximum of (the time is active until the Access Point is closed).

Motor operated lock

The Relay output (AUX) is activated before the Access Point.

- The time for A is set under the header **Delay between Door Strike (DOOR) and relay (AUX)**.
- The time for B is set under the header **Unlocked for a maximum of**.



A = Delay between Door Strike (DOOR) and relay (AUX).
B = Unlocked for a maximum of (the time is active until the Access Point is closed).

Manual control from Card Reader

The Relay output (AUX) is controlled via the keyboard of the Card Reader. For further information, please read the *User Manual for smartONE, Appenix II*.

- Activate the output = ⌗ + 1 + Card/tag (if the green/yellow light flashes, enter the PIN).
- Inactivate the output = ⌗ + 0 + Card/tag (if the green/yellow light flashes, enter the PIN).
- Activate the pulse. = ⌗ + 2 + Card/tag (if the green/yellow light flashes, enter the PIN).

The right to control the Relay Functions via the Card Reader is granted under the header **Cardholder**. Should a Cardholder which does not have the right attempt to control the Card Reader, a red light will flash.

Manual control from Card Reader and off by Exit button

The Relay output (AUX) is activated via the key board of the **Card Reader** and inactivated via the key board of the Card Reader or the Exit button. For further information, please read *Appendix II*.

- Activate the Relay output (AUX)= ⌗+ 1 + Card/tag (if the green/yellow light flashes, enter the PIN).
- Inactivate the Relay output (AUX).= ⌗ + 0 + Card/tag (activate the output PIN).
- Pressing the Exit button =inactivate the Relay output (AUX).

The right to control the Relay Functions via the Card Reader is granted under the header Cardholder. Should a Cardholder which does not have the right attempt to control the Card Reader, a red light will flash.

On at access from Card Reader + off by Exit button
The Relay output is automatically activated when the Access Point is opened with Card/tag or the Door code. It is inactivated via the Exit button.

- Activate the Relay output (AUX) = Card/tag or Door code.
- Inactivate the Relay output (AUX) = pressing the Exit button.

The right to control the Relay Functions via the Card Reader is granted under the header **Cardholder**. Should a Cardholder which does not have the right attempt to control the Card Reader, a red light will flash.

External Door bell
The Relay output (AUX) is activated via the key board of the Card Reader.

- ⊛ = activate the Relay output (AUX) for the set time (refers to Duration for Door bell / relay pulse).

Relay polarity (AUX)

Normally open (N/O)
Closure when activated (NO).
Normally closed (N/C)
Disconnection when activated (NC).

Time duration for Access Point

The settings of the time duration for the Access Point.

Unlocked for a maximum of
The time which is sent to the Electric Door Strike, (DOOR). Should this time be set as 0, the function toggles from locked to unlocked every second time. If the function **Door Contact** is applicable, the Electric Door Strike will lock as soon as the Access Point opens.

Delay between Door Strike (DOOR) and relay (AUX)
The function which is to be activated first is set under the header **Relay function (AUX)**.

Relay (AUX) delay after released Door Strike (DOOR)
States for how long time the delay remains after the Access Point is closed or locked, when the function **Door Contact** is selected.

Door held-open-warning
States for how long the Card Reader should give a warning signal via a buzzer if the Access Point is open for too long. If the Access Point is still open after the set time, the relay will activate an external alarm. If the time is set to 0, the alarm will be triggered as soon as the time for unlocked door is up. This function requires the function **Door Contact** to be selected. The Card Reader must have a buzzer in order to give a warning signal.

Anti-passback
The same card will not open the Access Point twice during the set time.

Door codes

The system supports two Door codes for each Access Point. The Door codes can be edited in both the **System**- and the **Admin-layer**.

Door code 1
Sets Door code 1, for general access to a building or premises. The Door code is four digits. If the field is blank, Door code 1 is blocked.

