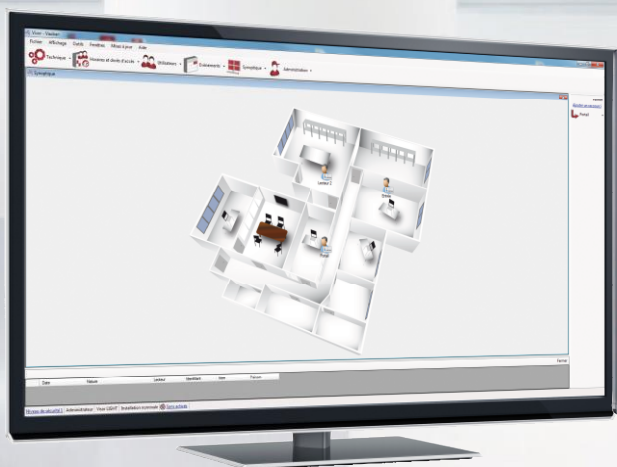


VISOR®

V2.0.0.25

USER GUIDE



Getting started	6
First launch of the software	7
Installations management	8
Creating an installation	9
Single-station installation (Access database):	10
Client/server installation : server station (SQL Server database) :	10
Client/server installation : client station (SQL Server database) :	11
Installation poste server (base de données ACCESS ou SQL Server) :	12
Changing the settings of an existing installation	13
Installation with an Access database:	13
Installation with a SQL Server database:	13
Removing an existing installation	14
Saving an existing installation	15
Restoring an installation	15
Restoring an installation using a SQL database:	15
Migrating an existing ACCESS database installation to a SQL SERVER database	16
Opening an existing installation	17
First opening of an installation:	17
Forgotten password	18
Managing the menus	19
The toolbar	19
The installation status	20
The additional list of events	20
The status bar	21
The shortcuts and the remote control	21
The shortcuts	21
The remote control	22
The File menu	22
The Display menu	23
The Tools menu	23
Event configuration	24
Favourites	25
Badge printing templates	39
Module management	41
Company management	42
Automatic import	46



Automatic export.....	51
The Windows menu.....	52
The Updates menu.....	52
Updating a unit or an extension module:	52
Software update	53
Technical menu	54
Units	54
Creating a unit.....	54
The VERSO, Verso+1, VERSO+2 and Verso+4 unit.....	56
The Digitouch unit	58
The Digitouch Mini unit	60
The Sootouch IP unit.....	62
Extension modules	63
Creating an extension module.....	63
V-EXT4, V-EXT4+ module	64
V-EXTIO module	66
V-EXTLCD module.....	67
APERIO® reader	68
SMART INERGO reader	70
V-EXTINT module	72
Automatic devices	74
ADDING A condition	75
Adding an action.....	78
Counters	80
Analogue inputs	81
LCD messages	82
Online automatic devices	82
Zones management.....	84
Video servers	86
Creating a video server	86
Create an IP camera	87
Camera settings.....	89
Creating a video matrix.....	92
Configuring a central unit reader	94
Advanced reader parameters	101
Wiegand keypad	101



Clock & data reader	102
Personalised Clock & Data	102
Deister Clock & Data reader	104
Digit MINI EXT reader	104
Reader with keypad (HID RK40 or other equivalent product)	106
OSDP reader (HID)	106
S33 Reader (STID)	107
SSCP Reader (STID)	108
Wiegand reader	108
26 bits Wiegand reader	109
30 bits wiegand reader	109
Wiegand Reader 32 bits	110
Wiegand Reader 56 bits	110
Wiegand decimal reader	110
Personalised decimal Wiegand	111
Personalised Wiegand	111
Multiformat Wiegand Reader	112
Wiegand Vauban Systems reader	113
Zomofi Reader	113
Display modules management	114
Lifts management	118
Autinor lifts management	120
Schedules and access groups menu	122
Managing time ranges	122
Managing public holidays	124
Managing special days	125
Managing access groups	125
Managing an access group	126
Exporting the access groups settings	129
Users menu	131
Creating users	131
Managing identifiers	135
Adding an identifier	136
Modifying an identifier	137
Deleting an identifier	137
Export the identifiers	138

Managing users	139
Adding or modifying a user	139
Deleting users	145
Modifying several users at a time	146
User privacy	147
Custom list of users	147
Managing a query	149
Reset users anti-passback.....	151
Importing a list of users	151
Presence time	153
Managing the present user	154
Events menu	156
Events display	156
Event history and reports	156
Managing a query	158
Daybook Menu	160
Adding an entry	161
Category management.....	161
Maps menu.....	162
Editing the maps	162
Opening the maps.....	163
Administration menu	164
Creating a manager.....	164
Managing shortcuts	169
Create a shortcut.....	169
Shortcut configuration	170
Types of shortcuts.....	170
Appendices	173
List and version of sdk integrated in VISOR	173
SQL Server Compatibility	173

GETTING STARTED

You have just installed VISOR, the access control software. The different stages described in this guide will provide you with all the information required to use the software.

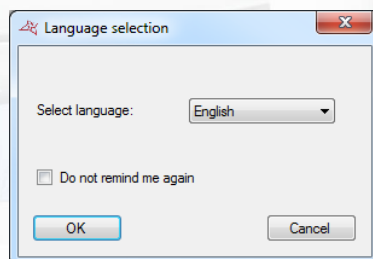
Happy reading!

Vauban Systems



FIRST LAUNCH OF THE SOFTWARE

At first launch of the software, VISOR asked to select your language:



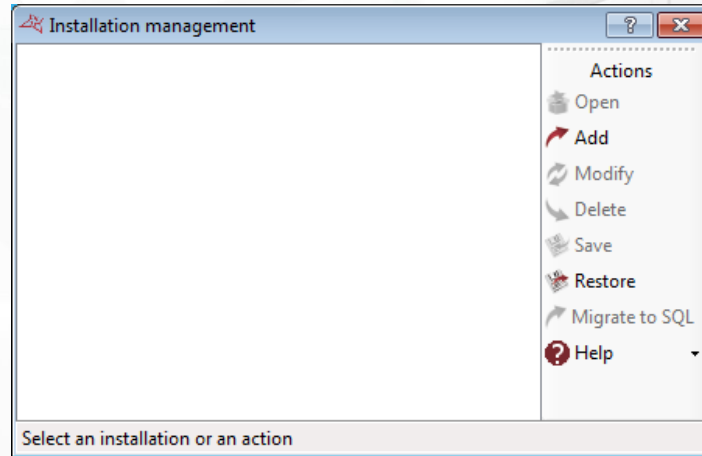
Select your language then press **"OK"**. You can also check the box **"Don't remind me again"** if you don't want VISOR to ask you for the language at every launch.

If you want to display the choice of language at startup again, go to the **"Tools"** menu, **"Preferences"** and check the **"Request language at startup"**.

If you want to create a new installation, click **"Yes"** when prompted.

INSTALLATIONS MANAGEMENT

After selecting your language, the following window appears:

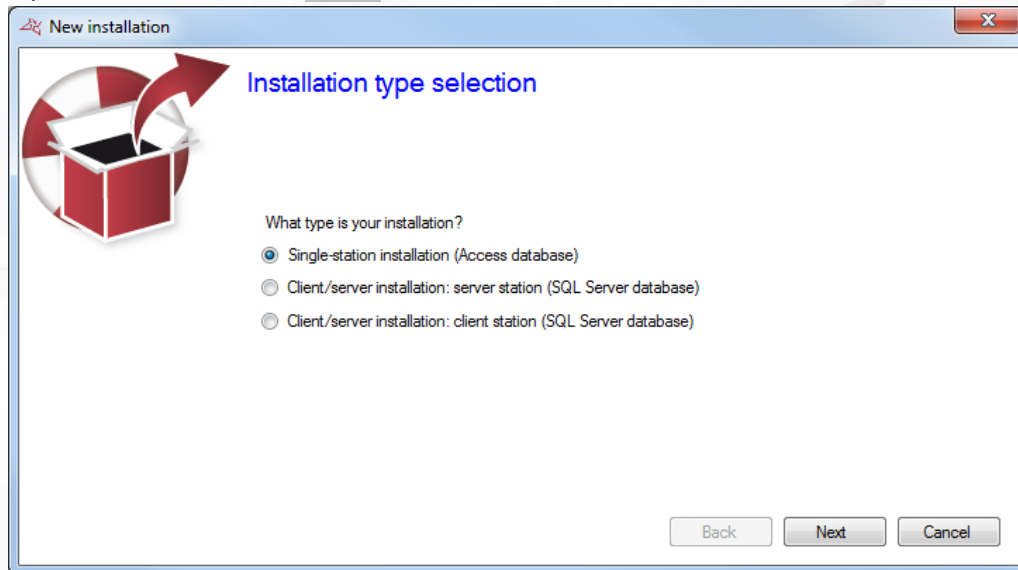


This window allows you to:

- + Open an existing installation
- + Add a new installation
- + Change the settings of an existing installation
- + Delete an existing installation
- + Save an existing installation
- + Restoring a system from a backup file
- + Migrate an ACCESS database installation to a database SQL SERVER
- + View the software help
- + Start a remote support session
- + Request a forgotten password

CREATING AN INSTALLATION

From the previous window, click "Add".



In this window, select the type of installation:

If you are only using one PC:

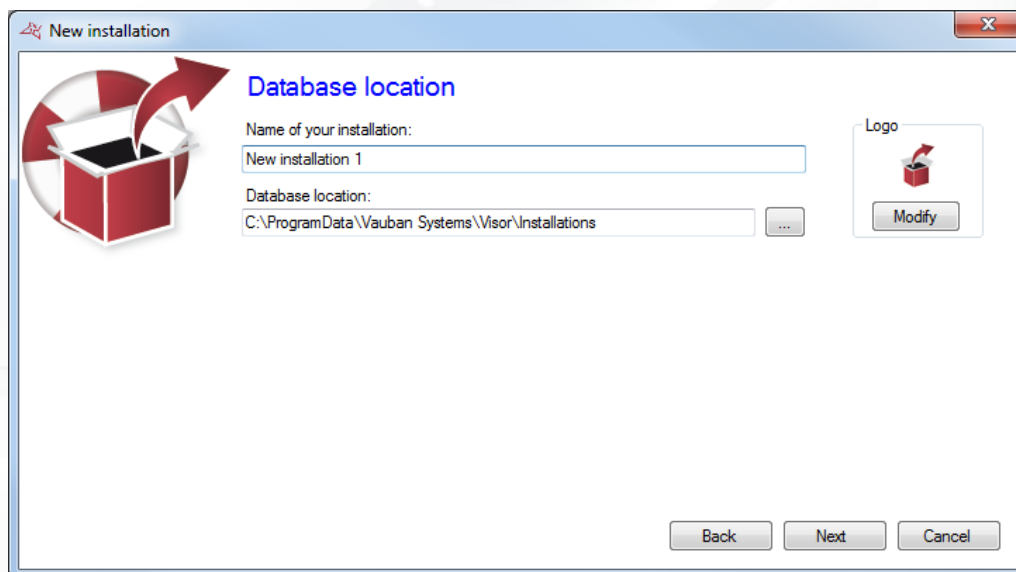
- + Select "Single-station installation (Access database)".

If you are using several PCs:

- + If you are installing VISOR on the server station, select "Client/server installation: server station (SQL Server database)".
- + Caution: the server station must always be left on.
- + If you are installing VISOR on a client station, select "Client/server installation: client station (SQL Server database)".

Click "Next".

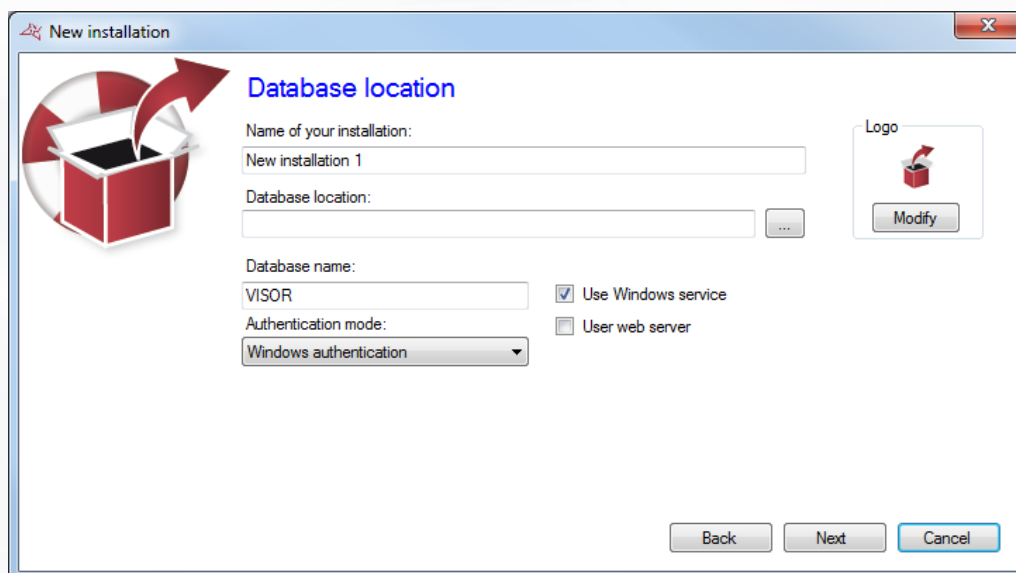
SINGLE-STATION INSTALLATION (ACCESS DATABASE):



From this window:

- + Specify the name of your installation
- + Specify the location of the database. You can use the button [...] to display the file system of your computer. The default directory is in the "ProgramData" folder of Windows. Be careful if you change this folder, make sure VISOR has access rights to read and write on it.
- + Change the image of the installation. To do this, click the "Edit" button.

CLIENT/SERVER INSTALLATION : SERVER STATION (SQL SERVER DATABASE) :




From this window:

- + Specify the name of your installation
- + Specify the path to your SQL Server. You can use the button [...] to display the list of the SQL servers on your network.
- + Specify the name of your database (default is "VISOR")

- + Specify the authentication mode of your SQL Server (Windows authentication - using the user of the Windows session currently opened on the computer - or SQL authentication - using the login "sa" or another and the password defined during the installation of the SQL Server instance). If you do not have a Windows domain and / or the user of the currently opened Windows session is not allowed on the database, use SQL Authentication.
- + Specify to use the Windows service: This allows to close the computer Windows session while maintaining active the dialogue with the units (eg the use of global anti-pass-back between several units, online automation, management of Galaxy HoneyWell units - Additional license required in this case - VISORWeb). If you use the Windows service, using SQL authentication is mandatory.
- + Specify to use VISORWeb if it is installed on your computer. In this case, using the Windows service is mandatory.
- + Specify the image of the installation. To do this, click the "Edit" button.

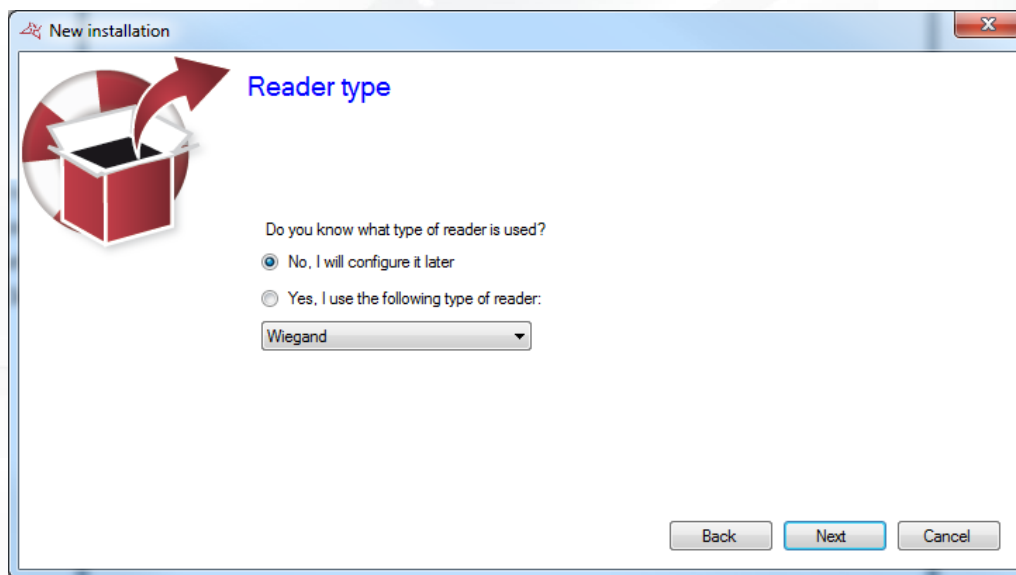
CLIENT/SERVER INSTALLATION : CLIENT STATION (SQL SERVER DATABASE) :

From this window:

- + Specify the name of your installation
- + Specify the path to your SQL Server. You can use the button  to display the list of the SQL servers on your network. Warning, if you want to access a remote SQL Server instance (eg VPN or NAT rule), scanning the server will not work. You must then specify the path to your database as follows: IPAddress,Port (eg 192.168.1.1,1433).
- + Specify the name of your database (default is "VISOR")
- + Specify the authentication mode of your SQL Server (Windows authentication - using the user of the Windows session currently opened on the computer - or SQL authentication - using the login "sa" or another and the password defined during the installation of the SQL Server instance). If you do not have a Windows domain and / or the user of the currently opened Windows session is not allowed on the database, use SQL Authentication.
- + Specify the image of the installation. To do this, click the "Edit" button.

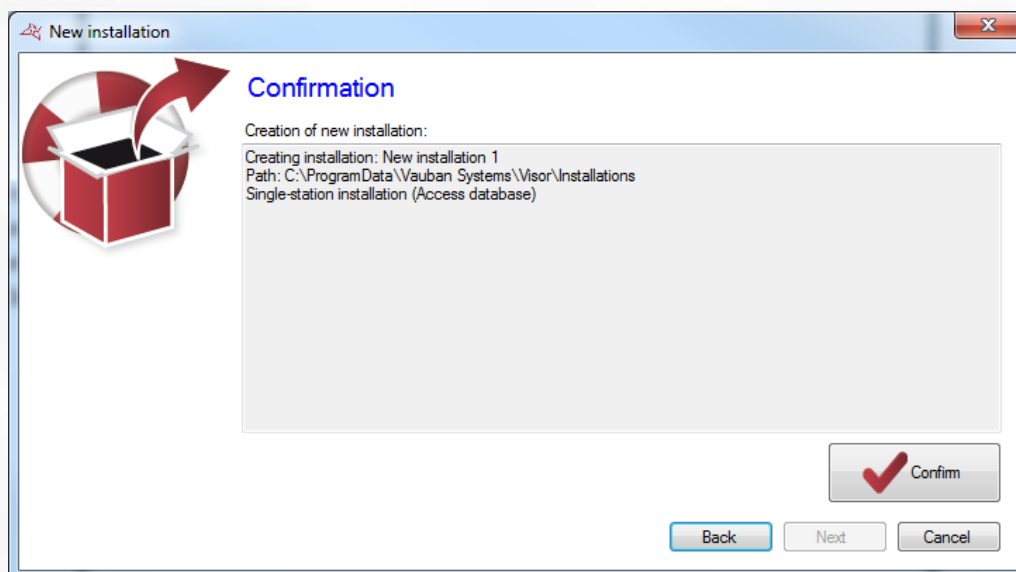
Click "Next".

INSTALLATION POSTE SERVER (BASE DE DONNEES ACCESS OU SQL SERVER) :



From this window, if you have the same type of reader for all your access, check the option "Yes, I use the following type of reader" and select your type or reader in the list. This will prevent you to set the type of reader for all units and extension modules of your installation.

Click "Next".



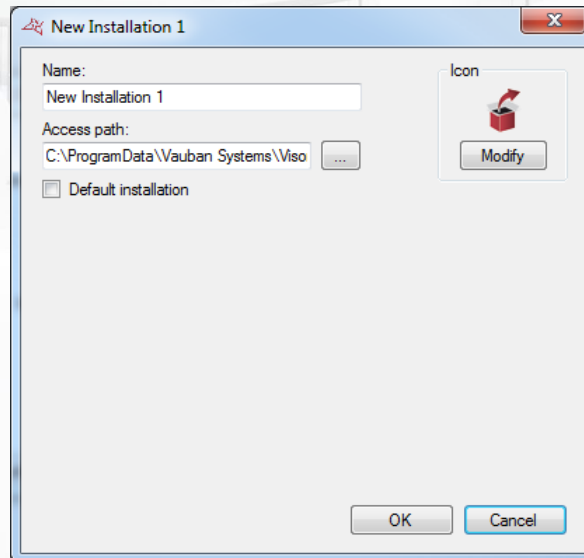
Check all the information based on your previous settings and click "Confirm".

If the Windows service is used, a message will appear asking you to restart it. Then click on "Yes" when prompted.

CHANGING THE SETTINGS OF AN EXISTING INSTALLATION

From the installation management window, select your installation and click "Edit".

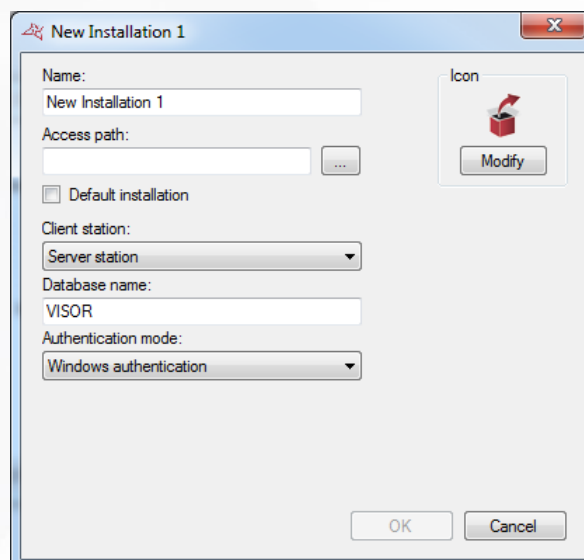
INSTALLATION WITH AN ACCESS DATABASE:




From this window:

- + Specify the name of your installation. Remember that this will not change the name of the folder used for your installation.
- + Specify the path of your installation. Note: ensure the installation folders are present in the new path before applying this modification.
- + Activate the default installation: at the start of VISOR, the default installation will start automatically after 30 seconds if no action is taken within this time.
- + Change the image of the installation. To do this, click the "Edit" button.

INSTALLATION WITH A SQL SERVER DATABASE:



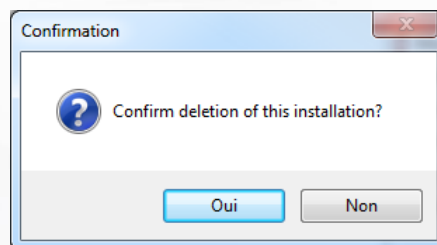
From this window:

- + Specify the name of your installation
- + Specify the path to your SQL Server. You can use the button  to display the list of SQL servers on your network.
- + Activate the default installation: at the start of VISOR, the default installation will start automatically after 30 seconds if no action is taken within this time.
- + Indicate the type of installation from the choices Server station, Server station with Windows Server service, Client station.
- + Enter the name of your database (default is "VISOR")
- + Specify the authentication mode of your SQL Server (Windows authentication - using the user of the Windows session currently opened on the computer - or SQL authentication - using the login "sa" or another and the password defined during the installation of the SQL Server instance). If you do not have a Windows domain and / or the user of the currently opened Windows session is not allowed on the database, use SQL Authentication.
- + Specify to use VISORWeb if it is installed on your computer. In this case, using the Windows service is mandatory.
- + Change the image of the installation. To do this, click the "Edit" button.

Click "OK" to confirm the changes. If the Windows service is used, a message will appear asking you to restart it. Then click on "Yes" when prompted.

REMOVING AN EXISTING INSTALLATION

From the installations management window, select the installation to remove and click "Delete".



Confirm the deletion by clicking "Yes".

When a SQL Server database is used, you will be prompted to confirm the deletion of the database on your SQL instance. Click "Yes" if you are sure to delete the database.

If the Windows service is used, a message will appear asking you to restart it. Then click on "Yes" when prompted.

Caution: Deleting will automatically destroy all data on your computer according to the selected installation. Reading the parameters from our units is impossible, so this operation is irreversible. Make sure you have a backup before performing this operation.

SAVING AN EXISTING INSTALLATION

From the installations management window, select the installation to save and click "Save".

Choose the location of the backup file and click "Save".

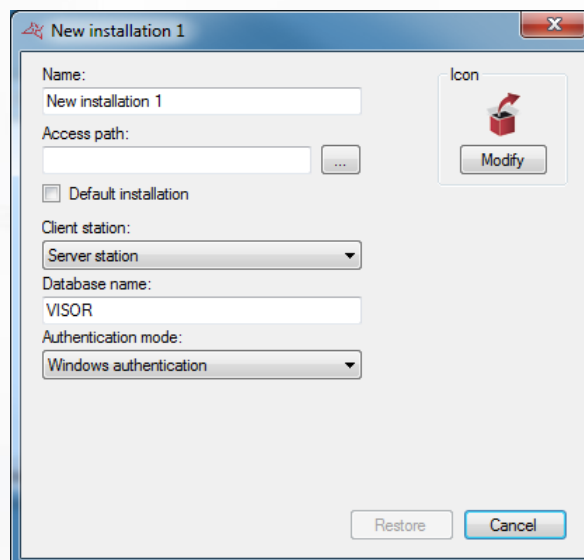
Enter the password of the administrator of your installation and click "OK".

Make sure you have write access rights to the selected location.

RESTORING AN INSTALLATION

From the installations management window, click "Restore."
Select the file to be restored in ZIP format and click "Open".

RESTORING AN INSTALLATION USING A SQL DATABASE:



From this window:

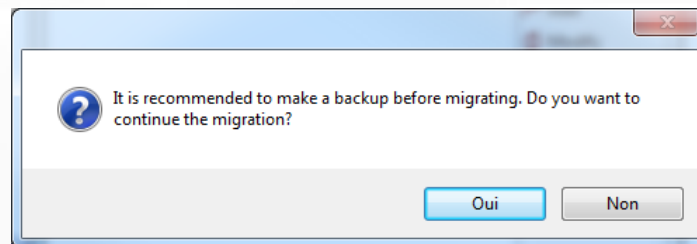
- + Specify the name of your installation
- + Specify the path to your SQL Server. You can use the button [...] to display the list of SQL servers on your network.
- + Activate the default installation: at the start of VISOR, the default installation will start automatically after 30 seconds if no action is taken within this time.
- + Indicate the type of installation from the choices Server station, Server station with Windows Server service, Client station.
- + Enter the name of your database (default is "VISOR")
- + Specify the authentication mode of your SQL Server (Windows authentication - using the user of the Windows session currently opened on the computer - or SQL authentication - using the login "sa" or another and the password defined during the installation of the SQL Server instance). If you do not have a Windows domain and / or the user of the currently opened Windows session is not allowed on the database, use SQL Authentication.

- + Specify to use VISORWeb if it is installed on your computer. In this case, using the Windows service is mandatory.
- + Change the image of the installation. To do this, click the "Edit" button.

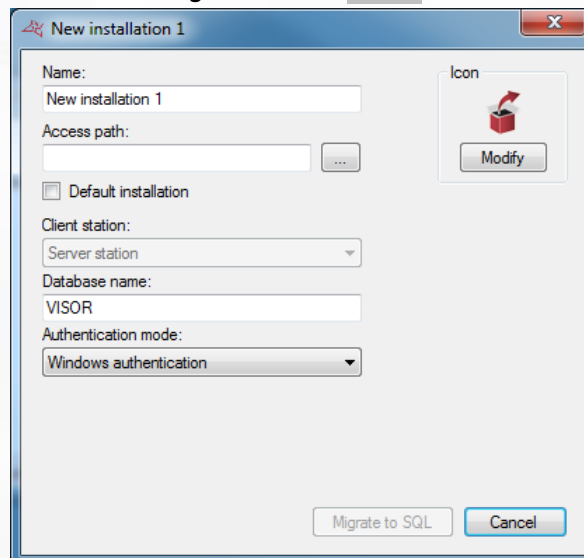
MIGRATING AN EXISTING ACCESS DATABASE INSTALLATION TO A SQL SERVER DATABASE

From the installations management window, select the Access database installation to migrate to SQL Server, then click "Migrate to SQL".