Door code 2
Sets Door code 2, for alternative access to a building or premises, to people who should have limited access. Door code is four digits. If the field is blank, Door code 2 is blocked.

Block duration after incorrect Door code
States for how long the Card Reader should be blocked if incorrect Door codes are entered.

Number of incorrect digits before the Card Reader blocks
How many times incorrect Door codes can be entered before the Card Reader is blocked.

PIN-codes

Decides how the Access Point should grant access when PIN is requested.

PIN code timer
PIN code timer is a function used when an Access Point grants access with Card/tag+PIN only to grant access if the same Card/tag is displayed to the Card Reader without requesting PIN for the set time. The function has great advantages in for example a warehouse, where the security calls for Card/tag and Card/tag + PIN, but for a short space of time, the convenience of displaying the Card/tag only is of help.

- Should PIN code timer be used, please state the time for how long the Access Point is to grant access by displaying the Card/tag only.
- Should PIN code timer not be used, leave the field blank.

Every Cardholder can use the function at each Access Point which it is connected to.

Request PIN

According to control + PIN code timer
According to Input EXTIN. The function PIN code timer is in use.
According to control (PIN code timer inactive)
According to Input EXTIN. The function PIN code timer is not in use.
Always request PIN + PIN code timer
According to PIN. The function PIN code timer is in use.
Always request PIN (PIN code timer inactive)
According to PIN. The function PIN code timer is not in use.

Miscellaneous

Further settings for the Access Point.

Grant from Authorized Level

This function is used when a Cardholder of the selected Authorized level or above must enter the Access Pointe before anyone below the selected Authorized level may enter the same Access Point. When a Cardholder of the selected Authorized level or above has entered the Access Point, Cardholders of any other Authorized level is granted access.

Show-card-twice function

The Card/tag is displayed to the Card Reader twice within a time span of 20 seconds. This function supports a variety of actions:

Toggle unlocked/locked

When the Card/tag is displayed to the Card Reader twice, the Access Point will toggle from being unlocked to locked. The Access Point is unlocked the first time the Card/tag is displayed twice in 20 seconds, and it is locked the second time it is displayed twice in 20 seconds.

Unlocked/locked by Exit button

When the Card/tag is displayed to the Card Reader twice, the Access Point is unlocked. By pressing the Exit button, the Access Point is locked.

Toggle relay

When the Card/tag is displayed to the Card Reader twice, the Relay will toggle.

*The window **My Access Points** in the user interface shows a yellow symbol when the Show-card-twice function is utilised. The function can be inactivated from that window.*

Card/tag format

The different Card Readers, smartONE Reader and OEM Reader sometimes identifies the Card/tag in different ways. By formatting the Card/tag manually, the same card data will be displayed no matter which Card Reader is being used.

The Card/tag format is stated as follows:

```
Cardformat string

[rn.] [s[-]n] cardbits. cardlen. sitebits. sitelen

r = reverse bits
s = shift bits, - => left shift.

cardbits Number of bits (LSB) from card data. - =>
reverse bits (0=auto)
cardlen Number of digits in card result  (0=auto)
sitebits Number of bits in sitecode (0=no
sitecode)
sitelen  Number of digits in sitecode result
(0=auto)

Exampel use 24 bits of card and 8 bytes in result.
24.8

Exampel use 14 bytes in result.
0.14

Exampel shift 1 bit and use 24 bits of card data.
  s1.24
```

Network Camera

Should you have connected a Network Camera to the Access Point, the name of it will be displayed in the dropdown menu. Select the Network Camera which is to be connected to the Access Point. *The images from each Network Camera are displayed in the windows of the Access Point,* ***My Access Points****.*

Last used Card/tag

The last Card/tag to be registered by the system is displayed here.

Log

A link to the settings for the Log of this Access Point.

The Exit button

The main use of the Exit button is for opening the Access Point when leaving a building.