The following message appears:



If you have not save your installation, click "No". Perform your backup (see previous section) and then try again. Otherwise, to start the migration, click "Yes".



From this window:

- + Specify the name of your installation
- + Specify the path to your SQL Server. You can use the button [...] to display the list of SQL servers on your network.
- + Activate the default installation: at the start of VISOR, the default installation will start automatically after 30 seconds if no action is taken within this time.
- + Indicate the type of installation from the choices Server station, Server station with Windows Server service, Client station.
- + Enter the name of your database (default is "VISOR")
- + Specify the authentication mode of your SQL Server (Windows authentication - using the user of the Windows session currently opened on the computer - or SQL authentication -

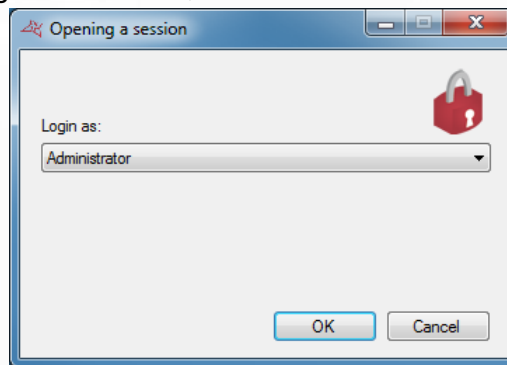
using the login "sa" or another and the password defined during the installation of the SQL Server instance). If you do not have a Windows domain and / or the user of the currently opened Windows session is not allowed on the database, use SQL Authentication.

- + Specify to use VISORWeb if it is installed on your computer. In this case, using the Windows service is mandatory.
- + Change the image of the installation. To do this, click the "Edit" button.

Click "Migrate to SQL" to start the migration.

OPENING AN EXISTING INSTALLATION

From the installations management window, select the installation to open, then click "Open".



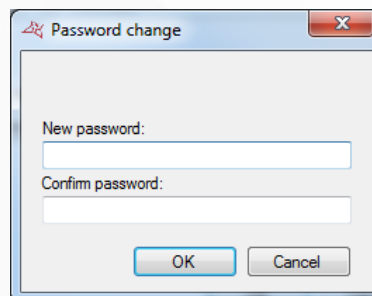
From this window, select the manager.

If the selected manager has protected his session with a password, enter it.

Click "OK".

FIRST OPENING OF AN INSTALLATION:

If you open an installation for the first time, VISOR will ask you to enter the password for the Administrator manager as follows:



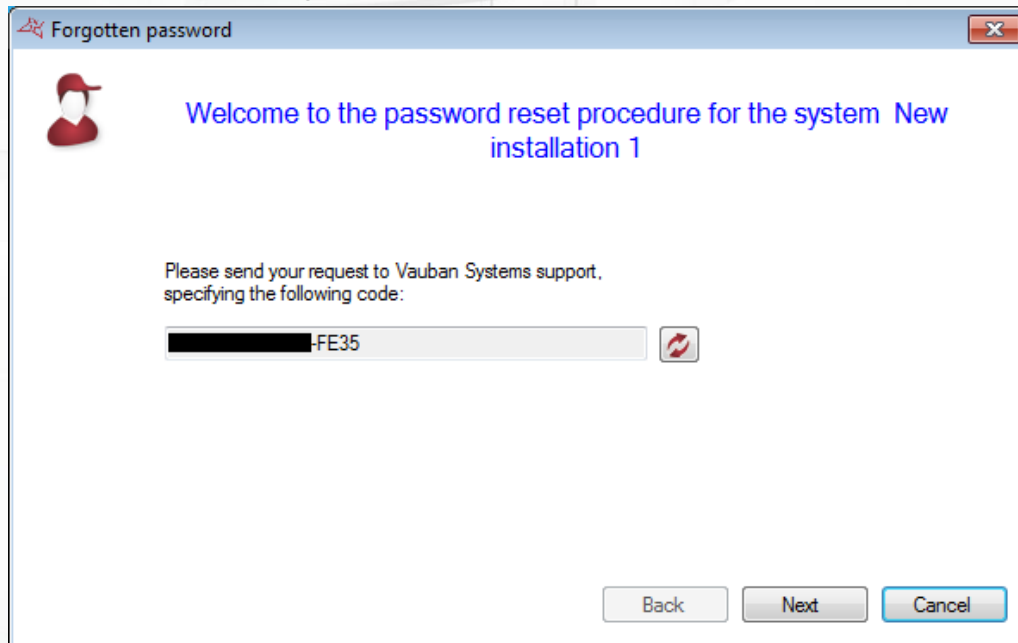
If you do not want to protect the Administrator with a password, click "OK". Otherwise, enter the password, confirm it and click "OK".

We recommend to enter a password to the Administrator Manager because this manager has unrestricted access to the software functions.

FORGOTTEN PASSWORD

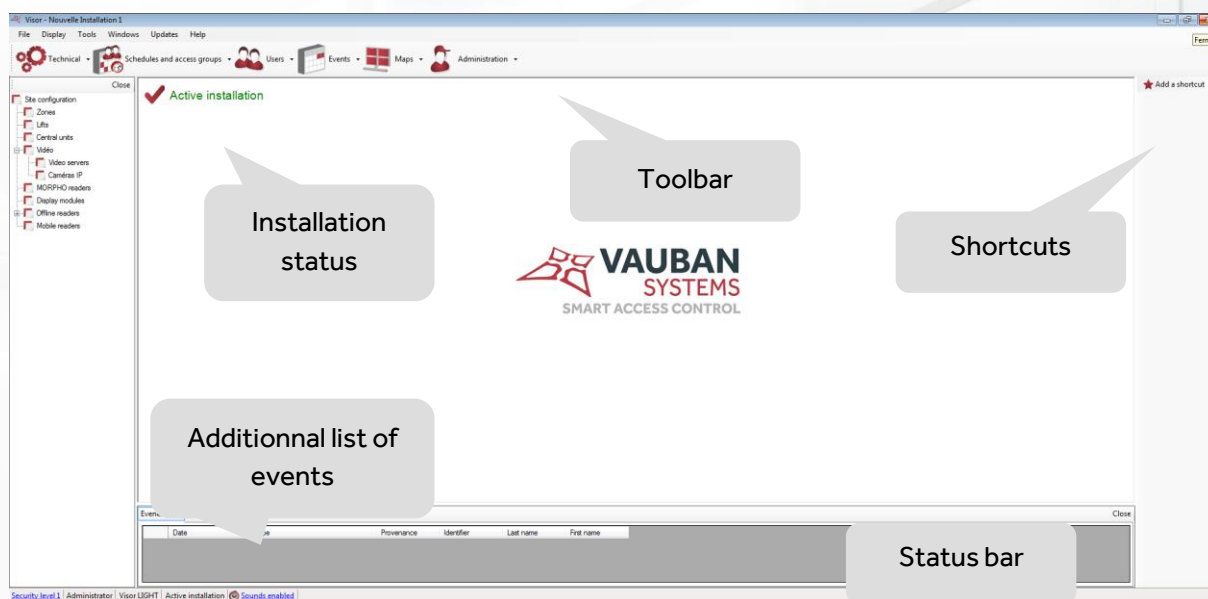
This procedure resets the administrator password.

From the Systems Management window, select the system for which you forgot the administrator password and click on "Help/Forgotten Password"



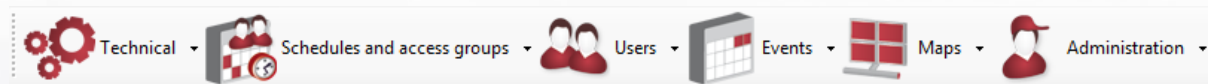
At this point, you must contact Vauban Systems Support and give them the reset code. Then follow the instructions.

MANAGING THE MENUS



This window provides several menus for using the software. Throughout this technical guide, you will receive all the information needed for getting started with the VISOR software.

THE TOOLBAR



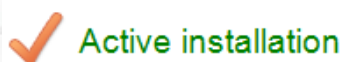
This toolbar represents all the functions of the software:

- + **Technical:** display all system configuration and status of each security element (units, extension modules, readers, ...)
- + **Schedules and access groups:** management of user's access rights, users access schedules but also free access (open maintained doors), holidays and special days (not holidays but different access times from usual hours)
- + **Users:** management of users accessing the facility and their identifiers (cards, transmitters, codes...), listing tool (creating custom lists of users based on many customizable filter lists), calculating the time of attendance, and display of user's current location.
- + **Events:** Display of events occurring in the facility and history tool (creating custom events list depending on many customizable filter lists)
- + **Overview:** Creating an interactive map of the facility to view and control the status of various elements graphically
- + **Administration:** Management of the Managers allowed to access VISOR software and visualization of their logs

To show or hide the toolbar, click the "Display" menu and then "Toolbar".

Tip: To hide this bar each time you start VISOR, go to the "Tools" menu, "Preferences", "Configuration" tab and uncheck the "Display toolbar on startup".

THE INSTALLATION STATUS



This status allows you to easily know the global status of the equipment of your installation. The statuses can be:

- + **Nominal Installation:** No fault of the equipment. The system is working properly.
- + **Check dongle:** No fault of the equipment. However, no dongle is detected which means that no updates and no collection of events can be done. This error can occur if you use more than 2 readers on your system and no unit is equipped with a dongle.
- + **Check status of equipment:** At least one device is not connected properly. In this case, open the equipment status from the "Technical" menu, "State of equipment" and check the status of all equipment. At least one of them must be connection failure or disconnected.
- + **Main station disconnected:** In case of a client / server installation, ensure that VISOR or VISOR service is launched on the server. If this status is displayed, no unit update or event collection is possible.
- + **Database access problem:** the database is no longer available. Restart VISOR and make sure the database is functional.
- + **Check status of equipment (no dongle detected):** At least one device is not connected properly. In this case, open the equipment status from the "Technical" menu, "Equipment status" and check the status of all equipment. At least one of them must be in connection failure or disconnected. Furthermore no dongle is detected. Very often, this status appears when the unit with the dongle is disconnected. Check its status.
- + **Time attendance exceeded:** a maximum attendance period has been defined for a specific zone and a user has exceeded that time allocation.

THE ADDITIONAL LIST OF EVENTS

Evenements	Présence						Close
	Date	Type	Provenance	Identfier	Last name	First name	

Two information can be displayed:

- + **Event list**

This list displays all events that occurred on your installation since the start of VISOR. It is always empty on the software startup.

- + **List of exceeded attendance times**


This list displays information pertaining to exceeded attendance times per zone

To close this list, click the "Close" button.

To view or hide this list, click on "Display" and then "Event List".

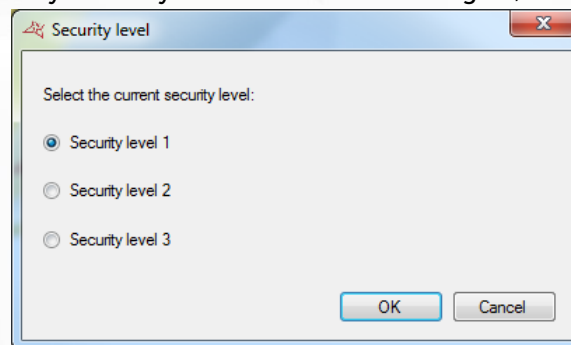
Tip: To hide the list each time you start VISOR, go to the "Tools" menu, "Preferences", "Configuration" tab and uncheck the "Display events list".

THE STATUS BAR

[Security level 1](#) | Administrator | Visor LIGHT | Active installation | No connection with the external server |  [Sounds enabled](#)

From this bar, you can:

- + Check the security level of your installation. To change it, click it and press "OK"



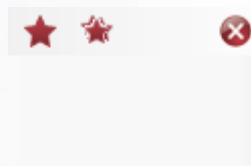
- + Check the name of the current session manager
- + Check the Software License Version (maximum number of readers allowed)
- + Check the status of the equipment in your system (see Installation Status above)
- + Check the connection status to the external server (available if external connections are enabled).
- + Enable or disable the sounds played on each received event.

Tip: To turn off the sounds each time you start VISOR, go to the "Tools" menu, "Preferences", "Configuration" tab and check the "Disable sounds on startup"

To show or hide this bar, click the "Display" menu and then "Status Bar".

THE SHORTCUTS AND THE REMOTE CONTROL

THE SHORTCUTS



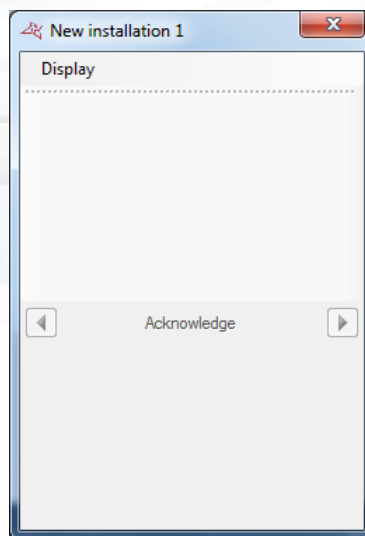
Shortcuts allow you to use a software function with a single click.

To show or hide the shortcuts, click the "Display" menu and then "Shortcuts". To hide the shortcuts, you can also click the "Close" button.

Tip: To hide the shortcuts each time you start VISOR, go to the "Tools" menu, "Preferences", "Configuration" tab and uncheck the "Display shortcuts on startup".

For more information, see "Shortcuts".

THE REMOTE CONTROL



This window allows you to use different shortcuts and see events scrolling.

To display this window, right click on the icon  next to Windows time and click "Display".

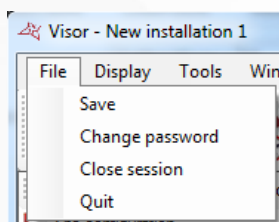
From the "Display" menu, you can choose to view shortcuts and / or events.

You can browse the events by clicking on the right and left arrow and choose to make disappear the event from the list by clicking the "Acknowledge".

To show or hide the icon,  click the "Display" menu and then "Remote Control".

Tip: To hide this icon each time you start VISOR, go to the "Tools" menu, "Preferences", "configuration" tab and uncheck the "Display remote control window on startup".

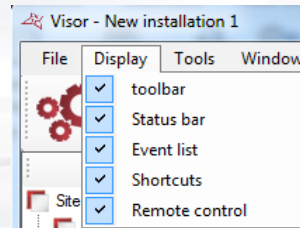
THE FILE MENU



From this menu, you can:

- + Save your installation on your PC in ZIP compressed format. Please note that this operation is not possible in case of using the Windows service. In this case, use the backup menu from the installations management window, or use the automatic backup ("Tools" menu, "Preferences").
- + Change the password of the current session manager.
- + Close the session without leaving the application.
- + Exit the application

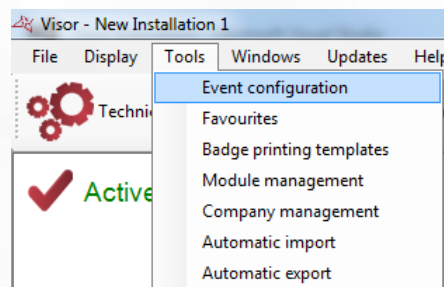
THE DISPLAY MENU



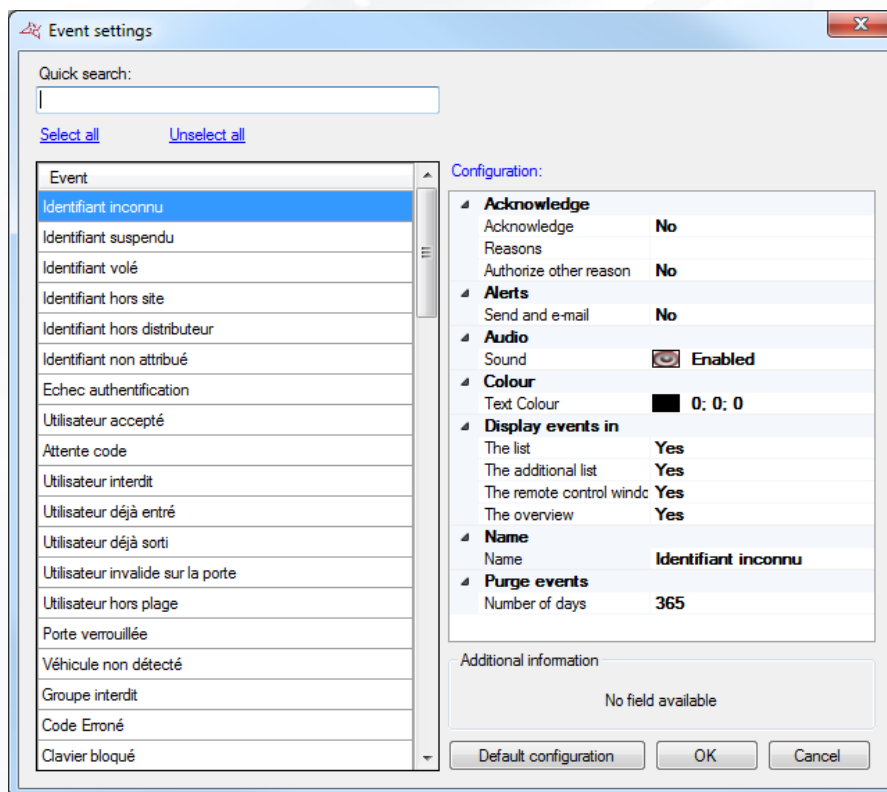
From this menu, you can:

- + Show or hide the toolbar
- + Show or hide the status bar
- + Show or hide the additional list of events (at the bottom of the main window)
- + Show or hide the shortcuts
- + Show or hide the VISOR icon in the Windows toolbar to display the Remote Control window.


THE TOOLS MENU



Event configuration



In this window, you can:

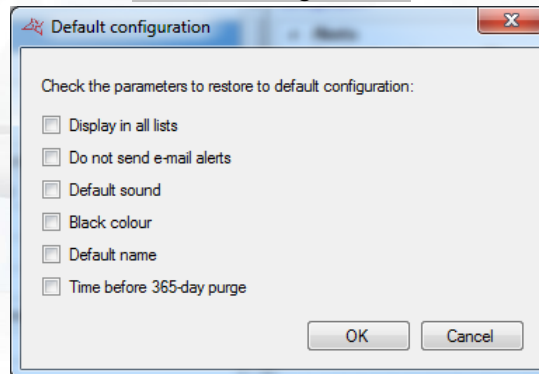
- + Perform a quick search for an event by entering part of the event name.
- + Order the events in alphabetical order by pressing 
- + Select or deselect all events with a **single click**.
- + See and change the configuration for one or more events.
- + Set the events in their default configuration
- + Set an additional information field used for events (additional information about user will be added to the according events). This option is only available if additional information has been created from the "Favourites" menu ("Additional information" tab).

From the configuration window, you can:

- + Choose to show events in:
 - The Event List (Menu Events and See events)
 - The additional list (bottom of the main window)
 - The remote control window
 - The map
- + Choose to send alerts by Email to the authorized managers. **Caution:** to use this feature, you must set the information of the sending email server from the Tools menu, then Preferences Emails tab.
- + Enable, disable or change the sound associated with the event.
- + Change the color of the event text.
- + Change the event's label.
- + Remove the events after a certain number of days (365 by default)
- + Choose to acknowledge the event, enter the different reasons (separated by commas) or let the manager enter his own reason

Back to the default configuration:

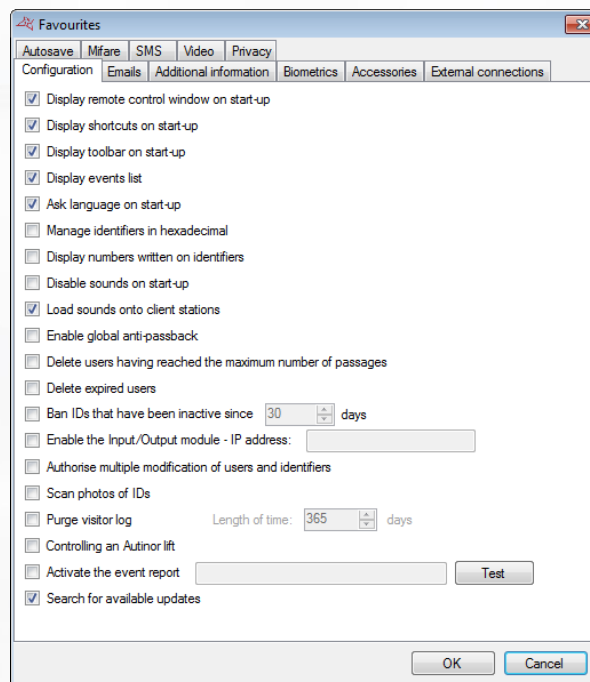
To do this, select the events and click "Default configuration".



Check the items to restore default settings and click "OK".

FAVOURITES

Configuration tab



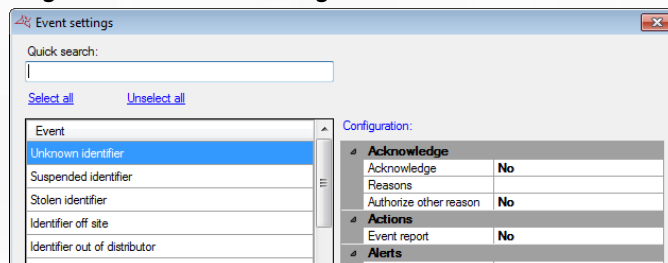
In this tab, you can:

- + Display the remote control window on start-up in the Windows taskbar.
- + Display the shortcuts when the software starts.
- + Display the event list.
- + Ask for the language when the software starts.
- + Manage badge numbers in hexadecimal.
- + Use the number written on the badges, instead of the number read by our central units (useful when the logical number is different to the physical number).
- + Disable the sounds when the software starts.

- + Load the sounds onto the client stations in case of a client/server installation (SQL SERVER database). This function can be useful for reducing the VISOR start-up time on client stations.
- + Enable global anti-passback: this function is useful if the installation comprises several entry or exit readers connected to several IP central units. Caution: to use this function, VISOR must be running continuously on the PC or use the Windows service.
- + Delete users that have reached their maximum number of passages. The number of passages or times that badges can be used is defined in the user's record in the **Options** tab. The passage count setting is configured in the reader via the Configuration tab. Caution: users will only be deleted every midnight. If you use this function, ensure that VISOR is running continuously on the P, because the operation is only performed twice a day (at noon and midnight).
- + Delete expired users. The user's validity period is configured in the user's record in the **Authorisation** Tab. Caution: users will only be deleted every midnight. If you use this function, ensure that VISOR is running continuously on the PC or use the Windows service because the operation is only performed twice a day (at noon and midnight).
- + Ban inactive IDs
- + Enable the I/O module, where eight inputs for a IP-12 central unit can be used to control a VISOR shortcut according to the input status.
- + Allow multiple users and identifiers to be deleted. As such, managers can delete several users and identifiers in just a **few clicks**.
- + Scan photos of IDs. Requires an ID reader compatible with ID Photo scan
- + Purge the daybook log: this feature is particularly useful to lighten the database by deleting the oldest events

Make it possible to control an Autinor lift

- + Activate the event report. This feature allows you to call a URL with the information of the event as settings for each event configured since the events were set up.



- + Search for software updates when available. VISOR in this case must have an Internet access.

Emails tab

This tab is used to configure the emails sent by the application.

Configuration Tab

The screenshot shows a software window titled 'Favourites' with a close button in the top right corner. Below the title bar is a series of tabs: 'Autosave', 'Mfare', 'SMS', 'Video', 'Privacy', 'Configuration', 'Emails', 'Additional information', 'Biometrics', 'Accessories', and 'External connections'. The 'Configuration' tab is selected. Within this tab, there are three sub-tabs: 'Accessories', 'Contacts', and 'Delivery options'. The 'Accessories' sub-tab is active. It contains the following elements:

- A text input field labeled 'Sender e-mail:'.
- Two input fields side-by-side: 'SMTP server (outgoing mail):' and 'SMTP server port:'.
- The 'SMTP server port' field has a value of '25' and a small up/down arrow icon.
- A dropdown menu labeled 'Encryption:' with 'None' selected.
- A checkbox labeled 'Authentication' which is currently unchecked.
- A 'Test' button located to the right of the 'Authentication' checkbox.

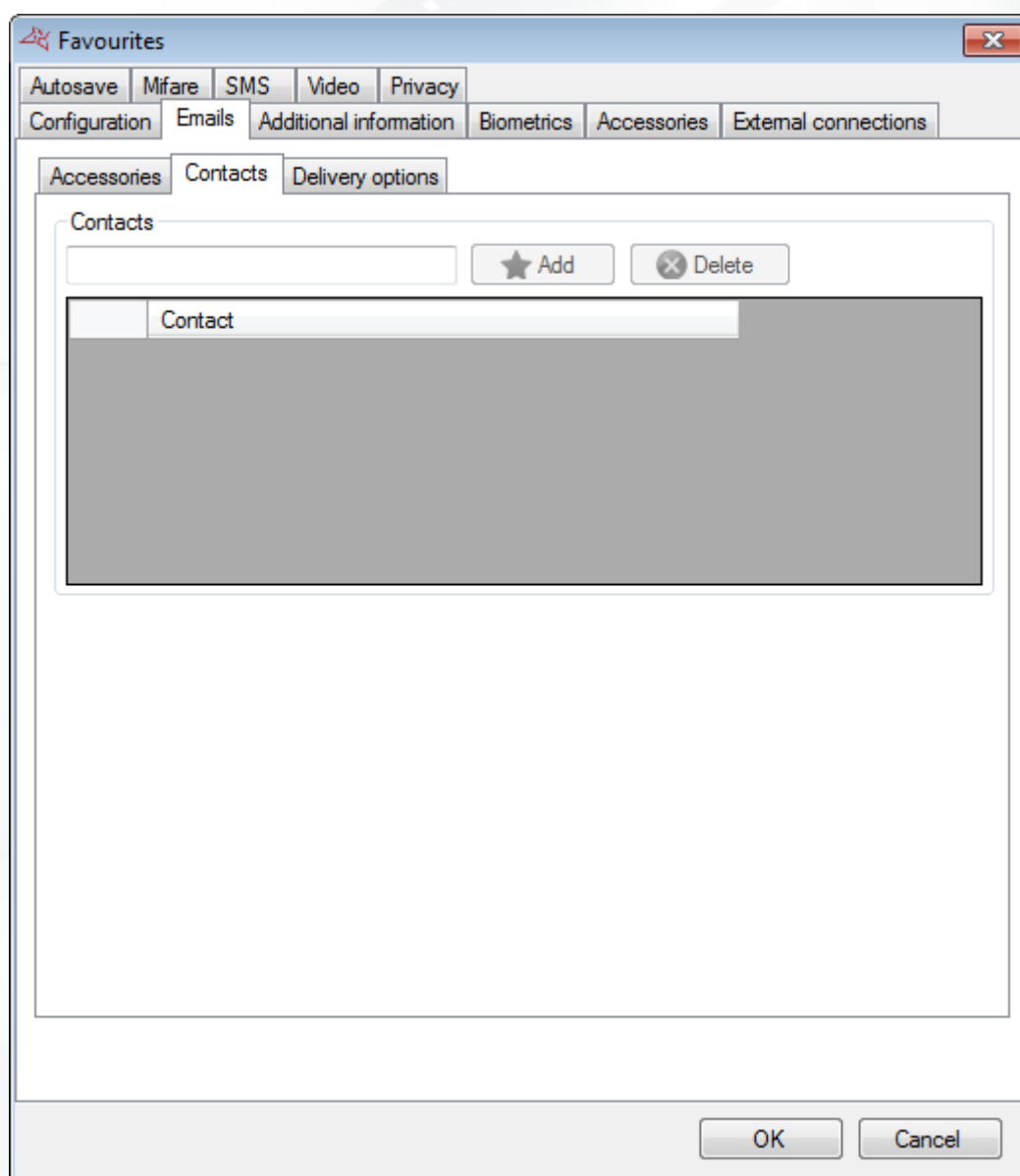
At the bottom of the window are 'OK' and 'Cancel' buttons.

In this window, you can:

- + Define the email sender.
- + Declare the SMTP server (outgoing mail) and the SMTP server port (25 by default).
- + Define the Encryption (None, TLS or SSL) if the SMTP server requires one.
- + Check authentication and then define the login and password if the SMTP server requires authentication.

Click the "Test" button to send a test email. Then enter the contact's email address to send this test.

Contact tab



From this tab, you can:

- + Manage contacts recipients of reports published from the tools Listing and History: To add a contact, enter his email address and click "Add". To delete a contact, select him in the list and click "Delete".

Delivery options Tab

Favourites

Autosave Mifare SMS Video Privacy
Configuration Emails Additional information Biometrics Accessories External connections

Accessories Contacts **Delivery options**

When users are created with the wizard

☒ Send and e-mail

Message:

When a user is accepted

☒ Send and e-mail

Message:

Readers

[All](#) [None](#)

☐ Reader 1

☐ Reader 2

Information to send

[All](#) [None](#)

☐ Reader

☐ Date

☐ Last name

☐ First name

☐ Identifier

☐ Validity dates

OK Cancel

From this tab, you can:

- + Enable the sending of emails when creating a user from the Wizard.
- + Send an email to authorized managers when a user is accepted on one of the selected readers.

The email will include all the information selected for that specific user

You must activate user tracking for an email to be sent. Cf. User management / Options.

Additional information tab

Favourites

Autosave Mifare SMS Video Privacy Configuration Emails **Additional information** Biometrics Accessories External connections

Additional information for users

Text ★ Add ✕ Delete

Name	Type	Choice	Mandatory	Identity window
Telephone	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Email	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

OK Cancel

In this window, you can configure up to 20 additional fields containing user-related information. These fields will be displayed in either the Identity tab or the Additional information tab in the users' records.

Note: 2 additional "Phone" and "Mail" fields are present by default. These fields cannot be deleted.

To add a field:

- ✚ Define the name of the field.
- ✚ Select the required type of field from the following choices: Text (simple text input), Multiple selection (selection from several values during input), Check box (equivalent to Yes / No-type information).
- ✚ Click on **Add**.

To change the list of values in Multiple selection fields, click on the **"..."** button as follows:

Additional information for users

Multiple selection ★ Add ✖ Delete

Name	Type	Choice	Mandatory	Identity window
Type	Multiple selec...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following window is displayed. Enter the required value types separated by commas:

Entry

Enter the selections, separated by commas

Technician,Commercial,Director

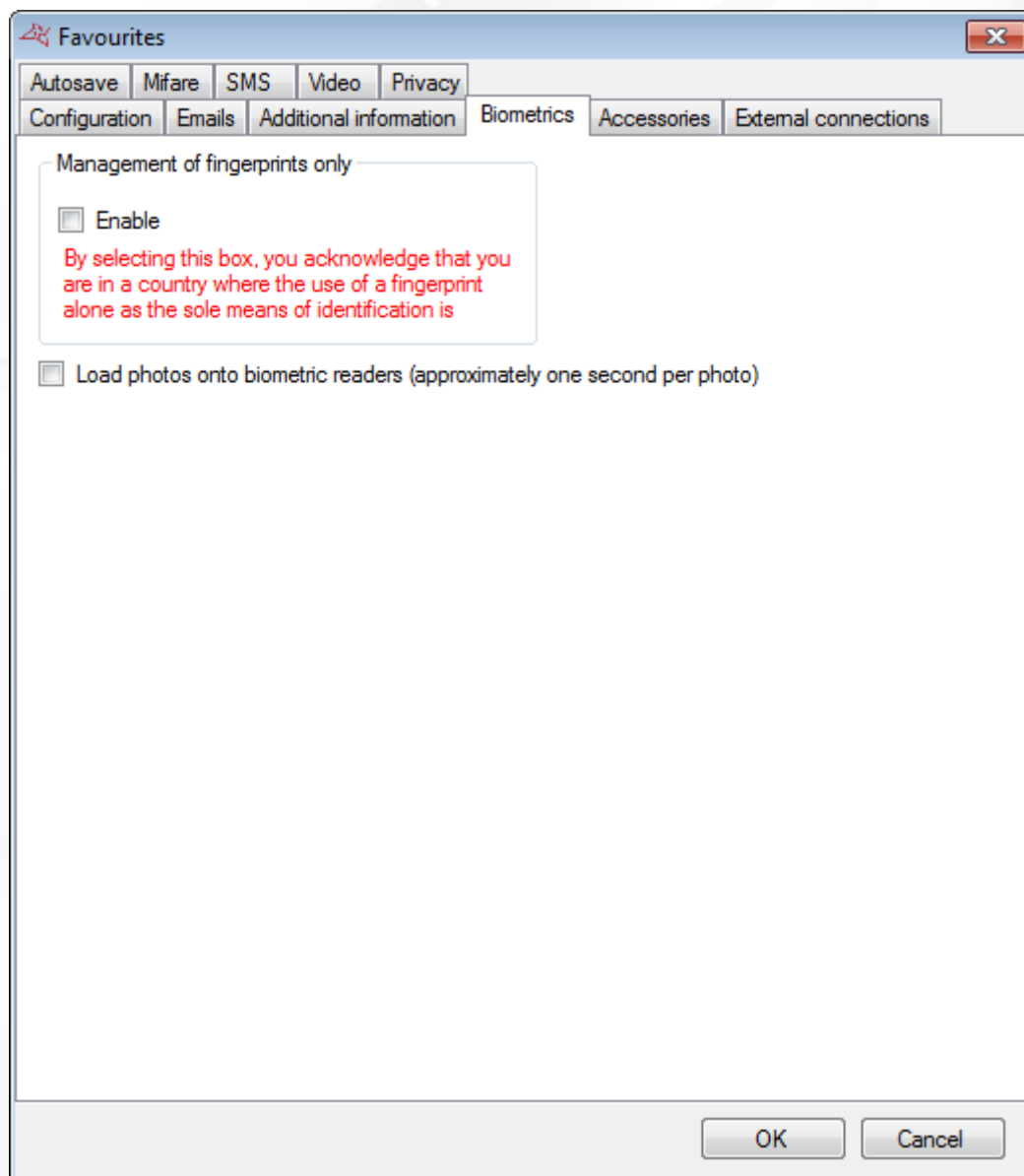
OK Cancel

To make a field mandatory when entering user information, check the "Mandatory" box.

To display a field in the identity tab of a user record, check "Identity window".

To delete a field, select the field and then click on the **"Delete"** button. Caution: the information entered in the field will be lost.

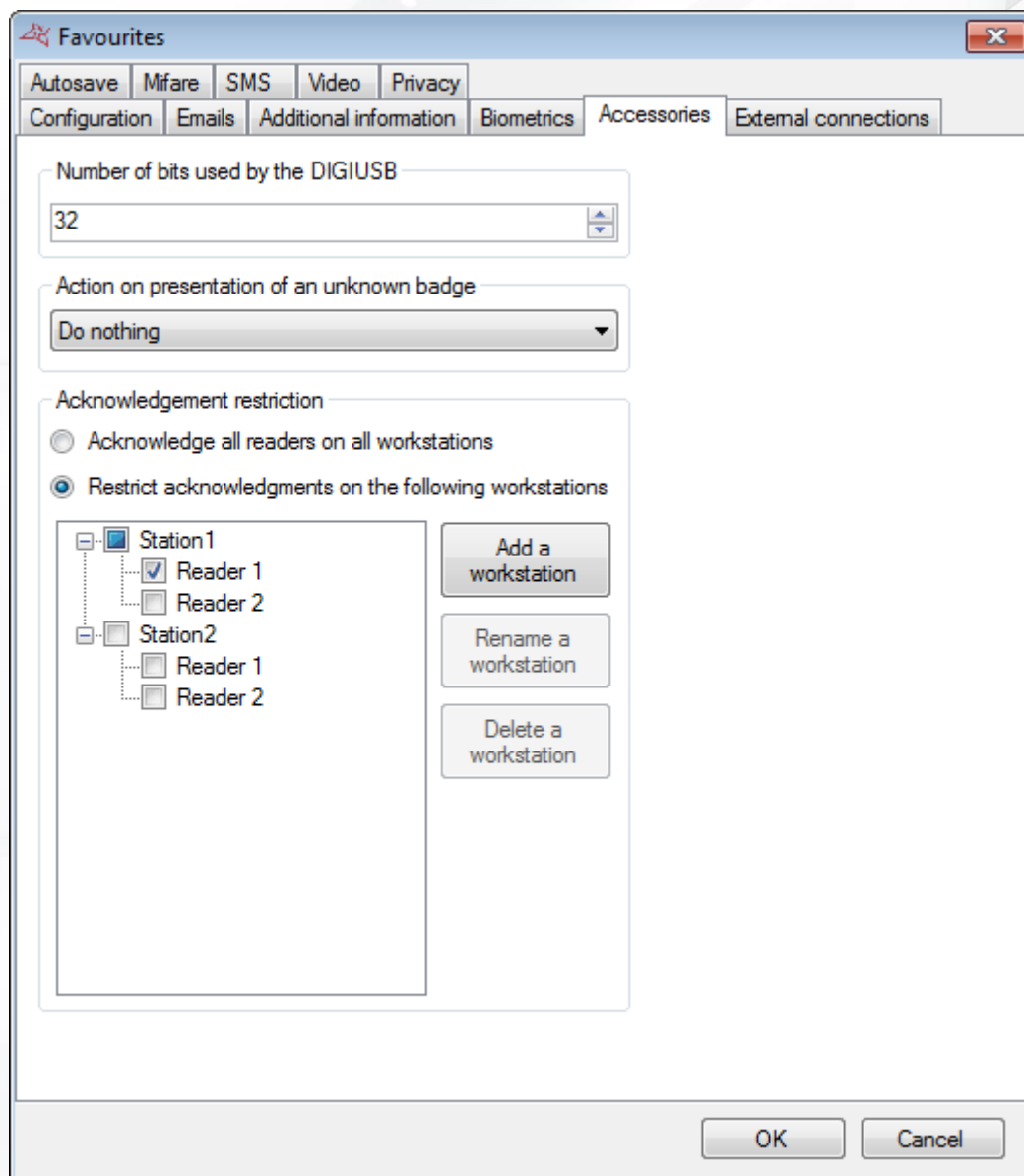
Biometrics tab



In this window, you can:

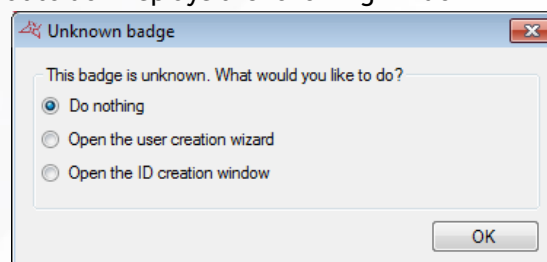
- + Enable the management of fingerprints only. Caution: before enabling this function, ensure that the country in which the system is being used permits the use of biometrics as the sole means of identifying users.
- + Load photos onto biometric readers (approximately one second per photo).

Accessories tab



In this window, you can:

- + Configure the number of bits managed by the DIGIUSB: The Mifare badge enroller / encoder (between 16 and 32 bits).
- + Configure what the system should do upon presentation of an un-recognised credential:
 - o Do nothing
 - o Ask what to do. Displays the following window:



- o Display a message specifying the user is not a known user.

- Open the user creation wizard. Cf. User creation
 - Open the ID creation window. Cf. New credential
 - + Enable the acknowledgment restriction. This feature allows you to filter acknowledgments by workstation. If enabled, each workstation (identified by its name on the network) that should not receive all acknowledgments must be declared.
- In the example above:
- The "Station1" computer will only pull acknowledgments from Reader 1
 - The "Station2" computer will not pull any acknowledgments
 - All other computers will pull all acknowledgments

External connections tab

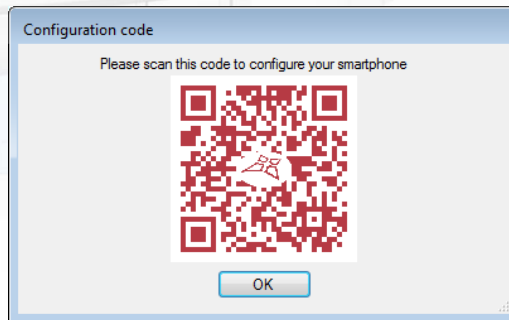
The screenshot shows the 'Favourites' window with the 'External connections' tab selected. The window contains the following elements:

- Navigation tabs:** Autosave, Mifare, SMS, Video, Privacy, Configuration, Emails, Additional information, Biometrics, Accessories, External connections (selected).
- Enable web server:** A checked checkbox. To its right are three buttons: 'SmartPhone application', 'Configure Windows', and 'Set up a smartphone'.
- IP port:** A text box containing '8080' with up/down arrow buttons.
- Authentication:** A dropdown menu showing 'Highly secure'.
- Encryption key:** A text box with a password icon (three dots) to its right.
- External server:** A checked checkbox.
- Identification key:** A text box containing 'N' followed by a blacked-out area, with a password icon to its right.
- Filter authorised IP addresses:** A checked checkbox.
- Add an IP address:** A radio button selected next to a text box.
- Add a range of IP addresses:** A radio button next to 'from' and 'to' text boxes.
- Authorised IP addresses:** A large list box with a '+' icon in the center.
- Buttons:** 'Add' and 'Delete' buttons to the right of the list box.
- Footer:** 'OK' and 'Cancel' buttons.

In this window, you can:

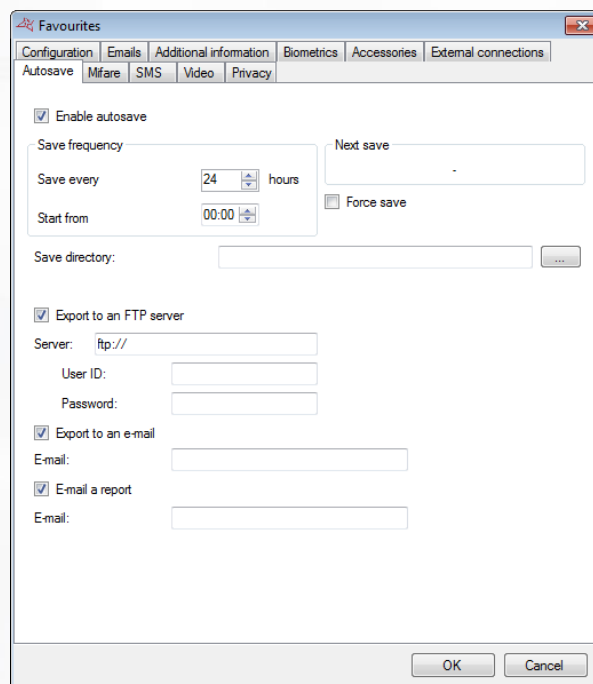
- + Click on "Smartphone configuration" to automatically configure the web server of VISOR for the Smartphone app (iPhone® and Android®)

- + Click on **"Configure Windows"** to configure Windows (this button does not appear in Windows XP).
- + Define the IP port (8080 by default).
- + Select an authentication level: **Very highly secure, Highly secure, Secure** or **Unsecure**.
- + Select an encryption key (Very highly secure mode only), or click on **"..."** to generate one.
- + Click on **"Configure Smartphone"** to display a code to configure a Smartphone directly from the "Visor smartphone" application



- + External server: Connects the application to the external server. The "Identification Key" field uniquely identifies the system on the external server.
- + Filter the IP addresses authorised to sign into VISOR, enter one or more IP addresses or define a range of IP addresses.

Autosave tab

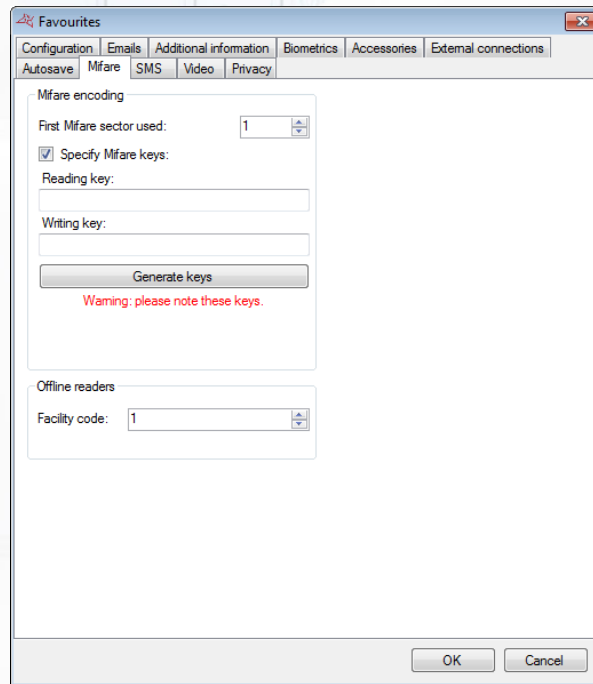


In this window, you can:

- + Enable the autosave feature. To do this, check the box "Enable autosave".
- + Configure the save frequency (expressed in hours) and then specify the start time.
- + View the time of the next save.
- + Force the save, which will be performed as soon as you click on **OK**.
- + Specify the save directory. If you use a SQL SERVER database installed on another PC, you will have to set the path to a readable / writable directory accessible by the SQL instance and by VISOR.

- + Choose to export the save to an FTP server and define the login and password in case of a secure server.
- + Choose to send the save by email. Caution: ensure that you configure the email server settings in the "Emails" tab and ensure sending "big" files is permitted.
- + Choose to send a report on the save process by email. In this case, enter the email address of the recipient of this report. Caution: Be sure to set the sending mail server from "Emails" tab.

Mifare tab



In this tab you can configure the encoding settings for the Mifare badges: you can then configure the index of the first sector that will be used, as well as the encryption keys.

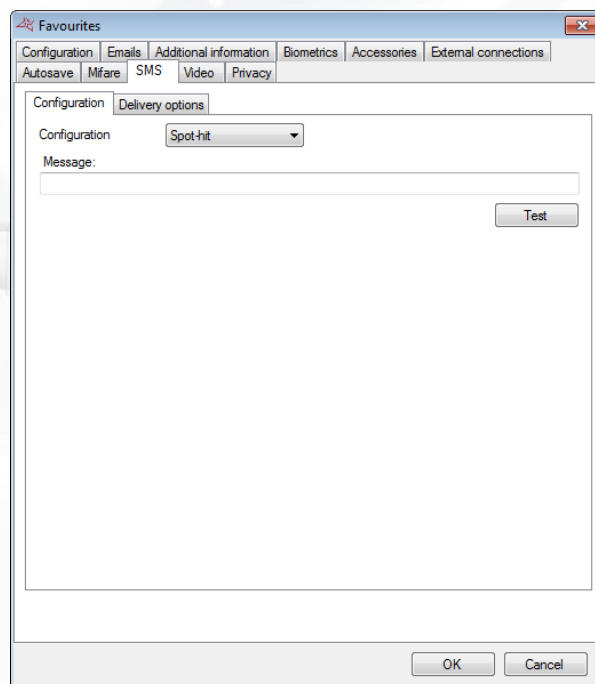
Caution: We recommend you to specify your own Mifare key for more security. In this case, note these keys. If you lose, you will not be able to use the badges already encoded.

SMS Tab

This tab is used to configure the SMS messages sent by the application.

Warning: To send an SMS, an Internet connection is required.

Configuration Tab

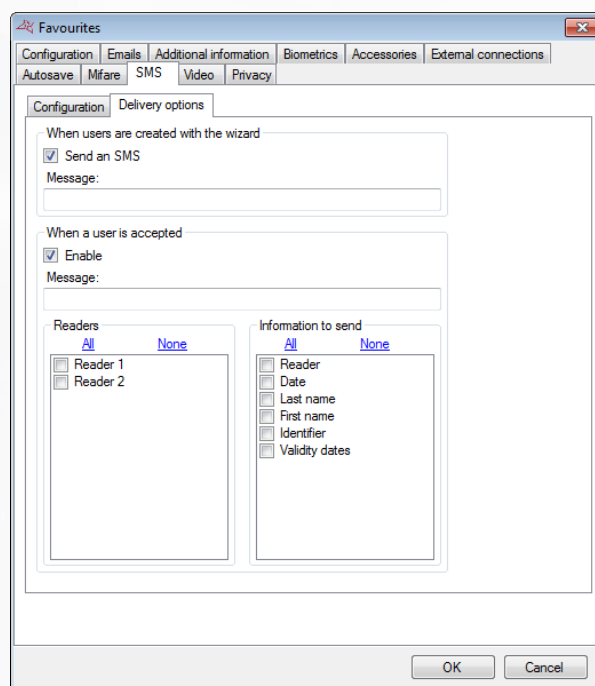


From this tab you can:

- + Configure the type of SMS which is sent.
- + The information linked to the selected configuration type

Click on "Test" to send a test SMS message. Enter the phone number of the contact to whom you want to send the message.

Delivery options Tab



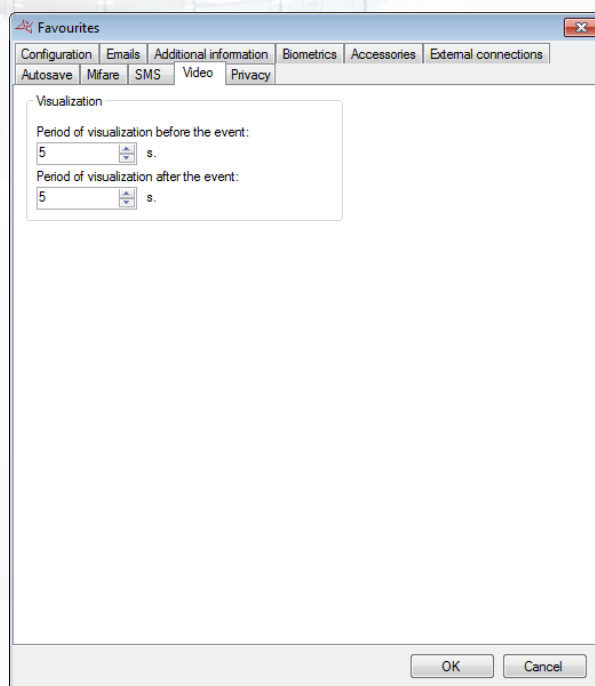
From this tab, you can:

- + Enable the sending of SMS when creating a user from the wizard.
- + Send an SMS message to authorized managers when a user is accepted on one of the selected readers.

The SMS will include all the information selected for that specific user

You must activate user tracking for an SMS message to be sent. Cf. User management / Options.

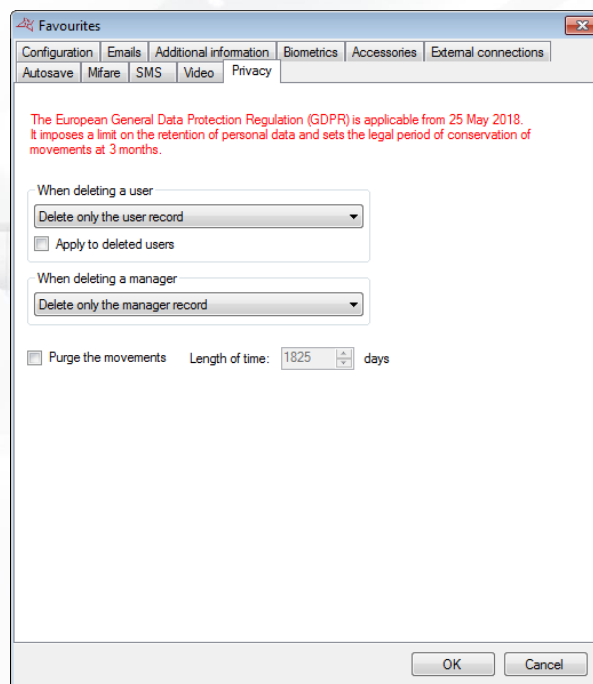
Video tab



From this tab, you can:

- + Select the display duration before and after the event from 0 to 60 seconds.

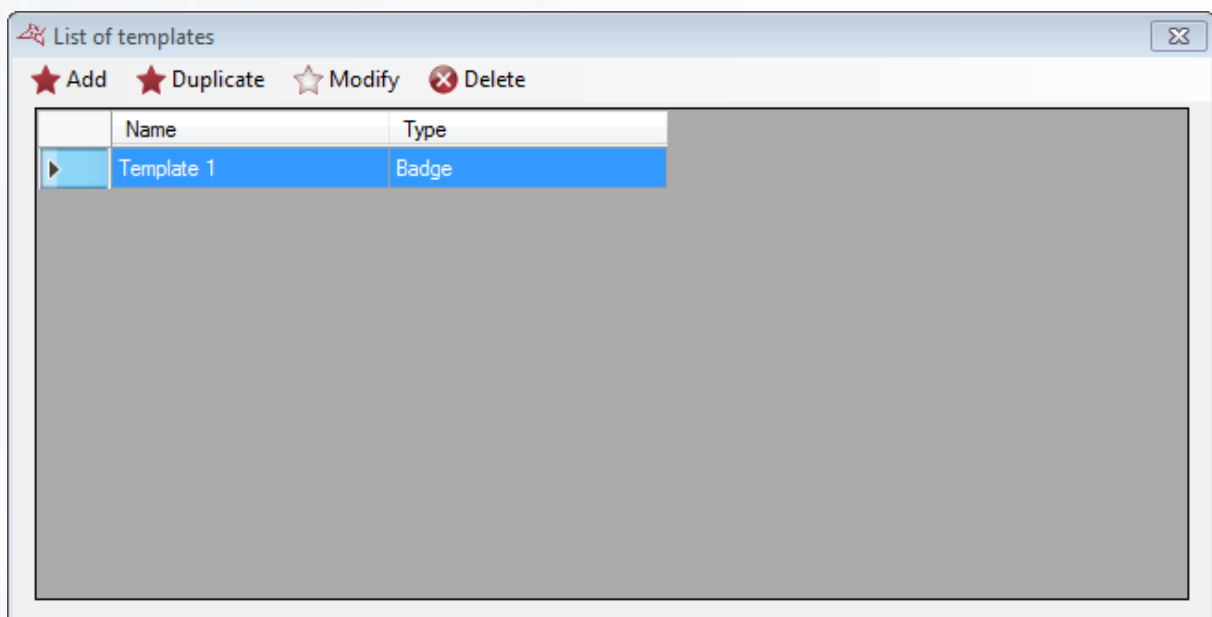
Privacy tab



From this tab, you can adjust the software privacy level:

- + Choose the actions to take when deleting a user.
 - Delete only the user record
 - Anonymise movements
 - Delete movements
- + Choose the actions to take when deleting a manager
 - Delete only the manager record
 - Anonymise the manager's actions
- + Choose the movement purge time. Default is five years.