The Exit button:

- Should be closed NO (potential free).
- Is not in operating mode when the Access Point is blocked.
- Is controlled by events, which means that it responds to when it is pressed by unlocking the Access Point. It will, nevertheless, only open the Access Point for the time set under the header **Access Points>Time Duration for Access Point>Unlocked for a maximum of (seconds)**. It is thus not possible to unlock the Access Point for longer than the set time by pressing the button.

Block Access Point

The Access Point can be blocked from **Time Channel>Time Channel New/edit>Type>Block Access Point** or via **Input EXTIN** under the header **Access Point New/Edit>Hardware configuration>Input EXTIN>Block Access Point**.

When the Access Point is blocked:

- The red light on the Card Reader will be on.
- If the Access Point is unlocked, it will switch to being locked.

Appendix II

Included is general information on how to use the Card Reader.

The Card Reader

Red light

- One fast flash = pressed key or registered Card/tag.
- Static light = the Access Point and/or the Card Reader are blocked.
- Constant, fast flashes 3 Hz = general or communications error.

Green light

- Static light = the Access Point is unlocked.
- Constant, fast flashes = display the Card/tag.
- Slow flash 1 Hz = enter PIN or select a function.

Yellow light (only applicable for Card Readers with yellow light)

- Slow flash 1 Hz = enter PIN or select a function.

Buzzer

- One, fast signal = pressed key or registered Card/tag.
- Repetitive signals = incorrect Door code or Access Point forced.
- Repetitive, fast signals = warning signals for an Access Point which is open for too long. The signal stops when the Exit button is pressed or the Access Point is closed.

Using the Door codes

- Enter the Door code. For every time a key is pressed, a red light will flash and a signal will make a fast, beeping sound.
- Should the Door code be correctly entered, the Card Reader will indicate so by showing a static green light and unlock the Access Point.
- Should nine incorrect keys be pressed (the number nine is a default value and can be edited under the heading **Access Point>New/Edit/Door codes> Number of incorrect digits before the Card Reader blocks**). The Card Reader is blocked for 30 seconds (which is the default value and can be edited under the heading **Access Point>New/Edit/Door codes> Block duration after incorrect Door code**).

To use the Card Reader with Card/tag without PIN

1. Display the Card/tag to the Card Reader.
2. If access is granted, the green light flashes and the Access Point unlocks.

To use the Card Reader with Card/tag and PIN

1. Display the Card/tag to the Card Reader.
2. If the Card/tag will grant access after the PIN has been entered, a green/yellow light will flash slowly,1 Hz.
3. Enter the PIN.
4. If the correct PIN is entered, the green/yellow light will be static and the Access Point is unlocked.

Manual control of the Relay Functions

To activate the Relay output

1. Press ⌗ (the green/yellow light will flash slowly) + ① (the green light will flash).
2. Display the Card/tag to the Card Reader.
3. If the green/yellow light flashes slowly, enter the PIN.
4. If the Cardholder has the right to control the Relay Function, the green light will be static for three seconds and the Relay output is activated.

To inactivate the Relay output

1. Press ⌗ (the green/yellow light will flash slowly) + ⓪ (the green light will flash).
2. Display the Card/tag to the Card Reader.
3. If the green/yellow light flashes slowly, enter the PIN.
4. If the Cardholder has the right to control the Relay Function, the green light will be static for three seconds and the Relay output is inactivated.

To activate the Relay pulse

1. Press ⌗ (the green/yellow light will flash slowly) + ② (the green light will flash).
2. Display the Card/tag to the Card Reader.
3. If the Cardholder has the right to control the Relay Function, the green light will be static for three seconds and the Relay pulse is activated.

Appendix III

Variables for smartONE

The variables for smartONE are used for custom messages. Those are applicable in the functions for Text-messages, IP notify and HTTP request.

Please note that some experience using Data Syntax is an advantage when applying smartONE variables.