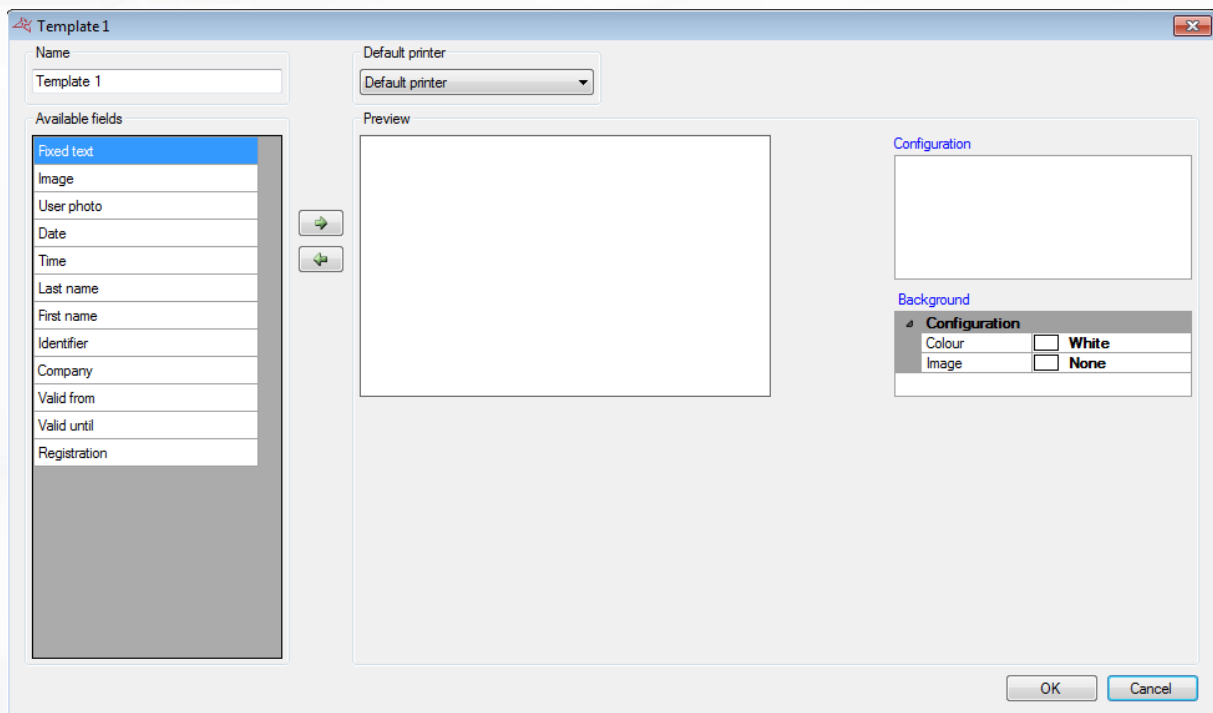
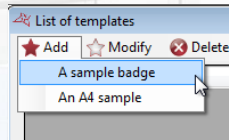
BADGE PRINTING TEMPLATES





From this window, you can:

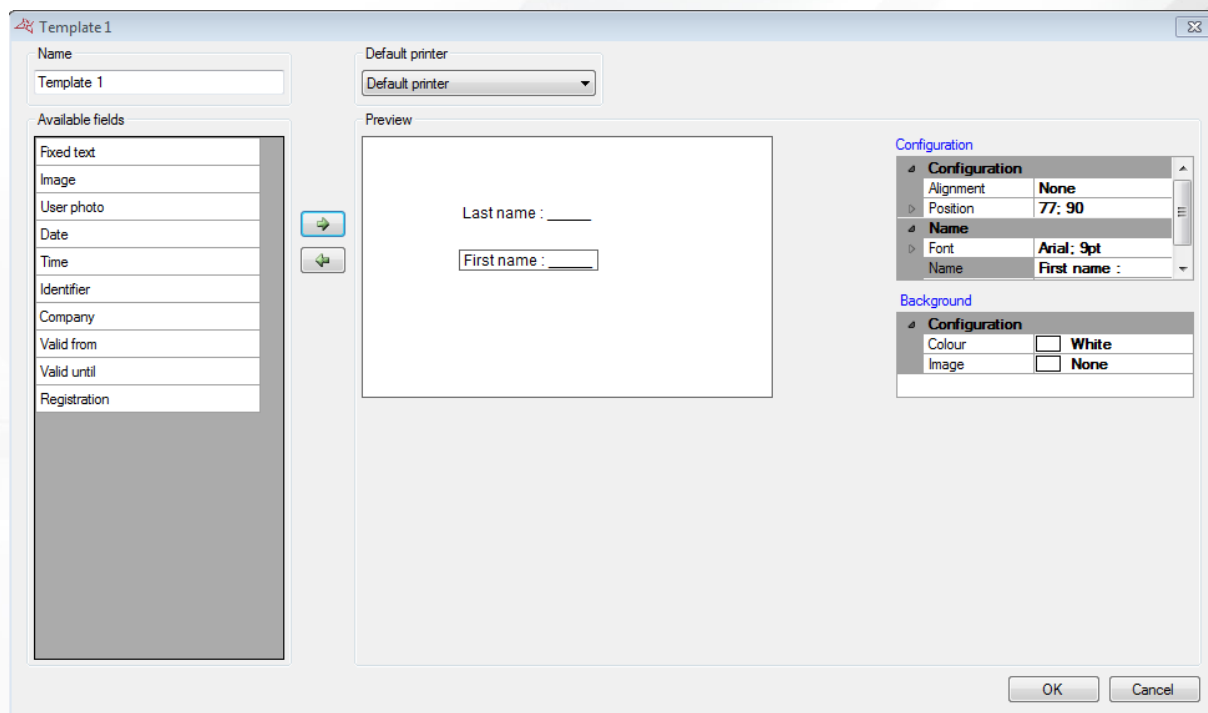
- + Add a new template
- + Duplicate an existing template
- + Edit an existing template
- + Delete an existing template

To add a new template, click on "Add", and select the type of template you want to create.



From this window, you can:

- + Name your printing template.
- + Select a default printer.
- + Configure the background of the template (color and back image)
- + Click on  or  to add or delete a field in the preview.



When a field is selected in the preview, a configuration window is automatically displayed. You can use the **Configuration** menu on the right side of the window.

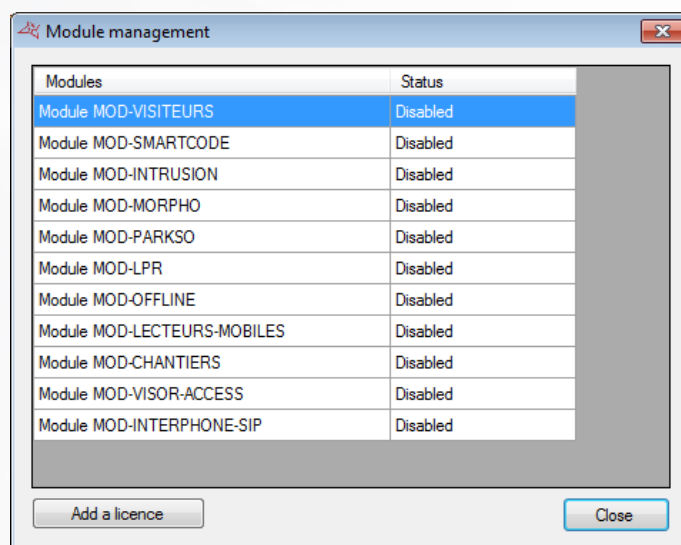
You can move a field on the preview by clicking and moving the mouse. You can also define its position from its pixel configuration.

Fields User Photo, Name, Company Name, and Identifiers can only be added once. Their value will be automatically replaced by the user information when printing a card.

When your template is finished, confirm by clicking on **OK**. You can see the result in the user's record. See "Managing users".

To use your template and print a user card, open the user record then go to the "Printing" tab.

MODULE MANAGEMENT



From this window, you can activate some additional software modules:

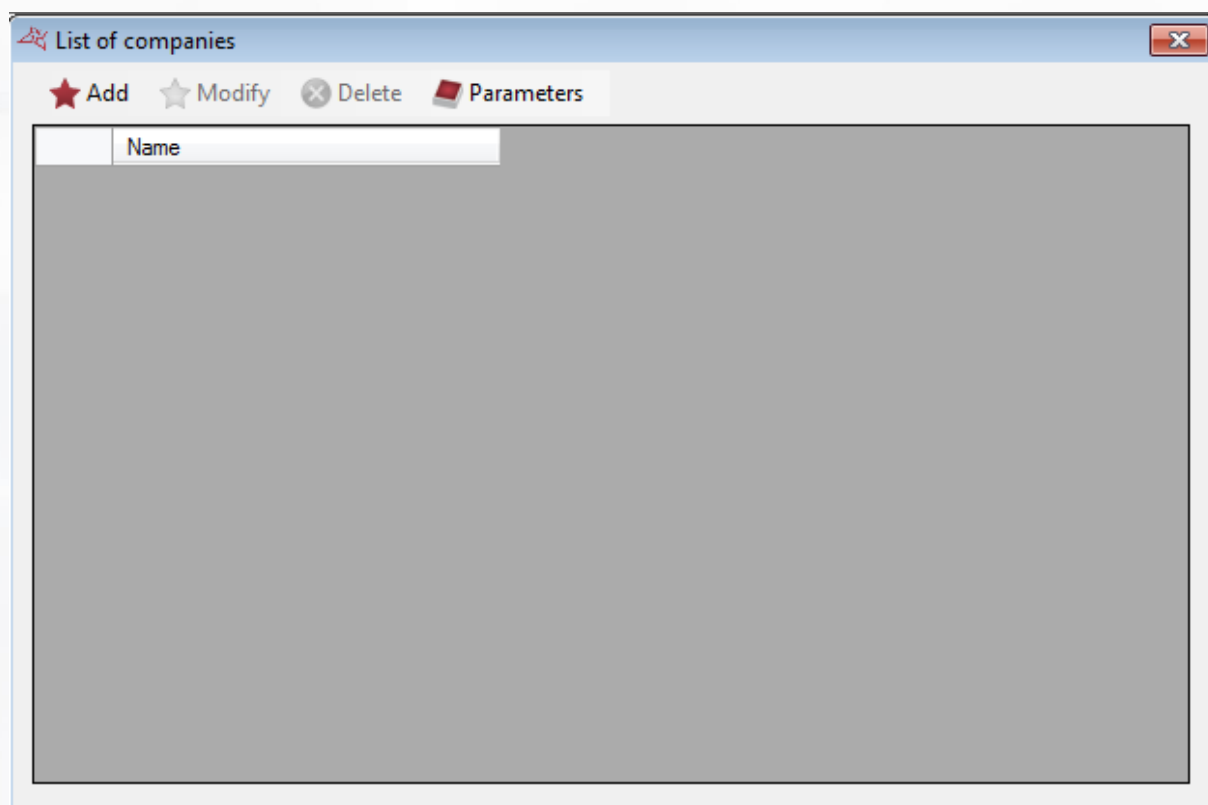
- + **MOD-VISITEURS:** visitor management, compatible with the use of an ID reader.
- + **MOD-SMARTCODE:** printable temporary codes on ticket management.

- + MOD-INTRUSION:** Intrusion unit management GALAXY HoneyWell®, BENTEL® Absoluta® or LIGHTSYS® Risco®. Caution: this module requires the use of SQL SERVER database and the Windows service.
- + MOD-MORPHO:** MORPHO biometric readers (VP Series, Series J, Series 100, Series 500 and Series 500 OMA) management.
- + MOD-PARKSO:** invoice management and manual or automatic cashiers
- + MOD-LPR:** recognition of license plates management. Caution: This module is compatible with the DIGIFORT® LPR software.
- + MOD-OFFLINE:** management of APERIO reader in offline mode.
- + MOD-LECTEURS-MOBLES:** management of smartphones as mobile readers for Visor.
- + MOD-CHANTIERS:** managing user authorisations
- + MOD-VISOR-ACCESS:** managing the opening of a door by scanning a code from a smartphone.
- + MOD-INTERPHONE-SIP:** managing intercom communication using the SIP protocol.

See the manual of each module for more information.

These modules require an additional license that can be activated automatically (24h / 24, 7/7) if your PC has an Internet connection, or manually by contacting our technical support.

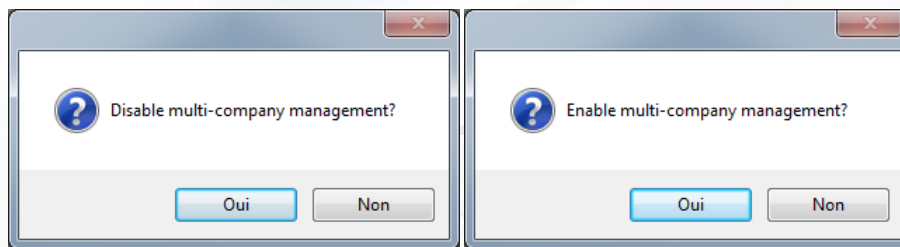
COMPANY MANAGEMENT



This window allows you to manage different companies present on your facility and which have access to the software.

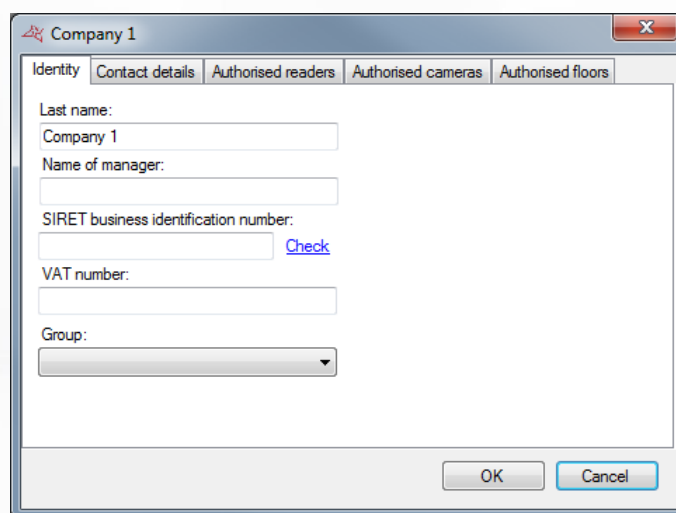
You can assign readers, cameras and floors to each company. This way you can distinguish the access rights and configuration of readers, cameras and floors for each of them.

To enable or disable the multi-company management feature, click on , followed by "Yes" or "No".



To add a new company, click on "Add":

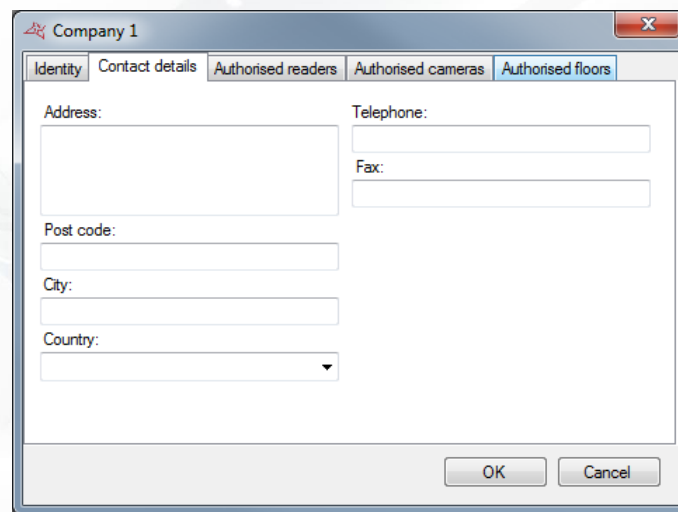
Identity tab

A screenshot of the 'Company 1' dialog box, 'Identity' tab. It contains fields for 'Last name:' (filled with 'Company 1'), 'Name of manager:', 'SIRET business identification number:' (with a 'Check' link), 'VAT number:', and a 'Group:' dropdown menu. At the bottom are 'OK' and 'Cancel' buttons. The tabs at the top are 'Identity', 'Contact details', 'Authorised readers', 'Authorised cameras', and 'Authorised floors'.

From this tab, you can:

- +** Define the name of the company and the manager.
- +** Enter and check the SIRET number (company incorporation number) by clicking on "Check" (the PC must be connected to the Internet).
- +** Enter a VAT number.
- +** Select a default access group.

Contact details tab

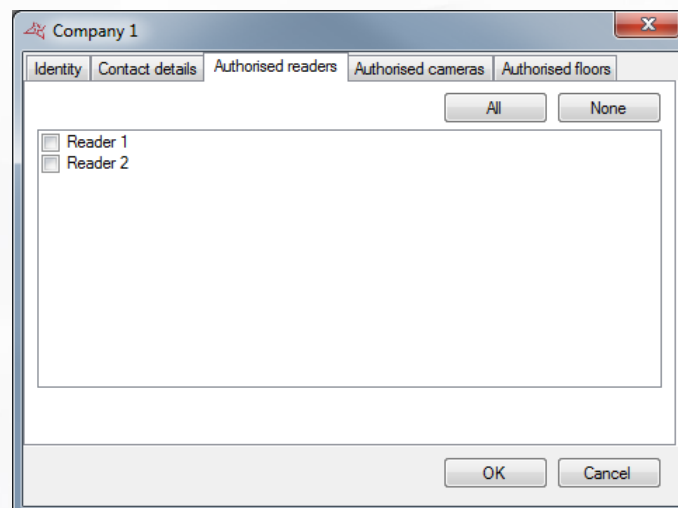


The screenshot shows a dialog box titled 'Company 1' with a close button (X) in the top right corner. It has five tabs: 'Identity', 'Contact details' (which is selected), 'Authorised readers', 'Authorised cameras', and 'Authorised floors'. The 'Contact details' tab contains several input fields: 'Address:' (a large text area), 'Post code:' (a text field), 'City:' (a text field), 'Country:' (a dropdown menu), 'Telephone:' (a text field), and 'Fax:' (a text field). At the bottom right, there are 'OK' and 'Cancel' buttons.

From this tab, you can enter the company's:

- + Address.
- + Postcode.
- + City.
- + Country.
- + Telephone number.
- + Fax number.

Authorised readers tab

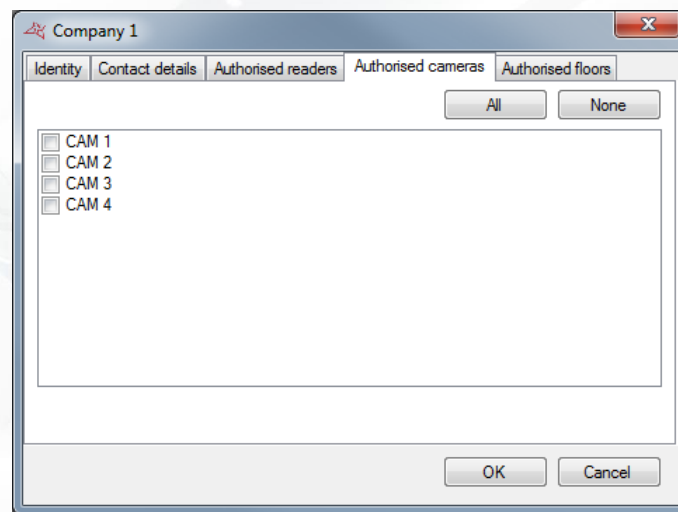


The screenshot shows the same 'Company 1' dialog box, but with the 'Authorised readers' tab selected. This tab contains two checkboxes labeled 'Reader 1' and 'Reader 2'. Above these checkboxes are two buttons: 'All' and 'None'. At the bottom right, there are 'OK' and 'Cancel' buttons.

From this tab, you can select which readers will be used by the company. This means that the company can only display events occurring on these authorized readers, only affect these readers to its users, or change their settings.

The **All** and **None** buttons can be used to quickly select or deselect all readers.

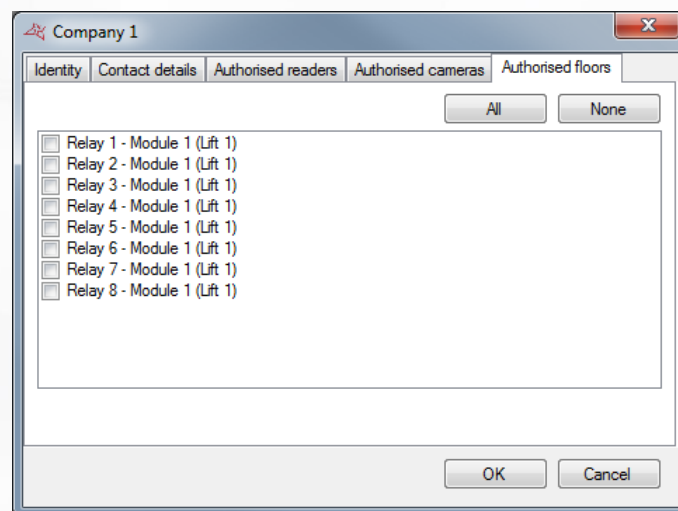
Authorised cameras tab



From this tab, you can select which cameras will be used by the company. This means that the company can only display and/or drive these authorised cameras.

The **All** and **None** buttons can be used to quickly select or deselect all cameras.

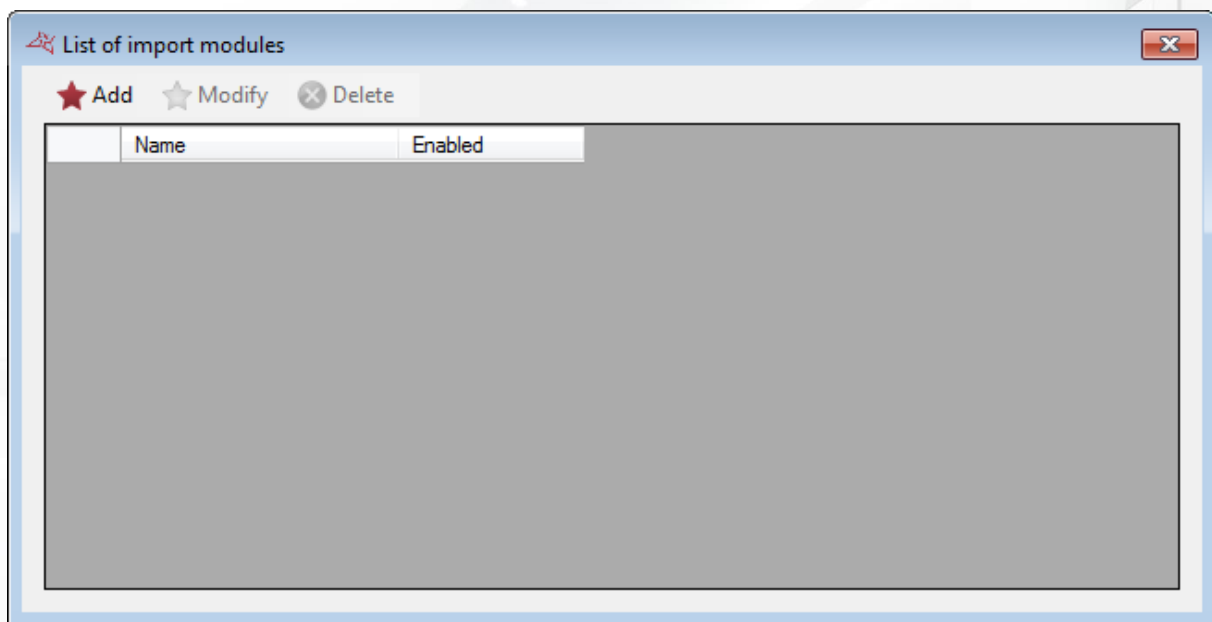
Authorised floors tab



From this tab and in case of lifts, you can select for which floors the company has authorised access.

This means that the company can only affect these floors to its users.

AUTOMATIC IMPORT

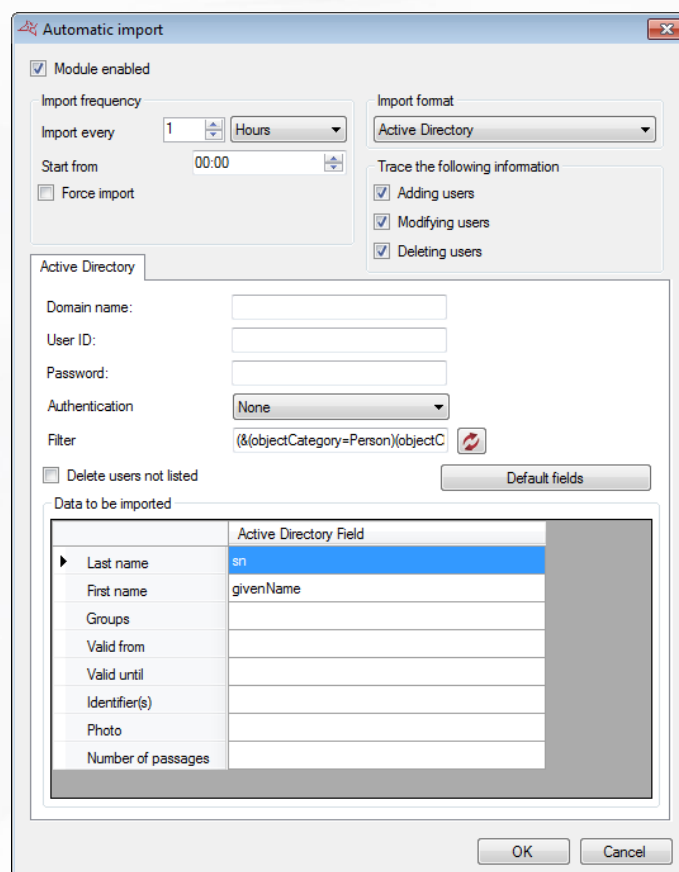


This window manages the various import modules present on your system.
You can add up to five import modules

An import module allows you to import data for one or more users from the Active Directory application or an XML file.

To add a new module, click on "Add"

Configuration



To enable the module, check the "Module enabled" box and then select the:

- + Import frequency. You can specify a value between 1 second and 60 days.
- + Start time for the next import.
- + Which traces will be recorded for import:
 - o Adding users
 - o Modifying users
 - o Deleting users
- + Import format.

The **Force import** option is used to immediately import the data after clicking on **OK**.

Active Directory

Automatic import

☒ Module enabled

Import frequency

Import every: 1 Hours

Start from: 00:00

☐ Force import

Import format: Active Directory

Trace the following information

☒ Adding users

☒ Modifying users

☒ Deleting users

Active Directory

Domain name:

User ID:

Password:

Authentication: None

Filter: (&(objectCategory=Person)(objectC

☐ Delete users not listed

Default fields

Data to be imported

	Active Directory Field
Last name	sn
First name	givenName
Groups	
Valid from	
Valid until	
Identifier(s)	
Photo	
Number of passages	

OK Cancel

With the **Active Directory** import format, specify the:

- + Domain name.
- + User ID and Password of a user with enough access rights to read your domain Active Directory.
- + Authentication type necessary for connection
- + User search filter. Button allow reset filter.

By checking the "Delete users not listed" box, any users listed in VISOR but not listed in the ACTIVE DIRECTORY will automatically be deleted during the import.

The following fields may be imported:

- + Last name: the user's last name.

- + First name: the user's first name.
- + Group: the user's access group.
- + Valid from: the start date of the user's validity.
- + Valid until: the end date of the user's validity.
- + Credentials: user's card number.
- + Photo: a photo of the user (JPEG format).
- + Number of accesses: number of remaining accesses available for the user.
- + Additional fields: you can add additional data fields (such as reservation number and location). These fields must be created in the software's Preferences.

XML

With the XML import format, specify the location of the XML file from the following choices:

- + A physical path pointing to a data directory.
- + A HTTP or HTTPS path (generally used by online reservation sites).
- + An FTP or FTPS path (you must then specify a user ID and password if necessary).

In case of a physical or FTP path, check the "Delete file after importing" box if you want VISOR to automatically delete the file after importing.

In the "Data to be imported" window, enter the different XML tags in the corresponding fields.

The following fields may be imported:

- + Last name: the user's last name.
- + First name: the user's first name.
- + Group: the user's access group.
- + Valid from: the start date of the user's validity.
- + Valid until: the end date of the user's validity.
- + Credentials: user's card number
- + Photo: a photo of the user (JPEG format).
- + Action: action to be performed according to the value of the field (1: modify, 2: add, 3: delete). If this field is left empty, users will always be added.
- + Additional fields: you can add additional data fields (such as reservation number and location). These fields must be created in the software's Preferences.
- + External key: used to synchronize data between Visor and an external software.
- + Number of accesses: number of remaining accesses available for the user.

XML file sample:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<RESERVATIONS>
  <RESERVATION>
    <GROUPE>location1</GROUPE>
    <NOM>PIERRE</NOM>
    <PRENOM>STEVEN</PRENOM>
    <ARRIVEE>30/07/2013 16:00</ARRIVEE>
    <DEPART>31/07/2013 11:00</DEPART>
    <COD>912491</COD>
  </RESERVATION>
  <RESERVATION>
    <GROUPE>location2</GROUPE>
    <NOM>OLIVIER</NOM>
    <PRENOM>HENRY</PRENOM>
    <ARRIVEE>10/08/2013 17:00</ARRIVEE>
    <DEPART>10/08/2013 15:00</DEPART>
    <COD>776085</COD>
  </RESERVATION>
</RESERVATIONS>
```

CSV

There are 3 possible CSV import types:

- + Files using commas as separators
- + Files using semicolons as separators
- + Files using tabs as separators

Automatic import

☒ Module enabled

Import frequency
 Import every: 1 Hours
 Start from: 00:00
☐ Force import

Import format
 CSV (separator: commas)

Trace the following information
☒ Adding users
☒ Modifying users
☒ Deleting users

CSV

Data location
☒ Path:
☐ HTTP:
☐ FTP:
 User ID:
 Password:
☐ Secure connection
☐ Delete the file after it is imported

Data to be imported

	Associated column
Last name	Column 1
First name	Undefined
Groups	Undefined
Valid from	Undefined
Valid until	Undefined
Identifier(s)	Undefined

OK Cancel

With the CSV import format, specify the location of the XML file from the following choices:

- + A physical path pointing to a data directory.
- + A HTTP or HTTPS path (generally used by online reservation sites).
- + An FTP or FTPS path (you must then specify a user ID and password if necessary).

In case of a physical or FTP path, check the "Delete file after importing" box if you want VISOR to automatically delete the file after importing.

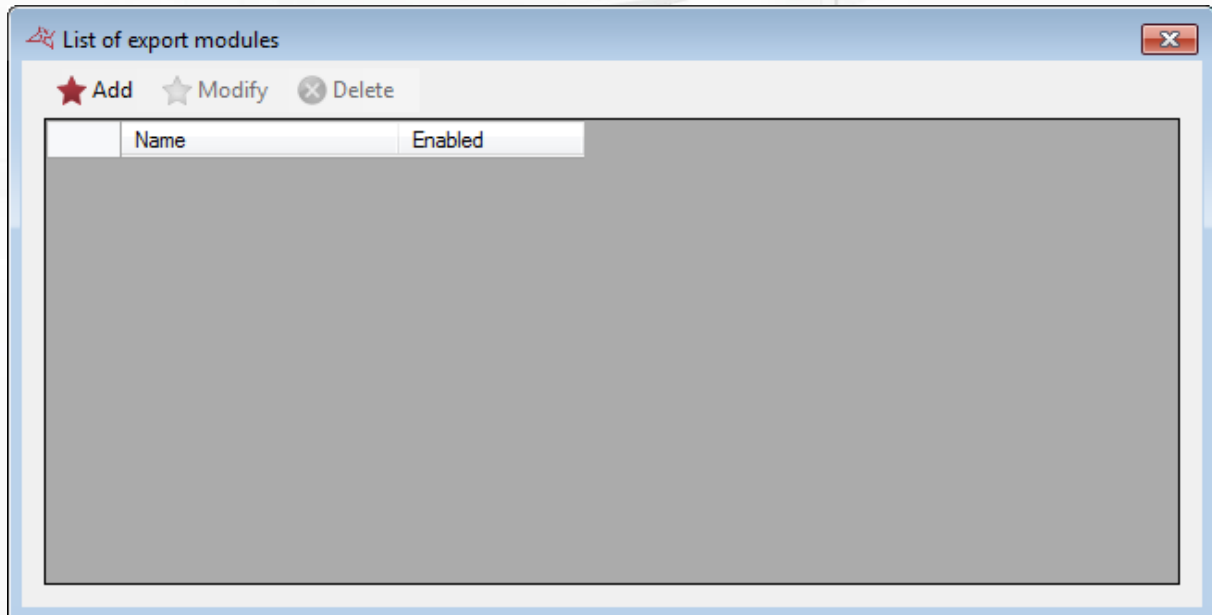
In the Information import window, enter the column numbers in the corresponding fields.

The following fields may be imported:

- + Last name: the user's last name.
- + First name: the user's first name.
- + Group: the user's access group.
- + Valid from: the start date of the user's validity.
- + Valid until: the end date of the user's validity.
- + Credentials: user's card number
- + Photo: a photo of the user (JPEG format).
- + Action: action to be performed according to the value of the field (1: modify, 2: add, 3: delete). If this field is left empty, users will always be added.
- + Additional fields: you can add additional data fields (such as reservation number and location). These fields must be created in the software's Preferences.
- + External key: used to synchronize data between Visor and an external software.
- + Number of accesses: number of remaining accesses available for the user.

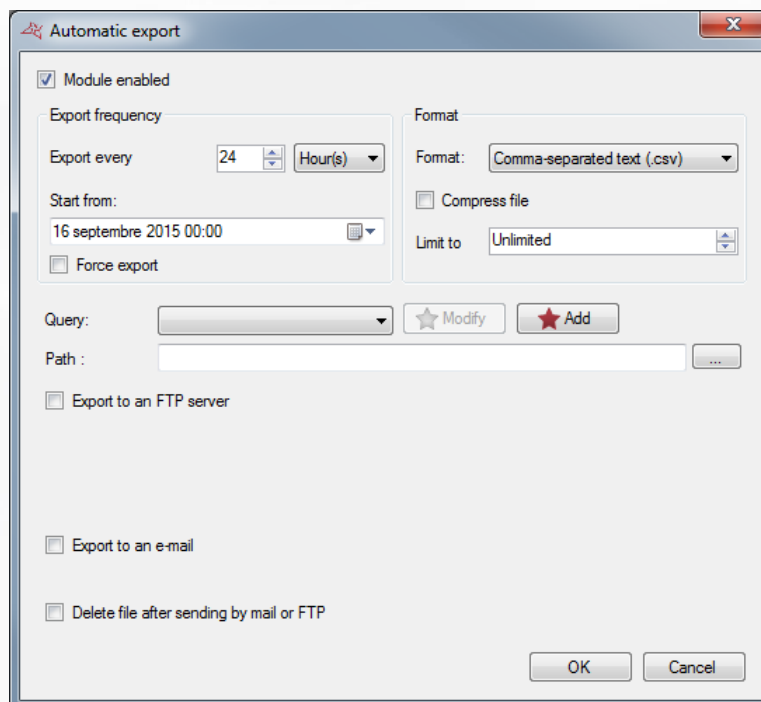
Note: To use the automatic import, make sure that the server machine is constantly running. VISOR or the Windows service must always run too.
Using the Windows service is highly recommended in this case.

AUTOMATIC EXPORT



This window manages the various export modules present on your system. You can add up to five export modules.

An export module allows you to export events automatically in different formats.



From this window, you can:

- + Enable the module by checking the "Module enabled" box:
- + Export frequency. You can specify a value between 1 hour and 200 months.

- + Start date and time for the next export.
- + Force export if you want to immediately export the events after clicking on **OK**
- + Export format (CSV, ACCESS, EXCEL, XML or PDF), compress the exported file, limit or not the number of exported events
- + Select a query (identical to History menu query). Note: filters to be entered upon execution and sub-totals are not authorised.
- + Path where the exported file will be created: use the button "... " to set the path.
- + Export to a FTP server: the exported file will be uploaded on a FTP server. Set the server path into the box "Server" (be careful to start the path with ftp://), set the user ID and password if required
- + Export to an e-mail: the exported file will be send to an email address
- + Delete file after sending by mail or FTP: if the file is uploaded on a FTP server or sent by email, check this box to delete the file on the computer after exporting

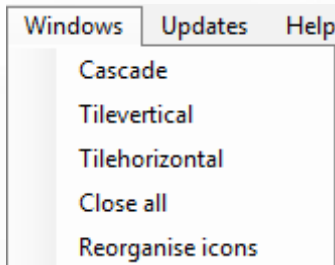
Press **OK** to store the configuration.

Note: To use the automatic export, make sure that the server machine is constantly running. VISOR or the Windows service must always run too.

Using the Windows service is highly recommended in this case.

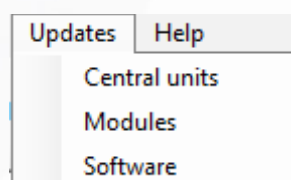
THE WINDOWS MENU

This menu allows you to reorder the windows using the following choices:



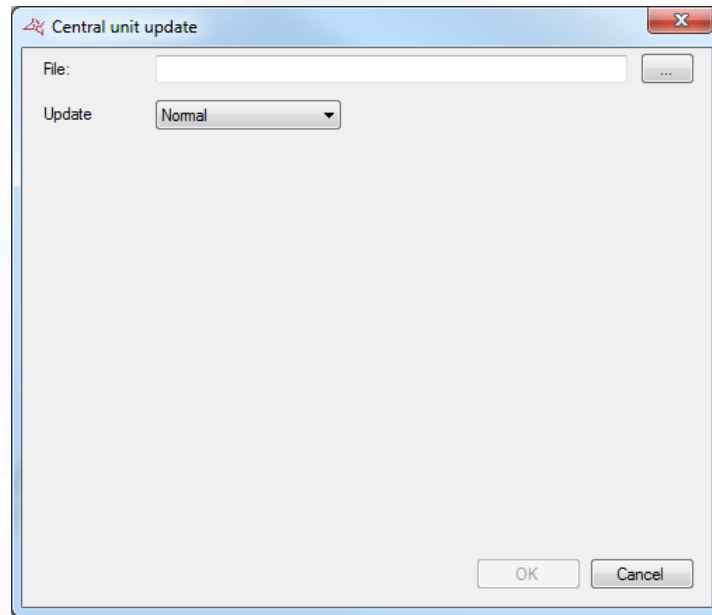
THE UPDATES MENU


This menu allows you to perform the updates of the units, extension modules and VISOR software. Depending on your choice, click **one of the following items:**



UPDATING A UNIT OR AN EXTENSION MODULE:

Caution: these updates must be performed by a qualified operator. We recommend you to perform these update with your fitter.



Select the file containing the update using the button .

Select the update mode:

- + Normal: Standard update procedure
- + Forced: If an attempt to update has already been carried out or interrupted

Check the unit or modules to update and click "OK".
Once the updates made, click "Cancel."

SOFTWARE UPDATE

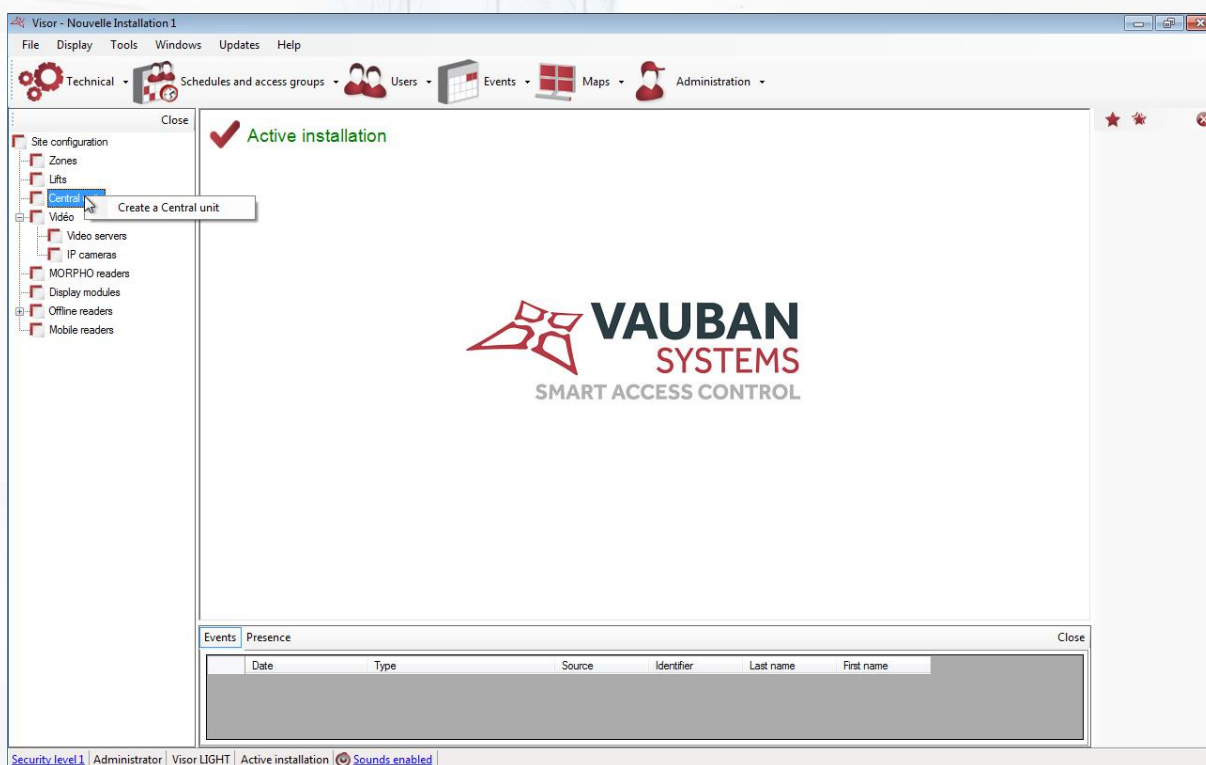
The software update needs an internet connection.
Then follow the instructions.


TECHNICAL MENU

UNITS

CREATING A UNIT

When your installation is started for the first time, you are prompted to create a central unit:



Otherwise, click on  Technical , "Site configuration", "Central units" and "Create a central unit":



From this window, you can:

- + Create a Verso+1 central unit.
- + Create a Verso+2 central unit.
- + Create a Verso+4 central unit.
- + Create a Digitouch central unit.
- + Create a Digitouch Mini central unit.
- + Create a Digitouch Mini+ central unit.
- + Create a SOOTOUCH IP central unit.
- + Create a Verso central unit.

THE VERSO, VERSO+1, VERSO+2 AND VERSO+4 UNIT

Parameters tab

Central unit VERSO+2

Parameters Operating mode

Name: Central unit 1

MAC address: [dropdown] - 10001

Search

☐ Disconnect

Connection type: Local network

Anti-passback

☐ Enable

Transit time

☐ Enable the transit time

Autoprotection

☐ Tamper Switch Input

☐ Power supply error input

Password protection

☐ Enable

Automatic time change

☒ Enable

Lobby management

Disabled

Automatic device relay

☐ Reverse its state

Clock drift

☐ Enable clock compensation

OK Cancel

From this tab, you can:

- + Name your central unit: enter the name in the "Name" field.
- + Choose the method for communicating with the central unit:
 - MAC address: before each connection, the IP address of the unit will be automatically searched by VISOR. This mode allows the use of a DHCP address on the unit. However, it is unusable in case of remote connection (VPN / NAT). In this case, use the IP address mode.
 - IP address: requires the use of a fixed IP address on the unit. This mode is also used in case of a remote connection (VPN / NAT) or when UDP is blocked on the network.
 - DNS: domain name or URL. This mode can be used when DYNDNS.
- + Click on the "Search" button to automatically detect the units connected (if using MAC address or IP address).
- + Disconnect the central unit: stops all communication with the central unit.
- + Select the connection type: local area network (if your unit is connected on the same network) or Internet / VPN (if your unit is accessible via Internet)
- + Enable **Anti-passback** and **Anti-time back**:

Anti-passback

☒ Enable

☒ Enable anti-time back

☐ 1 min

☒ Activate upon entry

☒ Activate upon exit

☐ Reverse the Anti-Time-Back

- **Anti-Pass-Back:** This mode allows you to control a user's transition cycle. The user must be out to get in and vice versa.
- **Anti-Time-Back:** users that have already entered can enter again once the specified time has elapsed (configurable between 1 and 60 minutes). The same applies to the exit.
 - Activate upon entry: Anti-Time-Back will be active upon entry
 - Activate upon exit: Anti-Time-Back will be active upon exit
 - Reverse the Anti-Time-Back: This function reverses the priority of the Anti-Time-Back and Anti-Pass-Back functions. Even if the user exits (Anti-Pass-Back), they will have to wait for the end of the Anti-Time-Back delay to enter again (valid on the entry and/or exit reader, according to the configuration).
- + Enable the transit time: A user that have already entered will not be able to go out if he exceeds that time.
- + Enable **Autoprotection**: check the "Tamper switch input" box to generate an event if the unit box is opened (a tamper switch must be wired to the unit). Select the type of contact (NO: normally open or NC: normally closed). Check the "Power supply error input" box to generate an event if a failure occurs in the unit's external power supply (a fault contact must be wired to the unit). Select the type of contact (NO: normally open or NC: normally closed).
- + Enable **"Password protection"**: protect the unit against any external connection attempts.

Password protection

☒ Enable

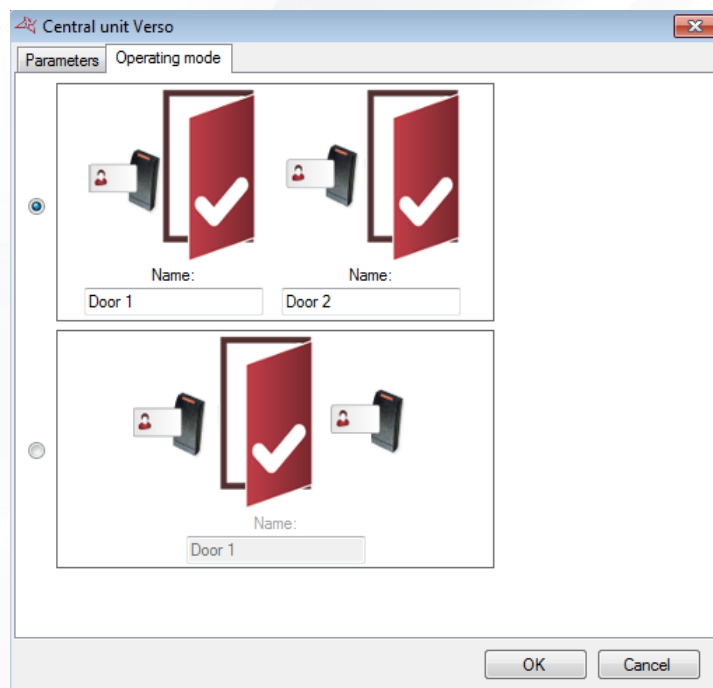
Password:

- + Enable **"Automatic time change"** (enabled by default): allows the summer / winter time to be automatically changed in the central unit (last Sunday of March and October).
- + Enable **Lobby management**: this feature prevents users from opening several lobbies at the same time. This function can be permanently operational or active during a specific time range.
- + Enable state **inversion** for automatic **relay**
- + Set the **clock drift** value.

Operating mode tab

Note: This option is not available on Verso+1

Note: On Verso+4, the operating mode is to be chosen for readers 1&2 and 3&4

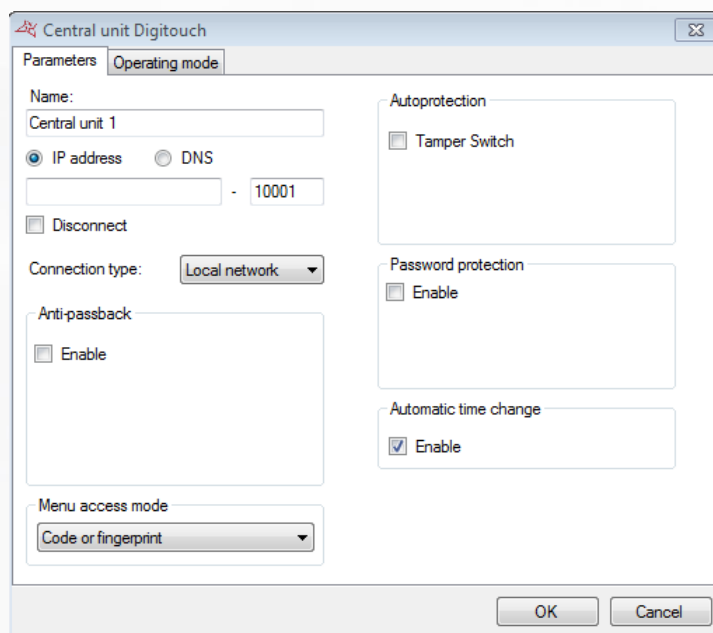


From this tab, you can:

- + Select the one reader per door mode.
- + Select the two readers for one door mode.
- + Name the doors associated with each reader.

THE DIGITOUCH UNIT

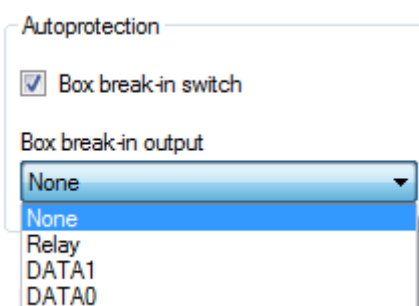
Parameters tab



From this tab, you can:

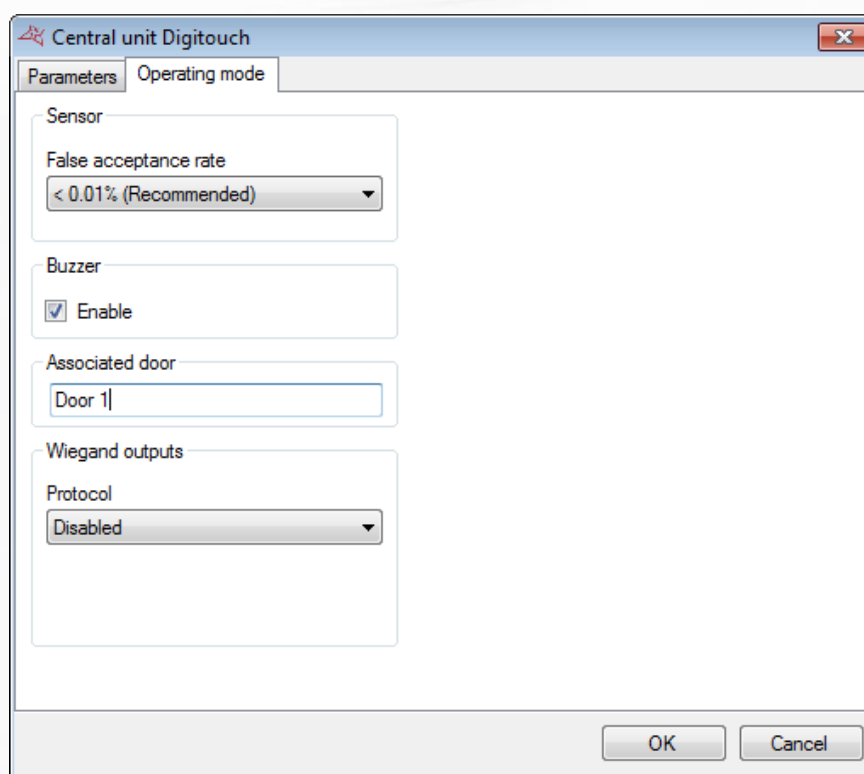
- + Name your central unit: enter the name in the "Name" field.
- + Choose the method for communicating with the central unit:

- IP address: requires the use of a fixed IP address on the unit. This mode is also used in case of a remote connection (VPN / NAT) or when UDP is blocked on the network.
- DNS: domain name or URL. This mode can be used when DYNDNS.
- + Disconnect the central unit: stops all communication with the central unit.
- + Select the connection type: local area network (if your unit is connected on the same network) or Internet / VPN (if your unit is accessible via Internet)
- + Activate "**Anti-Pass-Back**" and "**Anti-Time-Back**".
- + Choose the method for accessing the Digitouch menu: « **Code or fingerprint**" or "**Fingerprint**" only.
- + Enable **Lobby management**.
- + Enable "**Autoprotection**" with the option of using a command output available on the Digitouch or a remote command output on a V-EXTIO extension module relay.



- + Enable "Password protection".
- + Enable "Automatic time change".

Operating mode tab



From this tab, you can:

- + Change the sensor's "**False acceptance rate**" (< 0.01% by default).

- + Disable the **Buzzer**.
- + Enter the name of the "**Associated door**" for the unit.
- + Enable the "**Wiegand outputs**" and choose from the following three protocols:
 - Wiegand 26 bits.
 - Wiegand 30 bits.
 - Verso Wiegand - a dedicated protocol for the Verso central unit, whose reader type must be configured as "**DIGITOUCH**".

THE DIGITOUCH MINI UNIT

Parameters tab

From this tab, you can:

- + Name your central unit: enter the name in the "Name" field.
- + Choose the method for communicating with the central unit:
 - MAC address: before each connection, the IP address of the unit will be automatically searched by VISOR. This mode allows the use of a DHCP address on the unit. However, it is unusable in case of remote connection (VPN / NAT). In this case, use the IP address mode.
 - IP address: requires the use of a fixed IP address on the unit. This mode is also used in case of a remote connection (VPN / NAT) or when UDP is blocked on the network.
 - DNS: domain name or URL. This mode can be used when DYNDNS.
- + Click on the "**Search**" button to automatically detect the units connected (if using MAC address or IP address).
- + Disconnect the central unit: stops all communication with the central unit.
- + Select the connection type: local area network (if your unit is connected on the same network) or Internet / VPN (if your unit is accessible via Internet)
- + Enable **Anti-passback** and **Anti-time back**:
 - Anti-Pass-Back: This mode allows you to control a user's transition cycle. The user must be out to get in and vice versa.

- Anti-Time-Back: users that have already entered can enter again once the specified time has elapsed. The same applies to the exit.
- + Enable "**Autoprotection**": check the "Box break-in input" box to generate an event if the central unit box is opened (a tamper switch must be wired to the central unit). Select the type of contact (NO: normally open or NC: normally closed). You can also use a command output available on the central unit or a remote command output on a V-EXTIO extension module relay.

Check the "Power supply error input" box to generate an event if a failure occurs in the central unit's external power supply (a fault contact must be wired to the central unit). Select the type of contact (NO: normally open or NC: normally closed).

- + Enable "**Password protection**": protect the unit against any external connection attempts.

- + Enable "**Automatic time change**" (enabled by default): allows the summer / winter time to be automatically changed in the central unit (last Sunday of March and October).

Operating tab mode

From this tab, you can:

- + Select the one reader per door mode.
- + Select the two readers for one door mode.
- + Name the doors associated with each reader.

THE SOOTOUCH IP UNIT

Parameters tab

From this tab, you can:

- + Name your central unit: enter the name in the "Name" field.
- + Choose the method for communicating with the central unit:
 - o MAC address: before each connection, the IP address of the unit will be automatically searched by VISOR. This mode allows the use of a DHCP address on the unit. However, it is unusable in case of remote connection (VPN / NAT). In this case, use the IP address mode.
 - o IP address: requires the use of a fixed IP address on the unit. This mode is also used in case of a remote connection (VPN / NAT) or when UDP is blocked on the network.
 - o DNS: domain name or URL. This mode can be used when DYNDNS.
- + Click on the "Search" button to automatically detect the units connected (if using MAC address or IP address).
- + Disconnect the central unit: stops all communication with the central unit.
- + Select the connection type: local area network (if your unit is connected on the same network) or Internet / VPN (if your unit is accessible via Internet)
- + Enable **Anti-passback** and **Anti-time back**:
 - o Anti-Pass-Back: This mode allows you to control a user's transition cycle. The user must be out to get in and vice versa.
 - o Anti-Time-Back: users that have already entered can enter again once the specified time has elapsed. The same applies to the exit.
- + Enable "**Autoprotection**": check the "Box break-in input" box to generate an event if the central unit box is opened (a tamper switch must be wired to the central unit). Select the type of contact (NO: normally open or NC: normally closed). You can also use a command

output available on the central unit or a remote command output on a V-EXTIO extension module relay.

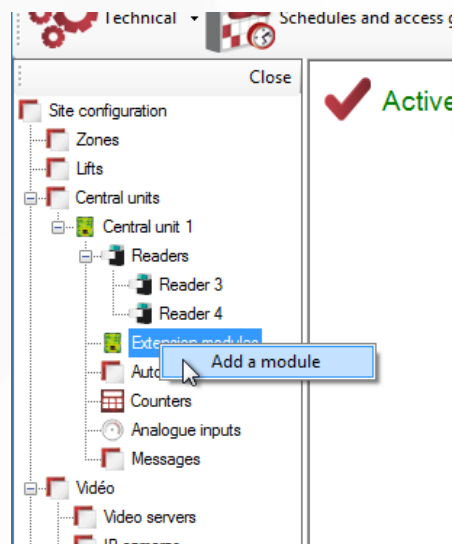
- + Check the "Power supply error input" box to generate an event if a failure occurs in the central unit's external power supply (a fault contact must be wired to the central unit). Select the type of contact (NO: normally open or NC: normally closed).
- + Enable **"Password protection"**: protect the unit against any external connection attempts.

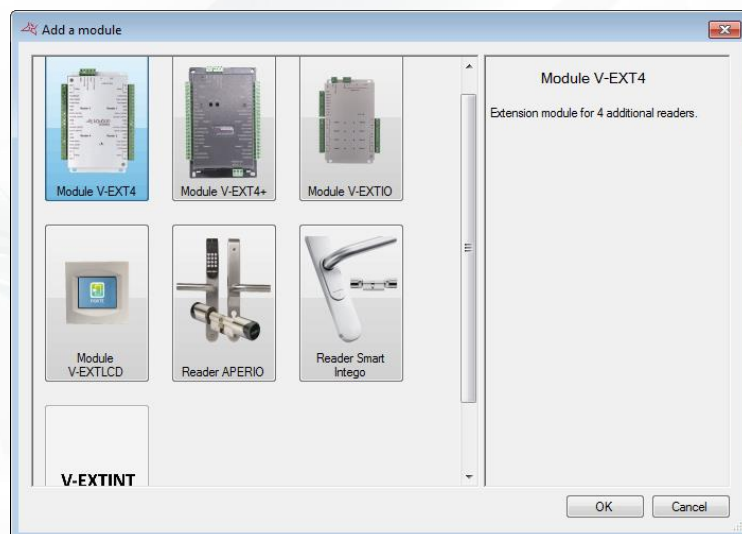
- + Enable **"Automatic time change"** (enabled by default): allows the summer / winter time to be automatically changed in the central unit (last Sunday of March and October).
- + Select the type of the RS485 reader:
 - o SSCP reader (STID)
 - o OSDP reader (HID)
 - o APERIO reader (electronic escutcheon or cylinder)
 - o ZOMOFI reader (active radio receiver)
 - o S33 (STID – high security reader, press **"Advanced configuration"** to configure the cipher key, the card number position and size)

EXTENSION MODULES

CREATING AN EXTENSION MODULE

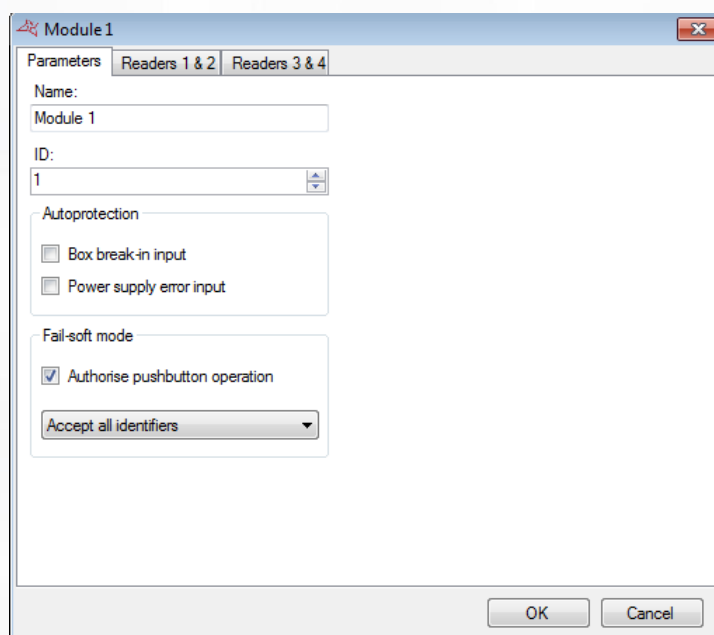
To add an extension module, click on **"Extension modules"** and then the type of module to be added as follows:





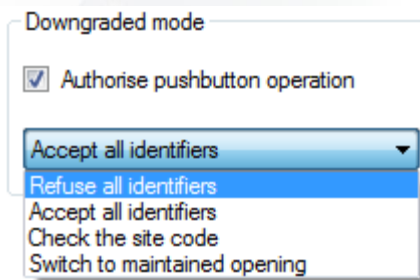
V-EXT4, V-EXT4+ MODULE

Parameters tab



From this tab, you can:

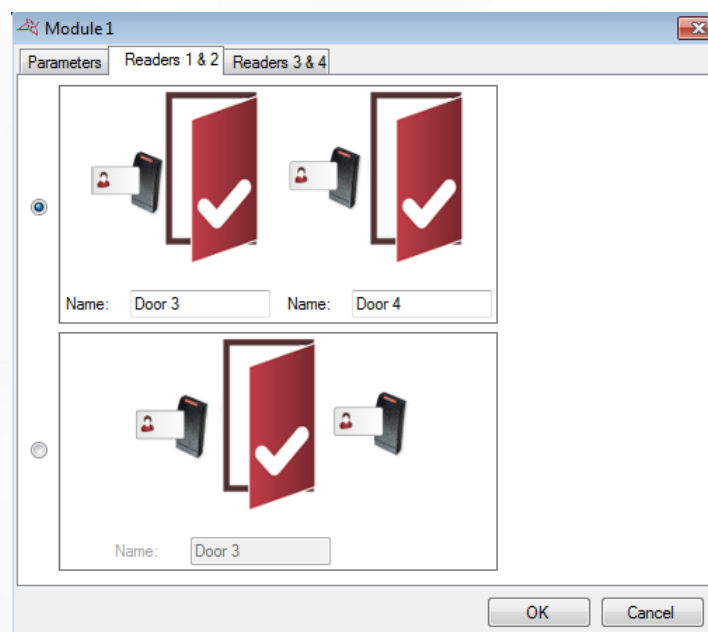
- + Name your module: enter the name in the "Name" field.
- + Define the module's identifier, which can be found on a label affixed to the module (e.g. **ID: 00051**).
- + Enable Autoprotection with the "Box break-in input" or "Power supply failure" options.
- + Select the required type of fail-safe behaviour from the following choices:
 - Disable the pushbutton: the pushbutton will not work in this mode.
 - Reject all identifiers (no badges will be accepted).
 - Check site code (only badges with authorised site codes will be accepted).
 - Switch to maintained opening (blocks all open doors).



This mode becomes effective 30 seconds after a communication failure with the VERSO central unit.

Caution: in fail-soft mode, no events will be recorded by the module.

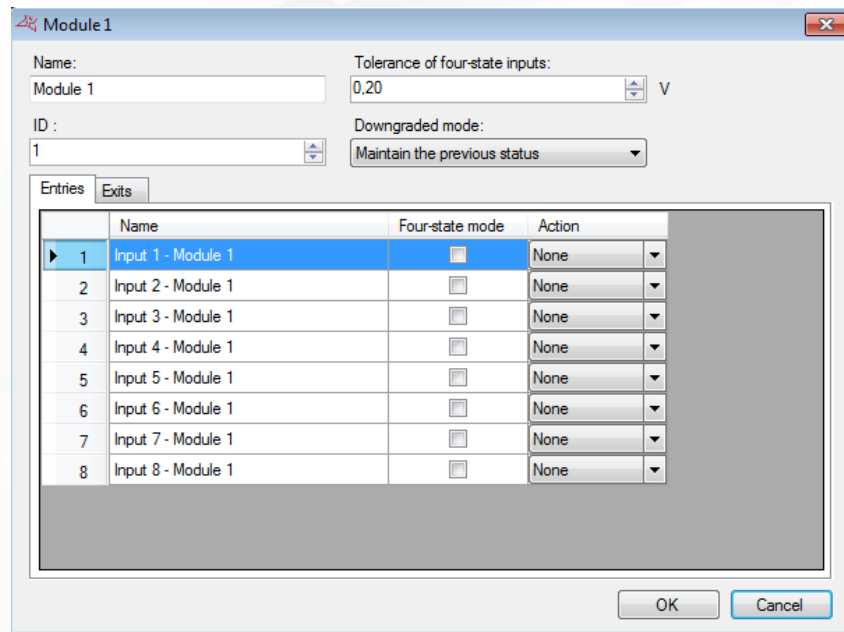
Readers 1 & 2 and Readers 3 & 4 tabs



From these tabs, you can:

- + Select the one reader per door mode.
- + Select the two readers for one door mode.
- + Name the doors associated with each reader.

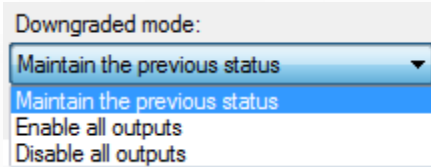
V-EXTIO MODULE



	Name	Four-state mode	Action
1	Input 1 - Module 1	<input type="checkbox"/>	None
2	Input 2 - Module 1	<input type="checkbox"/>	None
3	Input 3 - Module 1	<input type="checkbox"/>	None
4	Input 4 - Module 1	<input type="checkbox"/>	None
5	Input 5 - Module 1	<input type="checkbox"/>	None
6	Input 6 - Module 1	<input type="checkbox"/>	None
7	Input 7 - Module 1	<input type="checkbox"/>	None
8	Input 8 - Module 1	<input type="checkbox"/>	None

From this window, you can:

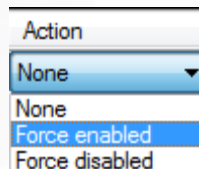
- + Name your module: enter the name in the "Name" field.
- + Define the module's identifier, which can be found on a label affixed to the module (e.g. **ID: 00051**).
- + Specify the tolerance of the four-state inputs (if applicable) between 0.20V and 1.20V.
- + In fail-soft mode, enable / disable all outputs or maintain the previous status.



This mode becomes effective 30 seconds after a communication failure with the VERSO central unit.

From the "Inputs" tab, you can:

- + Name the module inputs: enter the name in the "Name" field.
- + Enable the Four-state mode.
- + Force the input to Enabled or Disabled.



From the "Outputs" tab, you can name the module outputs: enter the name in the "Name" field.

V-EXTLCD MODULE

From this window, you can:

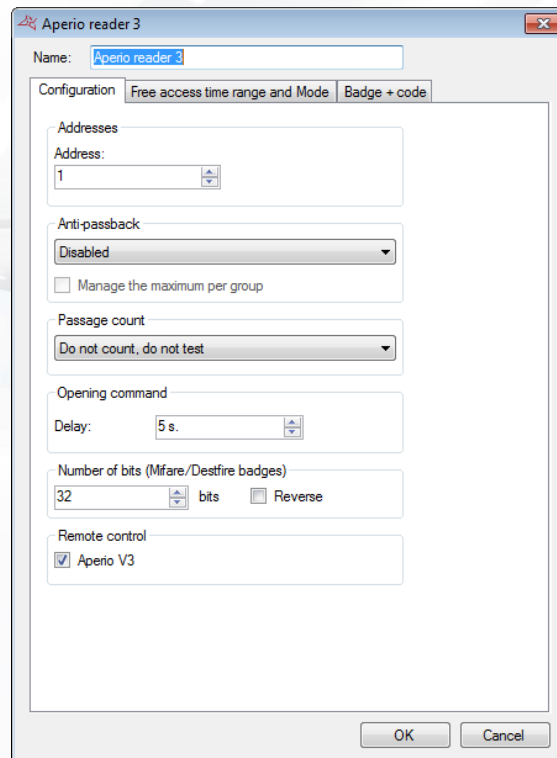
- + Name your module: enter the name in the "Name" field.
- + Assign a value from 1 to 255 seconds for the display stand-by feature.
- + Enable the cleaning code (9999): by entering this code, the keypad will be locked for 30 seconds so that it can be cleaned.
- + Define the module's identifier, which can be found on a label affixed to the module (e.g. ID: 00051).
- + Choose the default screen:

- Touch button.
- Keypad.
- Keypad (rolling code).
- Menu 1, 2, 3 or 4.
- + Name the menus and buttons: enter the name in the "Name" and "Buttons" fields.

Name	Button 1	Button 2	Button 3	Button 4
Menu 1 - Module 1				
Menu 2 - Module 1				
Menu 3 - Module 1				
Menu 4 - Module 1				

Each button is configured with one or more automatic devices that will need to be created.

APERIO® READER



From this window, you can name your reader: enter the name in the "Name" field.

Configuration tab

From this tab, you can:

- + Enter the reader's address.
 - + Enable the "**Anti-passback**" function and choose whether the reader is for an entry or exit.