The variables follow this syntax:

`$(VARIABLE[,Formatting Options[,..]])`

Add binary data to the message:

The syntax is as follows:

`$(n)`

For example:

`$(1)` ➔ SOH
`$(27)` ➔ ESC
`$(23)` ➔ ETB

System variables

Variable	Description	Note
SYS.DATETIME	Date & time `$(SYS.DATETIME, DATE=Y-m-d G:H:i)`	See table DateFormat, page 23.
SYS.SERNO	Serial number.	
SYS.VERSION	Version	
SYS.NAME	Name	

Database variables		
Variable	**Description**	**Note**
DB.CARDHOLDER	The field **Object designation**	Default: Cardholder
DB.LABEL1	Field 1designation	Default: First name
DB.LABEL2	Field 2 designation	Default: Surname
DB.LABEL3	Field 3 designation	
DB.LABEL4	Field 4 designation	
DB.LABEL5	Field 5 designation	
DB.DROPDOWN	Designation of the object Groups	Default: Department
DB.UNIQUE	Field 6 (unique for each)	Default: Employee number

Trigger variables - available in Triggers only		
Variable	**Description**	**Note**
TYPE	Event type	See table Event type, page 26.
TYPE.NAME	Event type (Text)	See table Event name, page 26.
TIMESTAMP	Date time	See table DateFormat, page 23.
DOOR.ID	Door id	
NAME	Door name	
PORT	Port (P1 to P16)	
LABEL1	Label1 from cardholder	
LABEL2	Label2 from cardholder	
LABEL3	Label3 from cardholder	
LABEL4	Label4 from cardholder	
LABEL5	Label5 from cardholder	
UNIQUE	Unique from cardholder	
TRIGGER.ID	Trigger id	
TRIGGER.NAME	Trigger Name	
COUNTER	The number of times the Trigger has been executed	

Formatting Commands

The formatting commands take a value and are separated by commas (`,`) one after another.

```
FORMATTINGOPTION1=VALUE, FORMATTINGOPTION2=VALUE
```

Option	Description	Note
LEN LENGTH	This parameter sets the width of the text output. The remaining space is filled using the fill character. "0" is variable width. If the text is larger than defined in LENGTH, the output width is enlarged automatically, if the Formatting Switch TRUNCATE has not been set. Default value: 0	
FIL FILL	Sets the fill character(s) to be used to format the output. Example: `$(ABC, LENGTH=5, FILL=*)` Default value: [Space]	
ALI ALIGN	This parameter sets the alignment of the text output within the specified length. Default value: LEFT	RIGHT CENTER LEFT
DATE	Format variable as a date field Default value: r	See table DateFormat, page 23.

QUOTE	Quote string Default value: “ Example: `$(TEST, QUOTE)` ➔ “TEST” Example: `$(TEST, QUOTE=[])` ➔ `[TEST]`	Add backslashes before QUOTE character in value
TRUE	Output string if value <> 0 Default value: on	
FALSE	Output string if value = 0 Default value: off	

Formatting Switches

The formatting switches do not take a value and are separated by commas (`,`) one after another.

Switch	Description	Note
TRU TRUNCATE	Cuts off any text longer than specified by LENGTH.	
B64 BASE64	Switches text output to Base64 encoding (this is required by some email servers, for example)	Use this switch to supply user information, for example: `$("name:pass", BASE64).`
REPEAT	Repeat text specified by LENGTH.	
URL	URL-encodes string	
UPPER	All alphabetic characters converted to uppercase. Characters such as umlaut-a (ä) will not be converted.	
LOWER	All alphabetic characters converted to lowercase. Characters such as umlaut-A (Ä) will not be converted.	

UCFIRST	First character capitalized, if that character is alphabetic. Characters such as umlaut-a (ä) will not be converted.	
HTML	Convert all applicable characters to HTML entities.	