 - + Enable the maximum number of users per group.
 - + Enable the passage count function.
-
- + Enter the delay of opening.
 - + Define the number of bits for Mifare/Desfire badges
 - o Reverse: allows you to indicate that the badge number is reversed for a 32- or 56-bit badge
 - + Specify whether the shell is an Apério V3

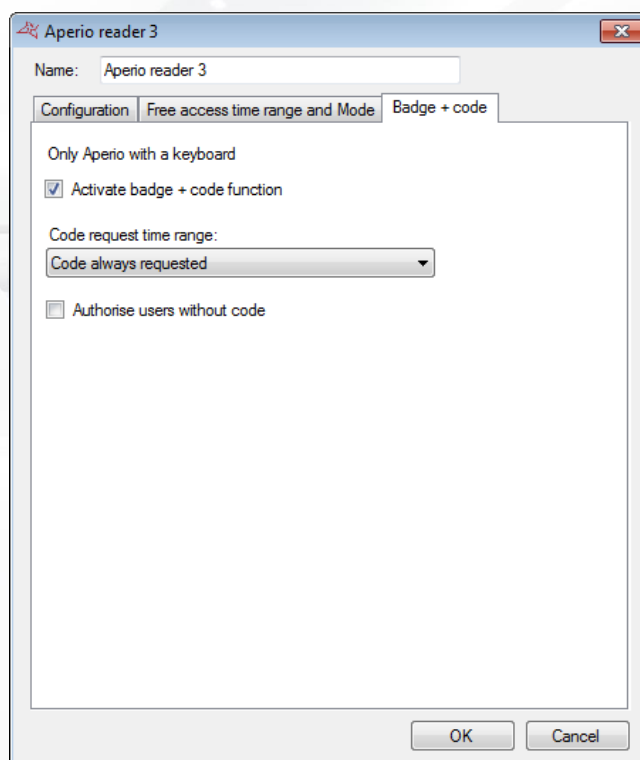
Free Access time range and Mode tab

The screenshot shows the 'Aperio reader 3' configuration window with the 'Free access time range and Mode' tab selected. The window has a title bar with a red 'X' icon. Below the title bar, there's a 'Name:' field with 'Aperio reader 3' entered. The main area is divided into three tabs: 'Configuration', 'Free access time range and Mode' (active), and 'Badge + code'. Under the active tab, there's a section for 'APERIO hub address' with three 'Free access time range:' labels, each followed by a dropdown menu (all set to 'None') and two buttons: 'See time range' and 'Add a time range'. Below this, there are two checkboxes: 'Start free access at first accepted user' and 'Enable office mode'. A section titled 'Profile 3 (enabled on Security Level 3)' contains three 'Mode (security level X):' labels, each followed by a dropdown menu (all set to 'Continuous monitoring'). At the bottom right, there are 'OK' and 'Cancel' buttons.

From this tab, you can:

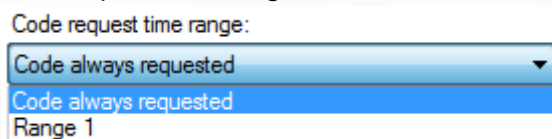
- + Set the free access range for each security level
 - Select "None" to apply no free access to the reader
 - Select a time range so that the reader will remain opened until the selected range will remained active
 - Click "Add a time Range" to create a new time range
 - Click "See time range" to edit the selected time
- + The free access time range (if selected) will only start until a user will be accepted
- + Enable office mode
- + Select the operating mode for 3 security levels
 - Either continuous monitoring, or
 - Opening maintained, or
 - Closure maintained.

Badge + Code tab



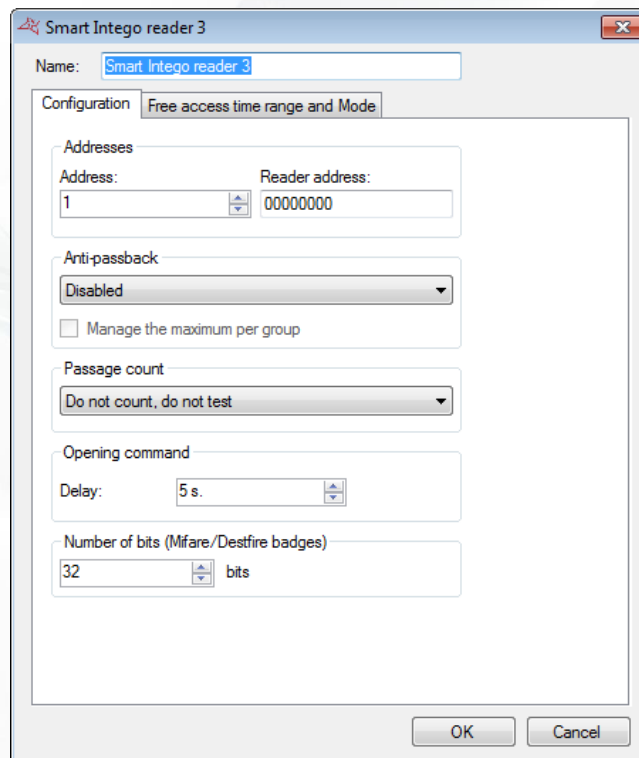
From this tab, you can:

- + Enable the badge + code function.
- + Enter a predefined code request time range.



- + Authorise users without a code.

SMART INERGO READER

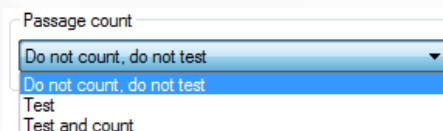


From this window, you can name your reader: enter the name in the "Name" field.

Configuration tab

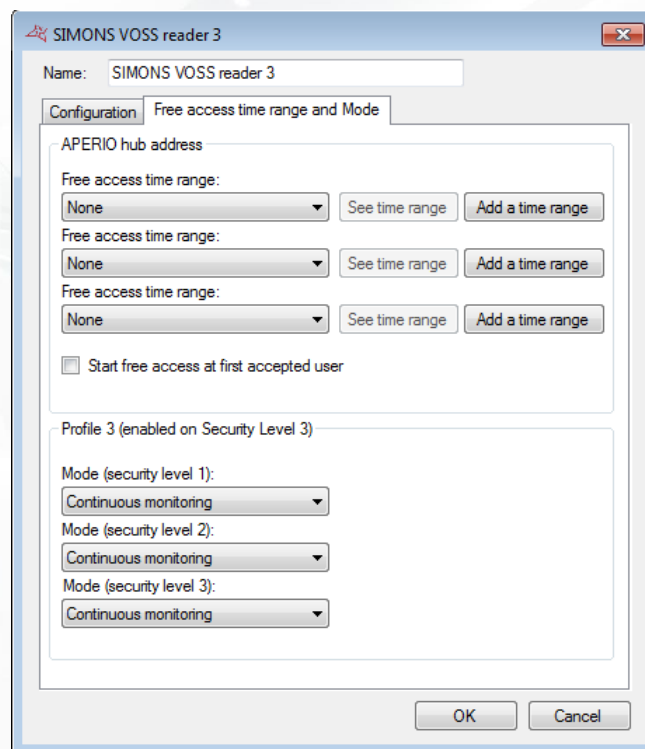
From this tab, you can:

- + Enter the Gateway node address.
- + Enter the reader's address.
- + Enable the "**Anti-passback**" function and choose whether the reader is for an entry or exit.
- + Enable the maximum number of users per group.
- + Enable the passage count function.



- + Enter the delay of opening.
- + Define the number of bits for Mifare/Destfire badges

Free Access time range and Mode tab

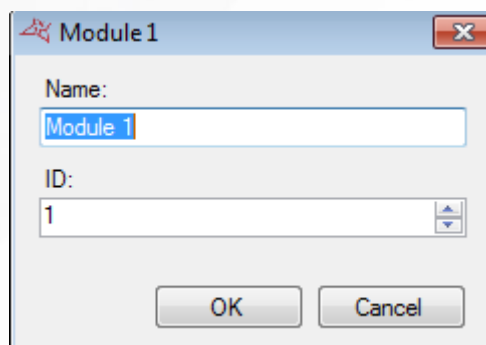


From this tab, you can:

- + Set the free access range for each security level
 - Select "None" to apply no free access to the reader
 - Select a time range so that the reader will remain opened until the selected range will remained active
 - Click "Add a time Range" to create a new time range
 - Click "See time range" to edit the selected time
 - Start free access at the first accepted user.
- + Select the operating mode for 3 security levels
 - Either continuous monitoring, or
 - Opening maintained, or
 - Closure maintained.

V-EXTINT MODULE

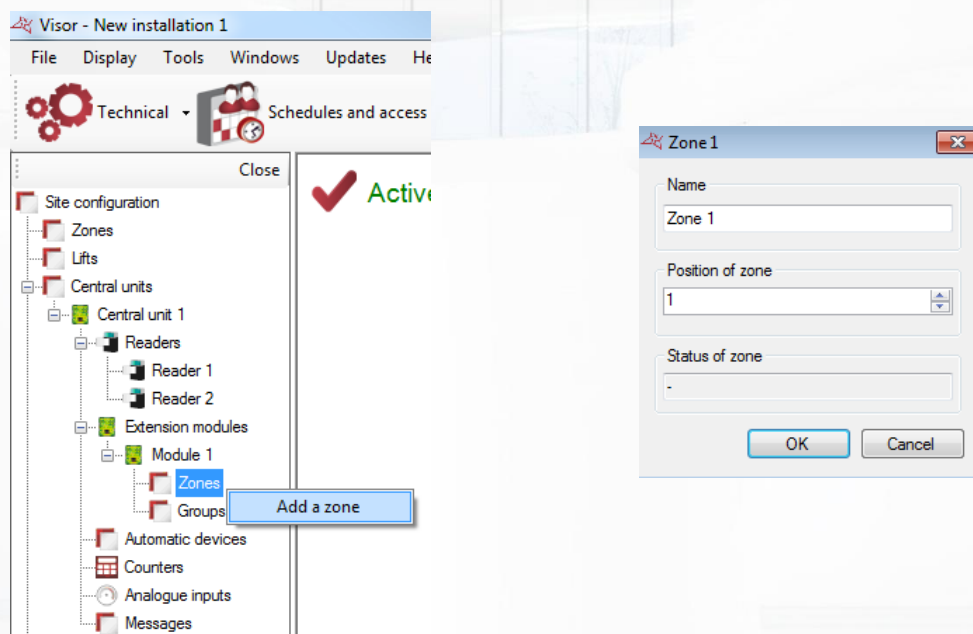
This module allows you to control a LIGHTSYS RISCO® intrusion unit. It requires an additional license MOD-INTRUSION.



From this window, you can:

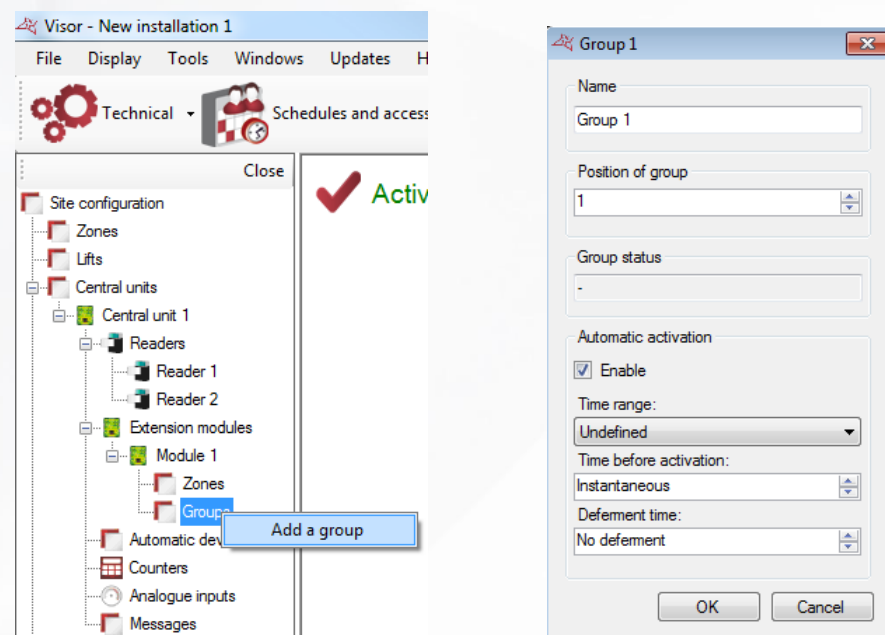
- + Name your module: enter the name in the "Name" field.
- + Define the module's identifier, which can be found on a label affixed to the module (e.g. ID: 00051).

To add a zone, click on "Zones" and click "Add Zone". You can add up to 8 zones per module.



From this window, you can give a name to your zone and set its position. You can also check its status.

To add a group, click on "Groups" and then click "Add Group". You can add up to 4 groups.

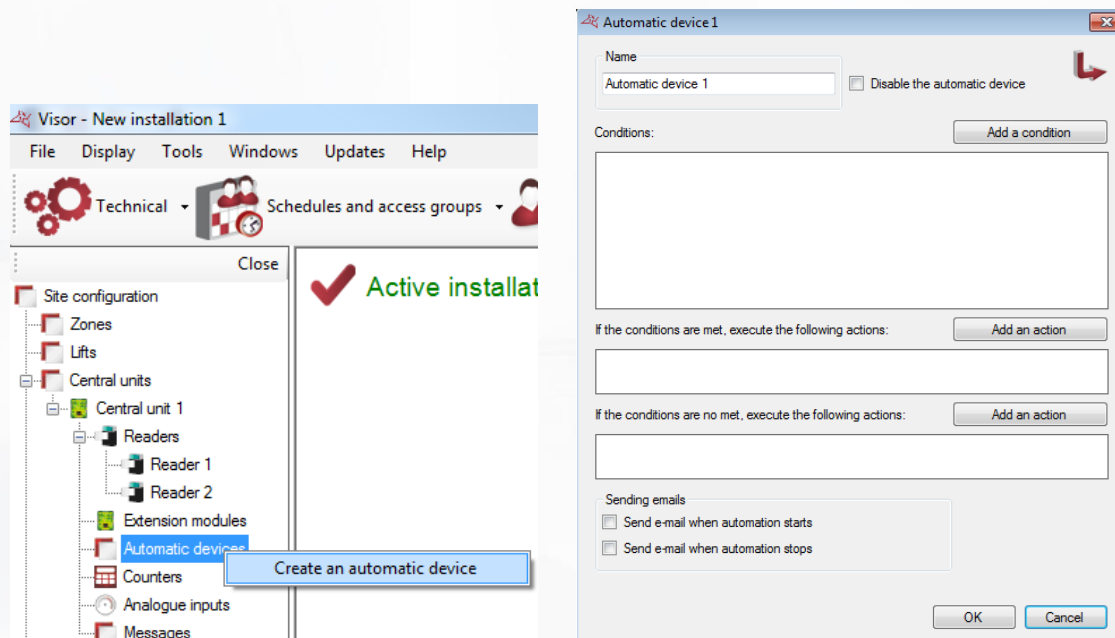


From this window, you can name your group, set its position, check its status and enable automatic start:

- + At a time range
- + With a delay before starting:
 - o Instantaneously
 - o From 1 to 255 minutes
- + With an extension time
 - o Without delay (Instant service)
 - o From 1 to 255 minutes: allows to report the automatic start if a user is accepted on a reader

AUTOMATIC DEVICES

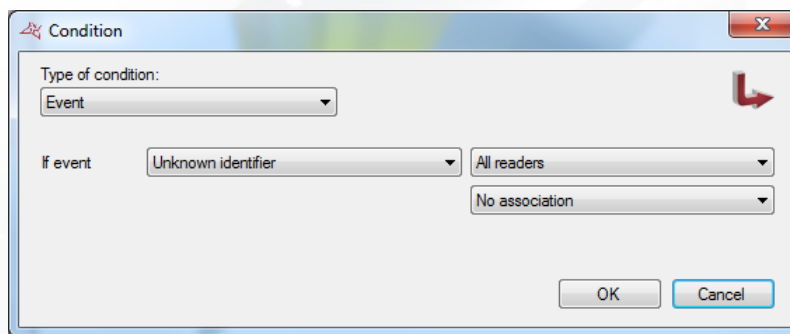
To add an automatic device, click on "Automatic devices" and then "Create an automatic device" as follows:



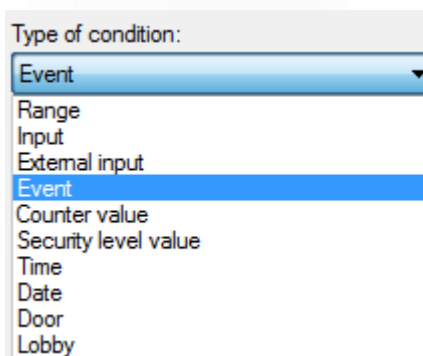
In the Automatic device window, you can:

- + Name your automatic device: enter the name in the "Name" field.
- + Disable the automatic device.
- + Add up to four conditions associated with an "AND" or "OR" logical operator.
- + Add up to two actions, which will be executed when the conditions are true.
- + Add up to two opposing actions, which will be executed when the conditions are false.
- + Choose to send an email to all managers authorized to receive alerts when the device starts
- + Choose to send an email to all managers authorized to receive alerts when the device stops

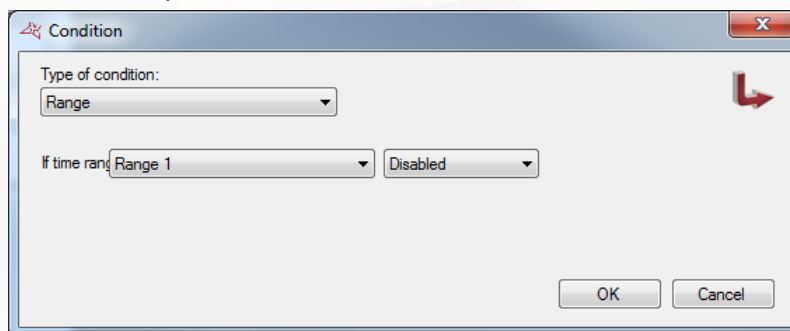
ADDING A CONDITION



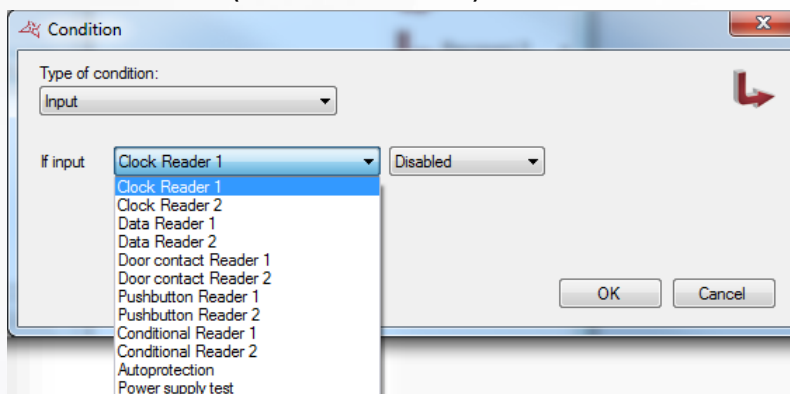
From the "Condition" window, you can select the type of condition:



- + For a "Range" condition, select the time range to be tested and then select its status (enabled or disabled).



- + For an "Input" condition, select the input to be tested (only those in the Verso central unit) and then select its status (enabled or disabled).



- + For an "External input" condition, select the input to be tested (only those in VEXTIO or VEXTLCD modules) and then select its status (enabled, disabled or sabotaged for the four-state inputs of the VEXTIO modules).

The screenshot shows the 'Condition' dialog box with the 'Type of condition' set to 'External input'. Under 'If external input', a dropdown menu is open showing a list of inputs: 'Input 1 - Module 1', 'Input 2 - Module 1', 'Input 3 - Module 1', 'Input 4 - Module 1', 'Input 5 - Module 1', 'Input 6 - Module 1', 'Input 7 - Module 1', and 'Input 8 - Module 1'. The status is set to 'Disabled'. The 'OK' and 'Cancel' buttons are at the bottom right.

- + For an "Automatic device" condition, select the automatic device to be tested and then select its status (enabled or disabled).

The screenshot shows the 'Condition' dialog box with the 'Type of condition' set to 'Automation'. Under 'If', a dropdown menu is open showing 'Automation 18'. The status is set to 'Disabled'. The 'OK' and 'Cancel' buttons are at the bottom right.

- + For an "Event" condition, select the type of event to be tested.

The screenshot shows the 'Condition' dialog box with the 'Type of condition' set to 'Event'. Under 'If event', there are three dropdown menus: 'Unknown identifier', 'All readers', and 'No association'. The 'OK' and 'Cancel' buttons are at the bottom right.

Depending on the type of event, you can add an additional condition, such as:

- The choice of reader on which the event occurs.
- The number of the identifier relating to the event.
- The group of the user relating to the event.
- The menu of a VEXTLCD relating to the event.
- The code entered on a VEXTLCD relating to the event.

- + For a "Counter value" condition (displayed if a counter is created), select the counter to be tested and the test method (if the value is lower than / greater than or equal to / equal to) and then enter the value to be compared.

The screenshot shows the 'Condition' dialog box with the 'Type of condition' set to 'Value of counter'. The 'If counter' dropdown is set to 'Counter 1'. The comparison method dropdown is open, showing options: 'less than', 'less than or equal to', 'greater than or equal to', and 'equal to'. The value field contains '1'. The 'OK' and 'Cancel' buttons are at the bottom right.

- + For a "Security level value" condition, select the test method (if the current security level is lower than / greater than or equal to / equal to) and then enter the value to be compared.

The screenshot shows the 'Condition' dialog box with the 'Type of condition' set to 'Value of security level'. The 'If the security level is' dropdown is open, showing options: 'less than', 'less than or equal to', 'greater than or equal to', and 'equal to'. The value field contains '1'. The 'OK' and 'Cancel' buttons are at the bottom right.

- + For a "Time" condition, select the test method (if the current time is lower than / greater than or equal to / equal to) and then enter the value to be compared.

The screenshot shows the 'Condition' dialog box with the 'Type of condition' set to 'Time'. The 'If the time is' dropdown is open, showing options: 'less than', 'less than or equal to', 'greater than or equal to', and 'equal to'. The value field contains '11:00'. The 'OK' and 'Cancel' buttons are at the bottom right.

- + For a "Date" condition, select the test method (if the current date is lower than / greater than or equal to / equal to) and then enter the date to be compared.

The screenshot shows the 'Condition' dialog box with the 'Type of condition' set to 'Date'. The 'If the date is' dropdown is open, showing options: 'less than', 'less than or equal to', 'greater than or equal to', and 'equal to'. The value field contains 'lundi 13 janvier 2014'. The 'OK' and 'Cancel' buttons are at the bottom right.

- + For a "Door" condition, select the door to be tested and then select its status (Closed or Open).

The 'Condition' dialog box shows 'Type of condition:' set to 'Door'. Below it, 'If door' is set to 'Porte 2'. A dropdown menu for status is open, showing 'Closed' (selected), 'Closed', and 'Open'. 'OK' and 'Cancel' buttons are at the bottom right.

- + For a "Lobby" condition, select its status (Closed or Open).

The 'Condition' dialog box shows 'Type of condition:' set to 'Lobby'. Below it, 'If lobby is' is set to 'Closed'. 'OK' and 'Cancel' buttons are at the bottom right.

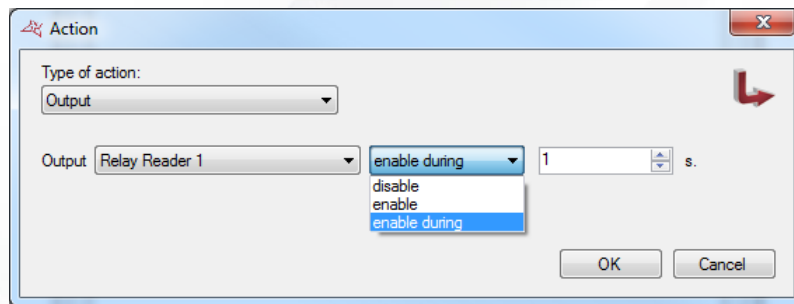
ADDING AN ACTION

The 'Action' dialog box shows 'Type of action:' set to 'Output'. Below it, 'Output' is set to 'Relay Reader 1' and the action is set to 'Disable'. 'OK' and 'Cancel' buttons are at the bottom right.

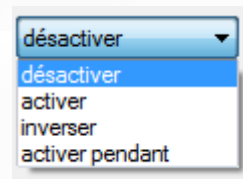
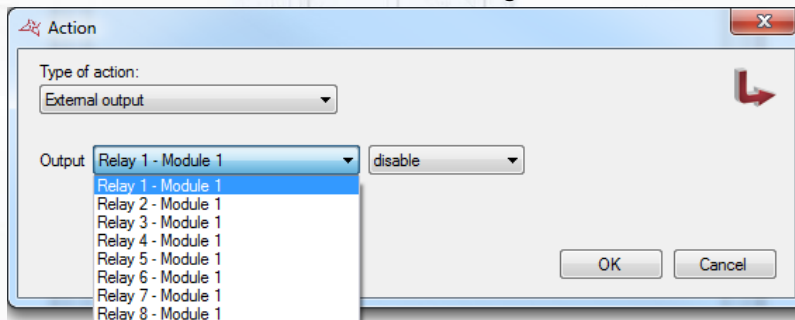
From this window, you can select the type of action:

A dropdown menu showing the following options: Output (selected), External output, Group, Reader, Counter, Forgiving, Security level, and Video event.

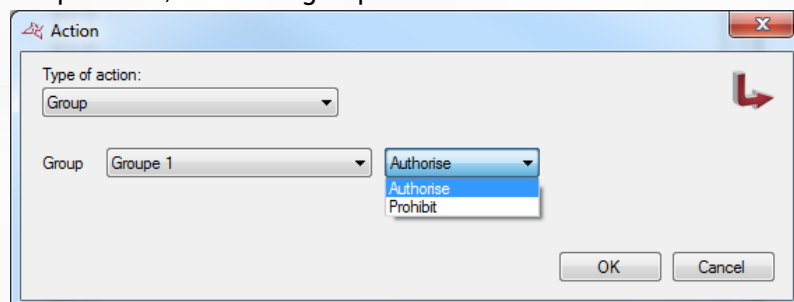