Table DateFormat

The following characters are recognized in the *format* parameter string

Format character	Description	Note
Day		
d	Day of the month, 2 digits with leading zeros	01 to 31
D	A textual representation of a day, three letters	Mon through Sun
J	Day of the month without leading zeros	1 to 31
l (lowercase L)	A full textual representation of the day of the week	Sunday through Saturday
N	ISO-8601 numeric representation of the day of the week.	1 (for Monday) through 7 (for Sunday)
S	English ordinal suffix for the day of the month, 2 characters	st, nd, rd or th. Works well with j
w	Numeric representation of the day of the week	0 (for Sunday) through 6 (for Saturday)
z	The day of the year (starting from 0)	0 through 365

Week		
W	ISO-8601 week number of year, weeks starting on Monday (added in PHP 4.1.0)	Example: 42 (the 42nd week in the year)
Month		
F	A full textual representation of a month, such as January or March	January through December
m	Numeric representation of a month, with leading zeros	01 through 12
M	A short textual representation of a month, three letters	Jan through Dec
n	Numeric representation of a month, without leading zeros	1 through 12
t	Number of days in the given month	28 through 31
Year		
L	Whether it's a leap year	1 if it is a leap year, 0 otherwise.
o	ISO-8601 year number. This has the same value as Y, except that if the ISO week number (W) belongs to the previous or next year, that year is used instead.	Examples: 1999 or 2003
Y	A full numeric representation of a year, 4 digits	Examples: 1999 or 2003
y	A two digit representation of a year	Examples: 99 or 03

Time		
a	Lowercase Ante meridiem and Post meridiem	am or pm
A	Uppercase Ante meridiem and Post meridiem	AM or PM
B	Swatch Internet time	000 through 999
g	12-hour format of an hour without leading zeros	1 through 12
G	24-hour format of an hour without leading zeros	0 through 23
h	12-hour format of an hour with leading zeros	01 through 12
H	24-hour format of an hour with leading zeros	00 through 23
i	Minutes with leading zeros	00 to 59
s	Seconds, with leading zeros	00 through 59
Full Date/Time		
c	ISO 8601 date	2004-02-12T15:19:21+00:00
r	RFC 2822 formatted date	Example: Thu, 21 Dec 2000 16:01:07 +0200
U	Seconds since the Unix Epoch (January 1 1970 00:00:00 GMT)	

Table Event type	
The outcome language depends on the selected language of the System Texts.	
TYPE	TYPE.NAME
0	Access Granted
1	Door Code Granted
2	Exit button
3	Access Granted from web
5	Access Point Forced
6	Show-card-twice
8	Access Denied
16	Output (EXT) OFF
17	Output (EXT) ON
18	Output (EXT) pulse
34	Locked
35	Unlocked
48	Unknown Card/tag
49	PIN Denied
50	Door Code Denied

Appendix IV

IP Notify

In order to send messages with IP Notify, please state the address of the receiver according to the instructions below.

Receiver

Enter the IP address/es and the port/s to which smartONE is to send the network message in the field for Receiver.
 	
Example
 	
`192.155.13.22:8000`
`Upd://192.155.13.22:8000`
`Alertcenter1.mycompany.net:8701`
 	
Please note that:
 	
• Should you wish to send the message to several computers, enter each address separately.
• It is also possible to use symbolic names. In order to do so, you need to enter a DNS server in the network dialog.

HTTP Request

In order to send messages with HTTP Request, please state the address of the receiver according to the instructions below.

Receiver

Enter the HTTP Request address to which the smartONE is to send the HTTP message in the field for Receiver.
 	
Example
 	
`http://192.155.13.22/cgi-path/trigger.cgi`
`alertcenter1.mycompany.net:8080/cgi-path/alert.cgi`
`http://username:password@hostname/path`
 	
Please note that:
 	
• It is also possible to use symbolic names. In order to do so, you must enter a DNS server in the network dialog.
• HTTP Authentication: enter the user name and password information (`user:password`) in this field.