- + For an "Output" action, select one of the outputs of the Verso central unit and then choose Enable, Disable or Enable during (1 to 65534 seconds).



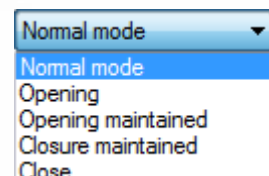
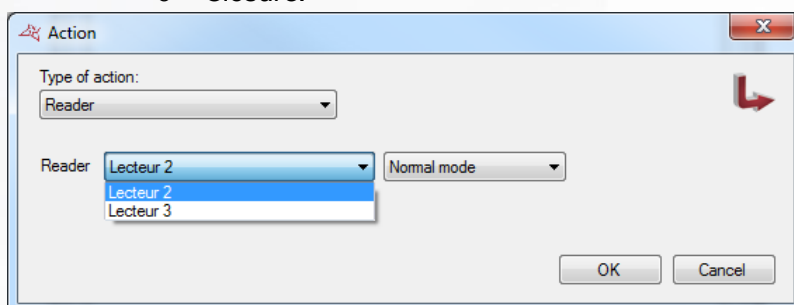
- + For an "External output" action, select a relay for a V-EXTIO module and then choose Enable, Disable, Invert or Enable during (1 to 65534 seconds).



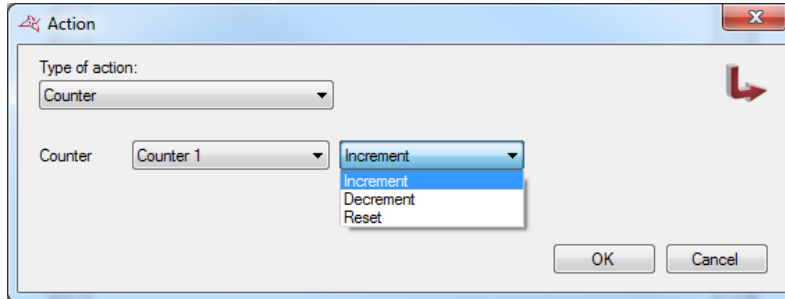
- + For a "Group" action, select the group and then Authorise or Prohibit.



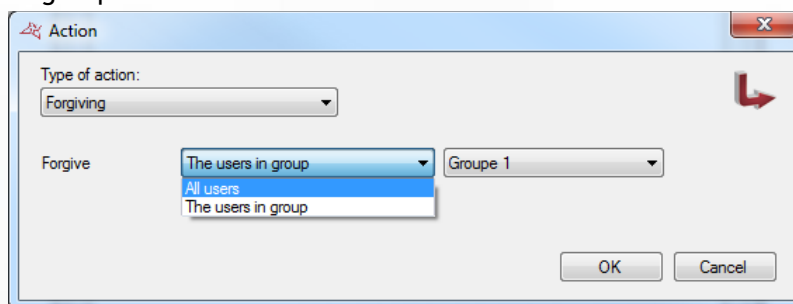
- + For a "Reader" action, select the reader and choose one of the following operating modes:
 - o Normal mode.
 - o Opening (delay).
 - o Opening maintained.
 - o Closure maintained.
 - o Closure.



- + For a "Counter" action, select a counter and then Increment, Decrement or Reset.

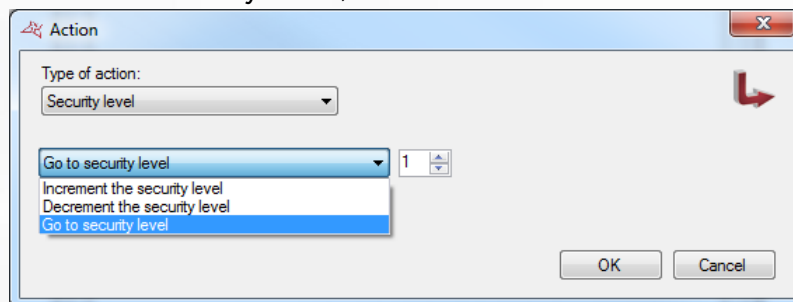


- + For a "Forgiveness" action, you can:
 - o Clear the anti-passback cycle for "All users".
 - o Clear the anti-passback cycle for all "The users in the group" and then select the group.



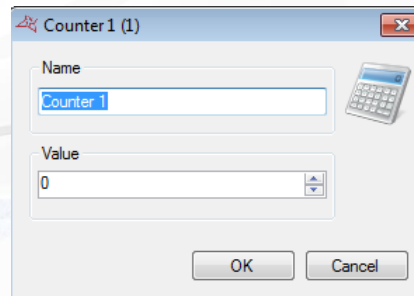
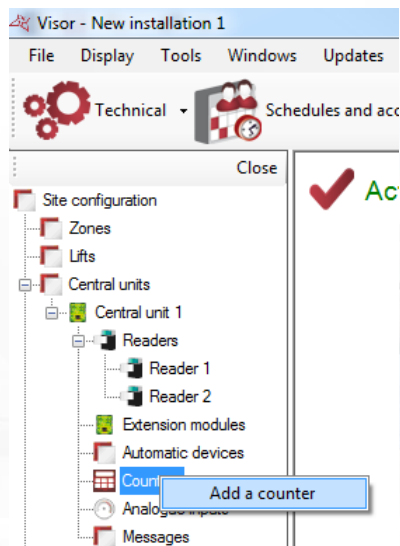
Caution: To execute this action, VISOR must be running on your computer.

- + For a "Security level" action, select:
 - o Increment the security level.
 - o Decrement the security level.
 - o Switch to security level 1, 2 or 3.



COUNTERS

To add a counter, click on "Counters" and then "Add a counter" as follows:

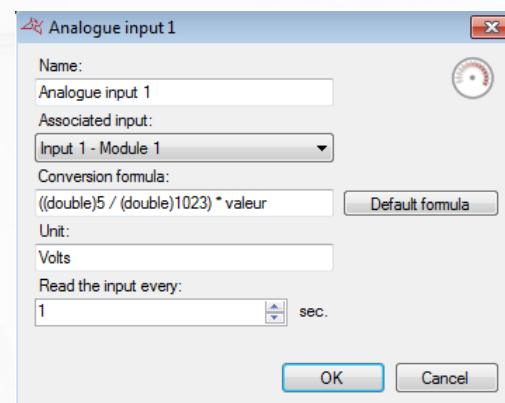
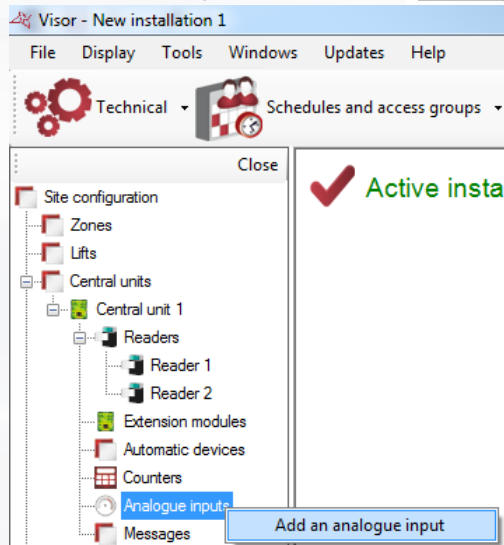


From the counter window, you can:

- + Change the "Name".
- + Enter a value between 0 and 65535.

ANALOGUE INPUTS

To add an analogue input, click on "Analogue inputs" and then "Add an analogue input" as follows:



The analogue input is associated with a V-EXTIO module that first needs to be created in VISOR.

In the "Analogue input" window, you can:

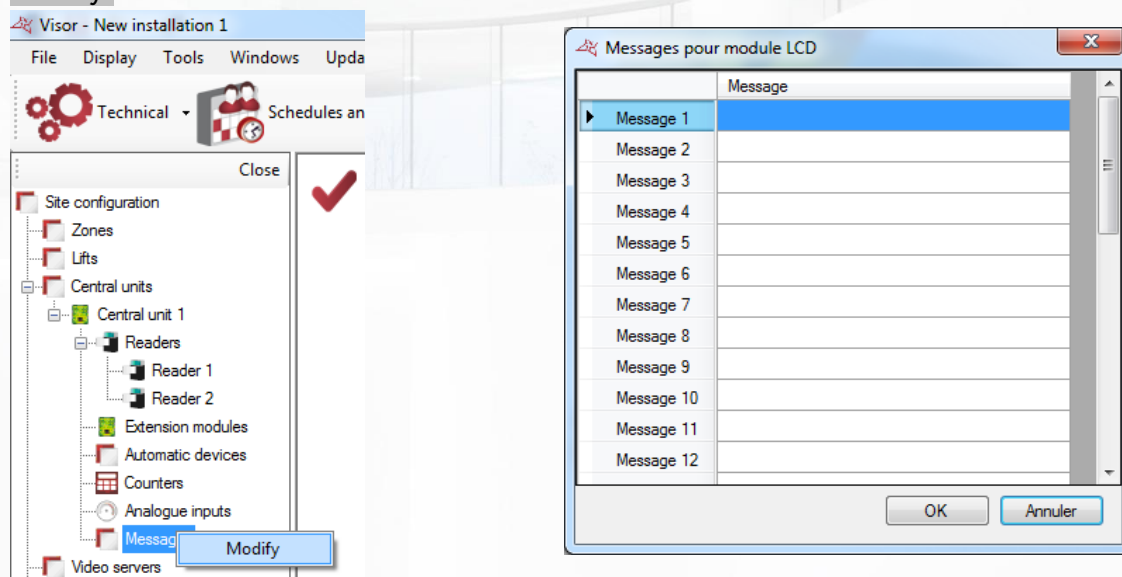
- + Change the "Name".
- + Choose the input associated with the V-EXTIO module.
- + Choose a conversion formula.
- + Choose a unit of measurement.
- + Enter a time value for reading the analogue input between 1 and 360 seconds.

The analogue input has a conversion range between 0V and 5V.

The converted value can then be displayed in the overview plan.

LCD MESSAGES

To configure the messages displayed on the VEXTLCD modules, click on "Messages" and then "Modify" as follows:



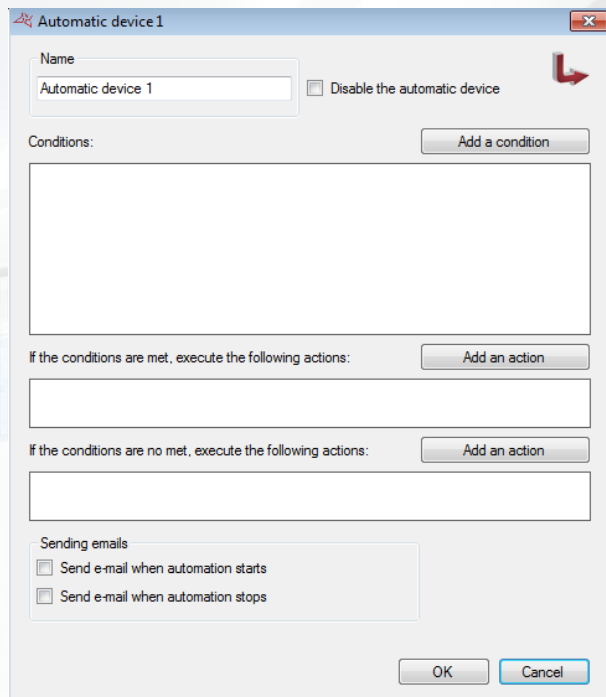
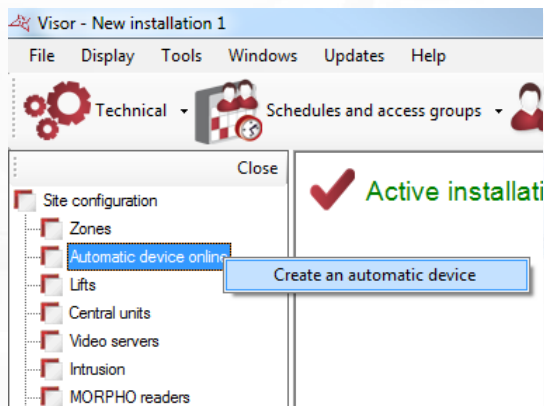
In the "Messages for LCD module" window, you can enter 32 messages of up to 32 characters each.

These messages can be displayed using an automatic device.

ONLINE AUTOMATIC DEVICES

Online automatic devices are only available in case of using a client / server installation (SQL database) with the Windows service. Under another type of installation, these devices do not appear. They are only managed by VISOR. So make sure that the server machine is constantly running.

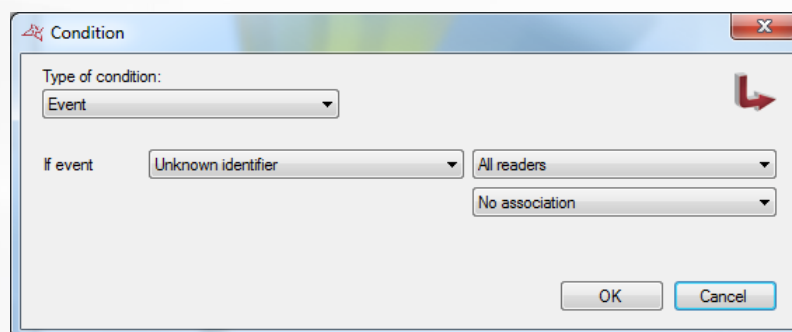
To add an automatic, click on "Online Automation" and then "Create an automatism" as follows:



From the window of the automatic device, you can:

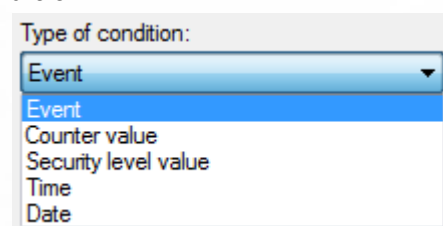
- + Give a name to your device: Type in the "Name" field
- + Disable the device
- + Add up to four conditions associated with an "AND" or "OR" logical operator.
- + Add up to two actions, which will be executed when the conditions are true.
- + Add up to two opposing actions, which will be executed when the conditions are false.
- + Choose to send an email to all managers authorized to receive alerts when the device starts
- + Choose to send an email to all managers authorized to receive alerts when the device stops

Adding a condition:

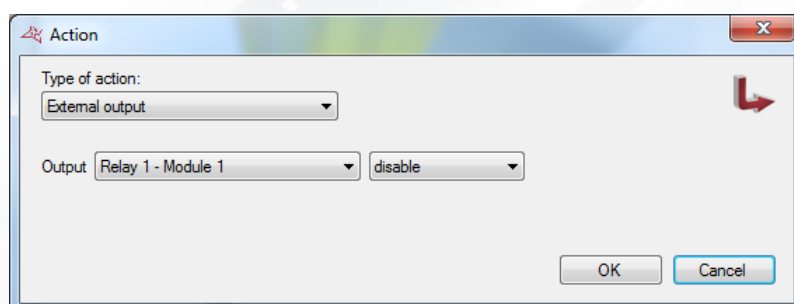


From the "Condition" window, you can select the type of condition:

- + An event
- + A value for a counter
- + A value for security
- + A time
- + A date

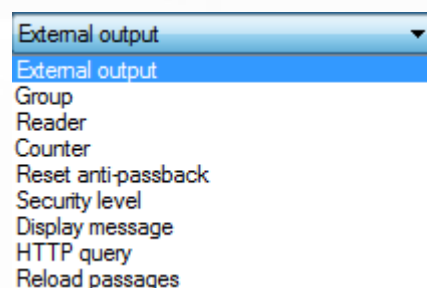


Adding an action:



From the "Action" window, you can select the type of action:

- + Drive an external VEXT-IO output
- + Grant/deny an access group
- + Drive a reader
- + Change the value of a counter
- + Reset the users anti-passback cycle
- + Change the security level
- + Display a message on a MOD-AFF module
- + Execute a HTTP query
- + Reload users number of passages

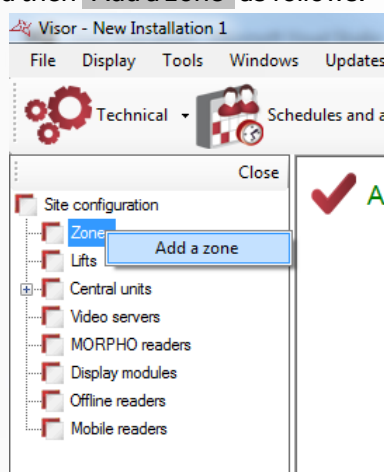


For more information about the parameters, see chapter "Automatic devices" above.

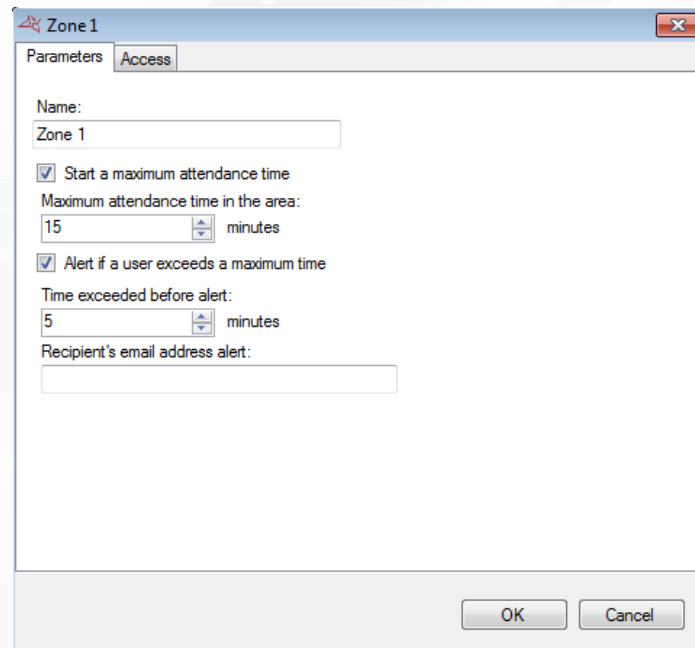
ZONES MANAGEMENT

The zones management allows you to locate users. For this, you can either edit a user's record or consult the "Present user management" (available from the "Users" menu").

To add a zone, click on "Zones" and then "Add a zone" as follows:



Parameters tab

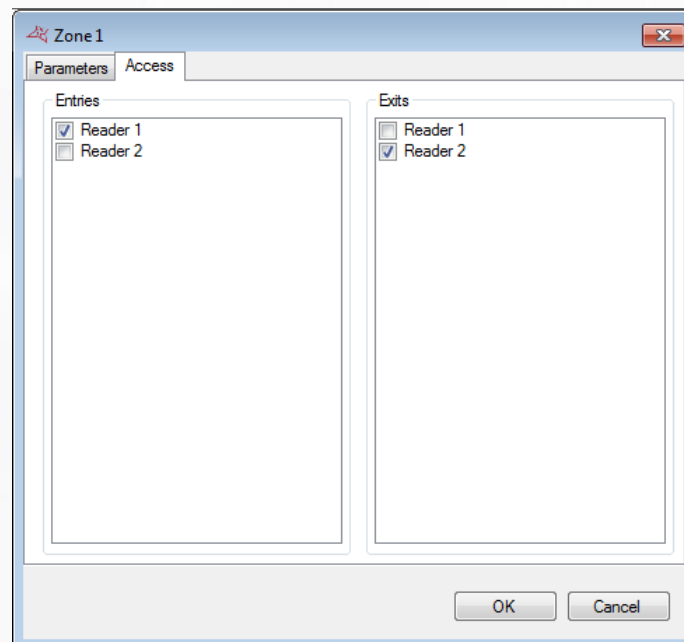


The screenshot shows a window titled 'Zone 1' with a 'Parameters' tab selected. The 'Access' sub-tab is active. The 'Name' field is set to 'Zone 1'. The 'Start a maximum attendance time' checkbox is checked, with a value of '15' minutes. The 'Alert if a user exceeds a maximum time' checkbox is also checked, with a value of '5' minutes. The 'Recipient's email address alert' field is empty. 'OK' and 'Cancel' buttons are at the bottom right.

From this tab, you can:

- + Name your zone
- + Start a maximum attendance time if a user exceeds the specified time, an alert is displayed in Visor.
- + Define an email alert when attendance time is exceeded.

Access tab



The screenshot shows the same 'Zone 1' window, but with the 'Access' tab selected. It features two lists: 'Entries' and 'Exits'. In the 'Entries' list, 'Reader 1' is checked and 'Reader 2' is unchecked. In the 'Exits' list, 'Reader 1' is unchecked and 'Reader 2' is checked. 'OK' and 'Cancel' buttons are at the bottom right.

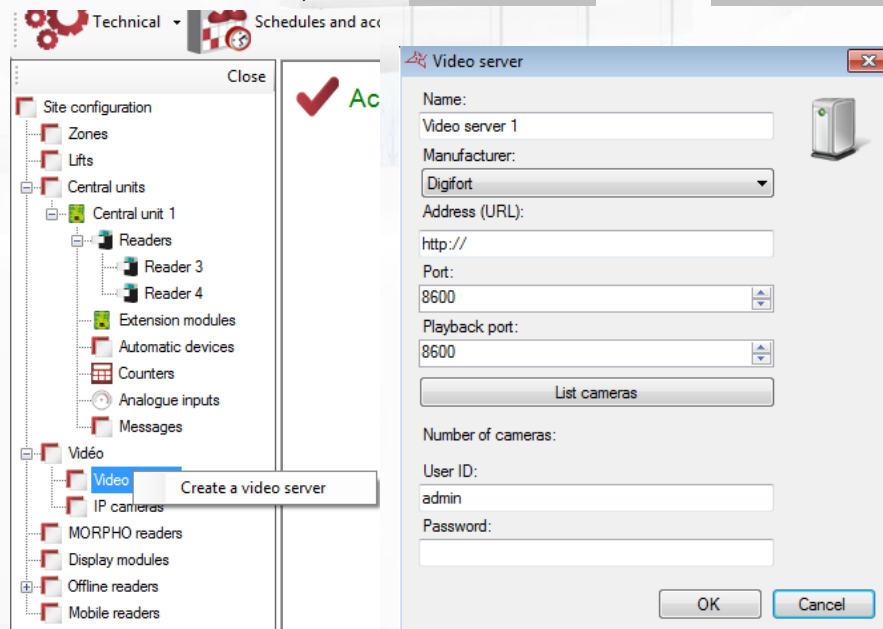
From this tab, you can select the readers as entry and exit of the zone.

You can also place an icon on the overview in order to see the number of people in each zone in real time.

VIDEO SERVERS

CREATING A VIDEO SERVER

To create a video server, click on "Video servers" and then "Create a video server" as follows:



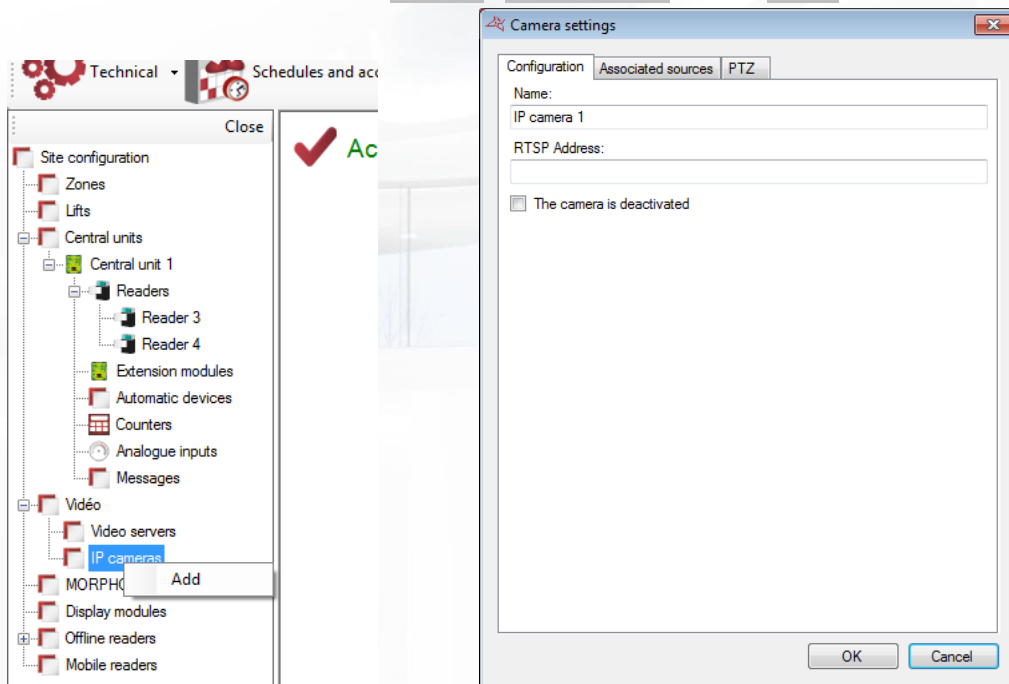
From this window, you can:

- + Name your server: enter the name in the "Name" field.
- + Choose the server manufacturer:
 - o DIGIFORT V7
 - o SAMSUNG
 - o DAHUA
 - o NUUO
 - o MILESTONE
 - o HIK
 - o GIGAMEDIA
- + Enter the server's address (URL).
- + Modify the port
- + Modify the port for video playback
- + Click on the "List cameras" button to detect all the cameras on the video server.
- + Enter the login for your server.
- + Enter the password.

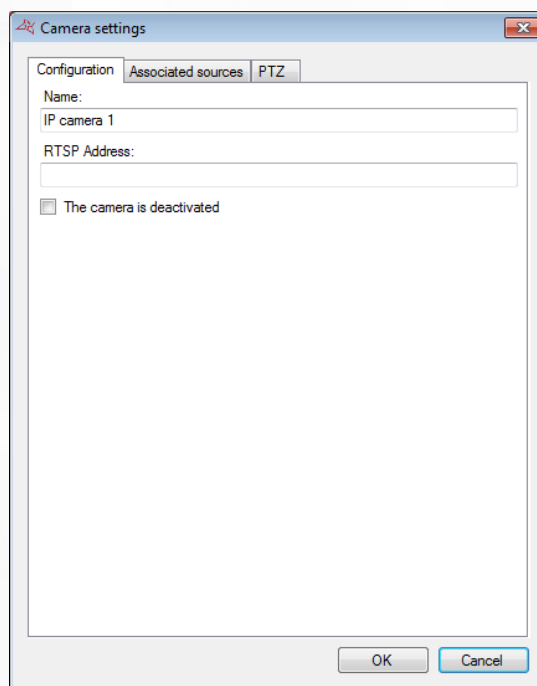
Then you will be able to view the cameras video from a shortcut or video matrices.

CREATE AN IP CAMERA

To create an IP camera, click on "Video" / "IP Cameras" then on "Add" as illustrated below



Configuration tab



From this tab, you can:

- + Select the name of the camera.
- + Specify an RTSP address for the camera.
- + Specify whether or not the camera is deactivated.

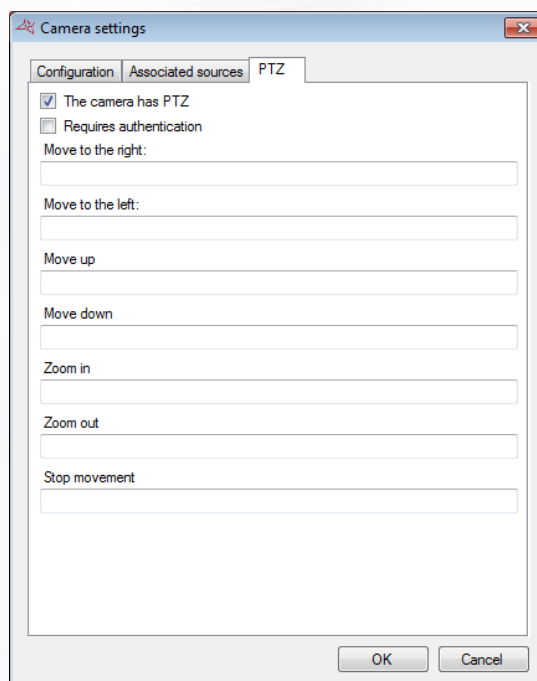
Associated Sources Tab



From this tab, you can:

- + Select the associated sources (readers, LPR readers, Groups intrusion and Zone intrusion) which will enable you to display the video from this camera for acquittal.

PTZ Tab

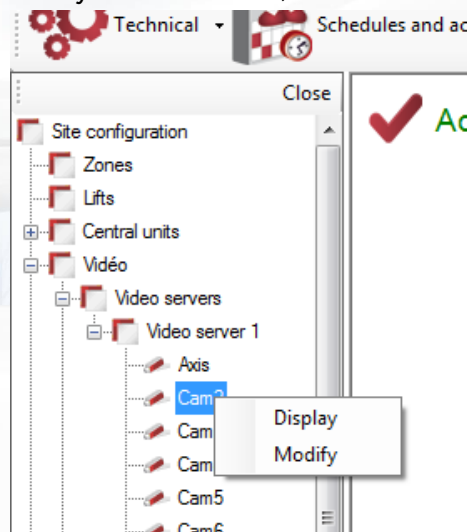


From this tab, you can:

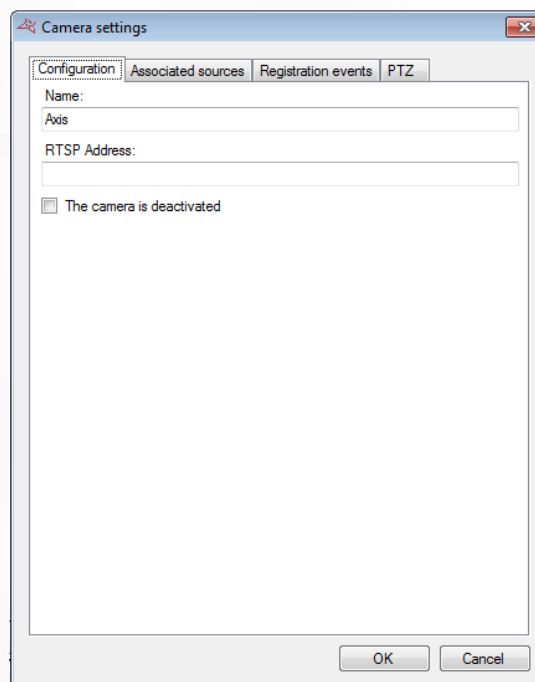
- + Define whether or not the camera handles the PTZ.
- + Specify whether an authentication is required to move the camera
- + Define the different RTSP channels required to move the camera

CAMERA SETTINGS

To configure a camera, click on "Modify" from a camera, as indicated below:



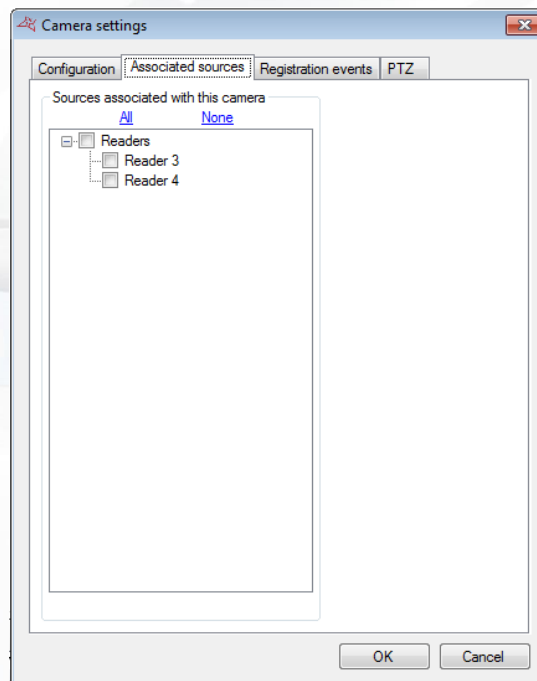
Configuration Tab



From this tab, you can:

- + Select the name of the camera.
- + Specify an RTSP address for the camera. This address will enable you to access the camera from the Smartphone App.
- + Specify whether or not the camera is deactivated.

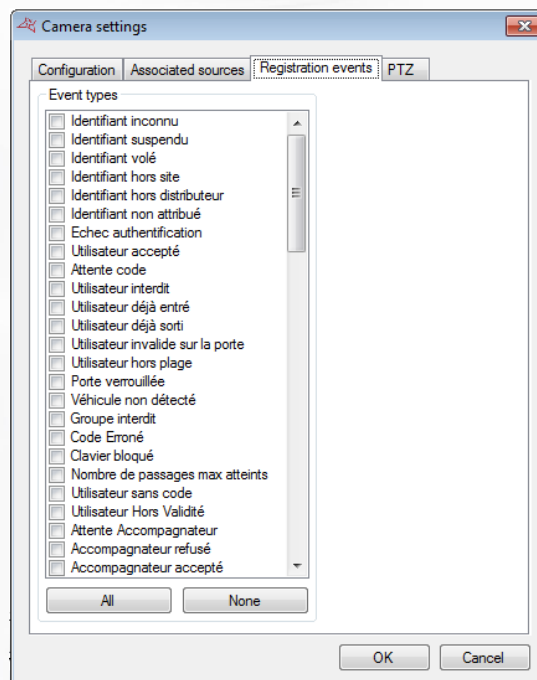
Associated Sources Tab



From this tab, you can:

- + Select the associated sources (readers, LPR readers, Groups intrusion and Zone intrusion) which will enable you to display the video from this camera for acquittal.

Registration Events Tab



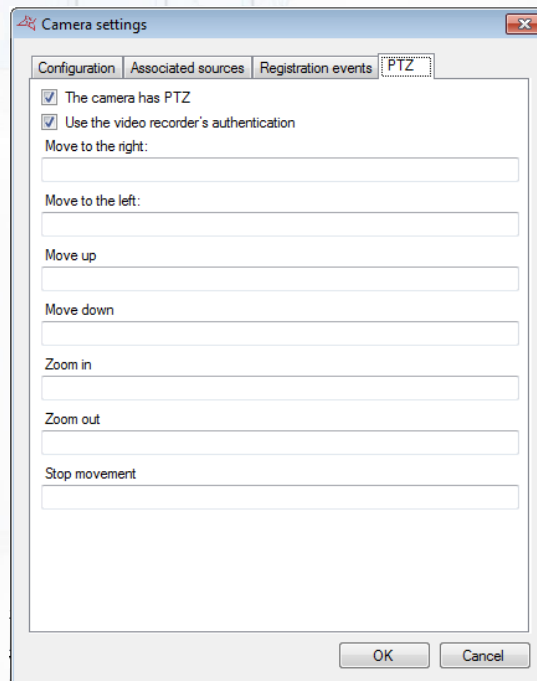
From this tab, you can:

- + Select one or more types of events for triggering the video.

To watch the video according to an event, display the list of events ("Events" then "See Events") and click the camera image in front of the desired event. A window will open and you will be able to watch the video.

Caution: this feature only allows to view a video from a recorder. DOMOS will never trigger the video recording on the recorder. This recorder will have to be configured accordingly (permanent recording, motion detection ...).

PTZ Tab

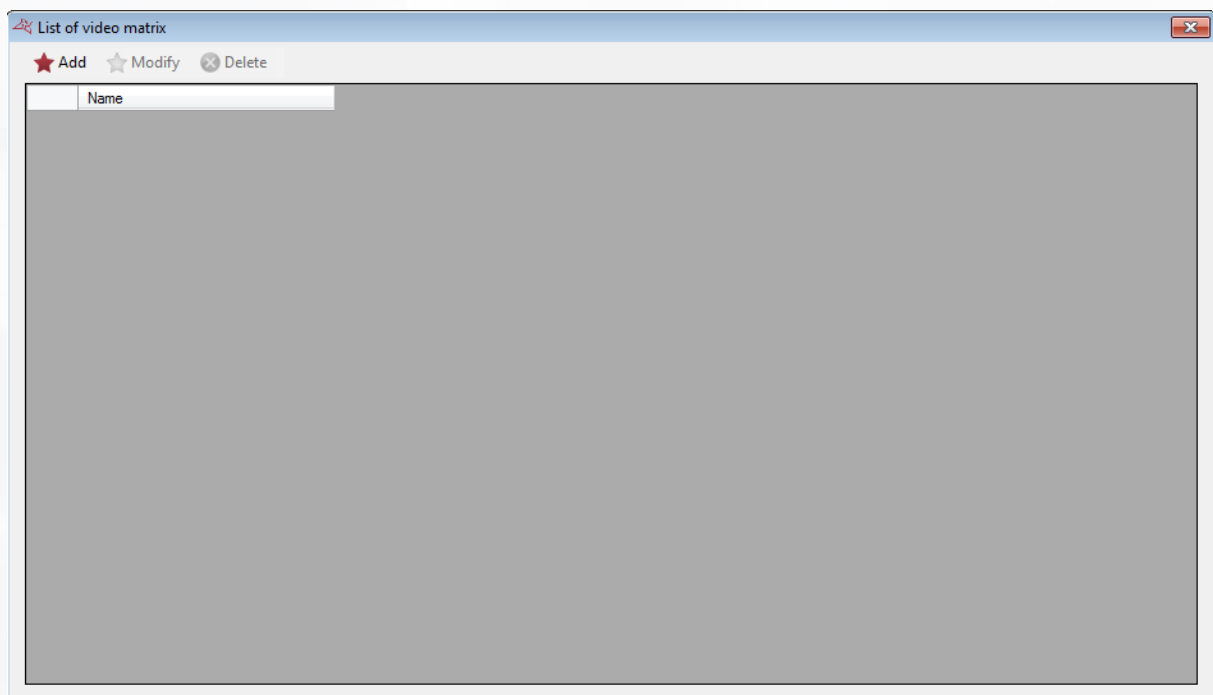
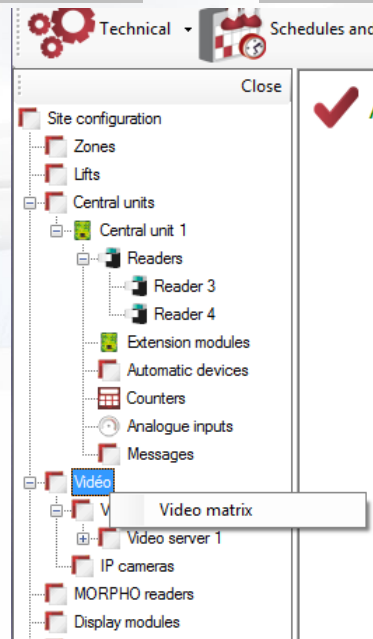


From this tab, you can:

- +** Define whether or not the camera handles the PTZ.
- +** Specify whether or not stocker authentication is required to move a camera in RTSP
- +** Define the different RTSP channels required to move the camera from the Smartphone App.

CREATING A VIDEO MATRIX

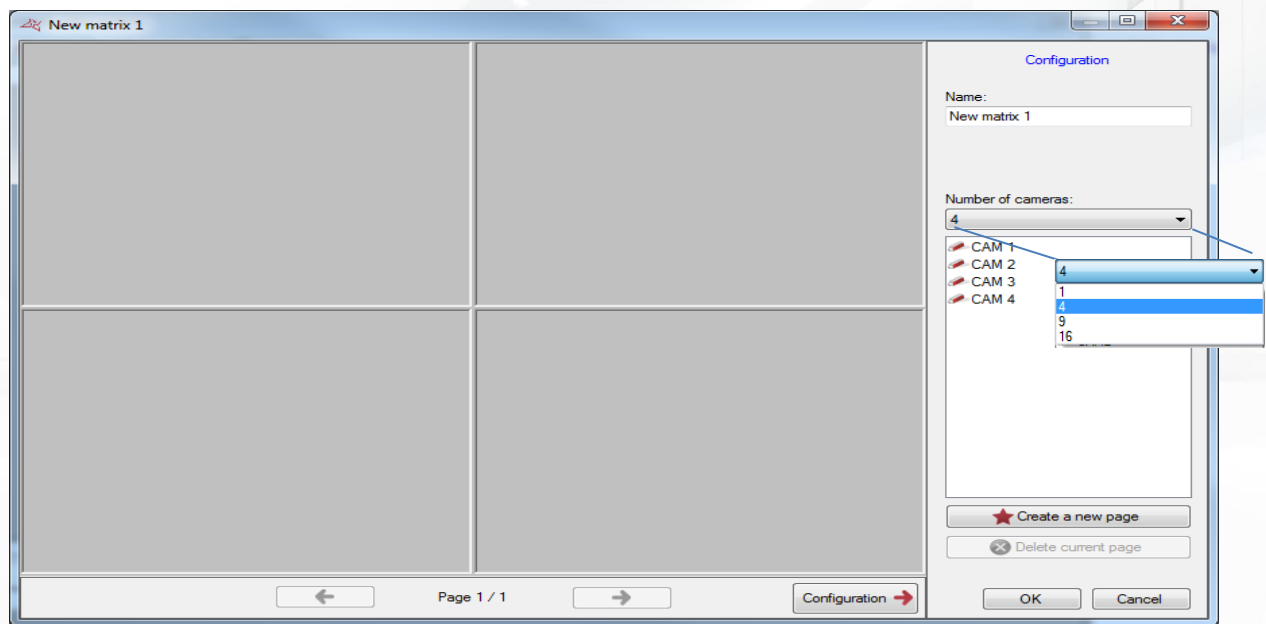
To create a video matrix, click "Video Servers" and then "Video Matrix" as follows:



From this window, you can:

- + Add a new matrix by clicking the "Add" button
- + Modify an existing matrix by selecting the desired matrix and clicking "Modify"
- + Delete an existing matrix by selecting the desired matrix and clicking "Delete"

Configuring a video matrix

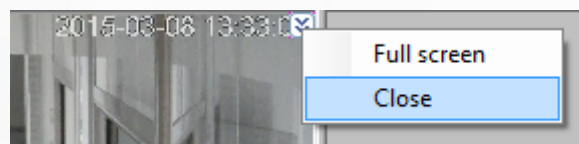


From this window, you can:

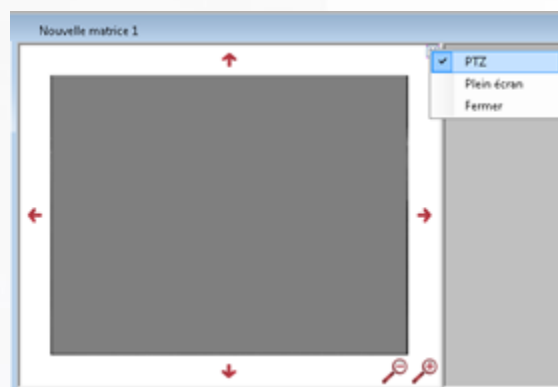
- + Give a name to your matrix
- + Change the number of cameras to display in the matrix (1, 4, 9 or 16)
- + Create or delete pages
- + Show or hide the configuration menu

To add a camera, select it in the right list and drag it into an available slot (gray rectangle).

To remove a camera from the current page, click the button on the camera top right corner and then click "Close" as follows:



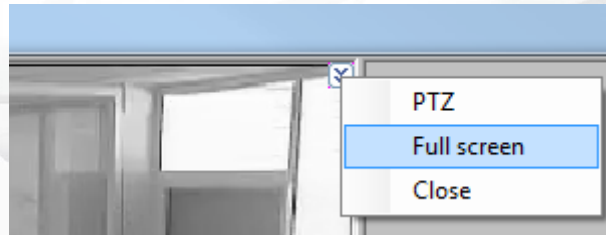
If your camera is motorized, click the button on the camera top right corner, then click "PTZ" as follows:



Then use the arrow and magnifiers to control your camera.

To hide the controls of the camera, click again on the button in the upper right corner, then click "PTZ".

To view a camera in full screen, click the button in the upper right corner of the camera and click "Full Screen" as follows:

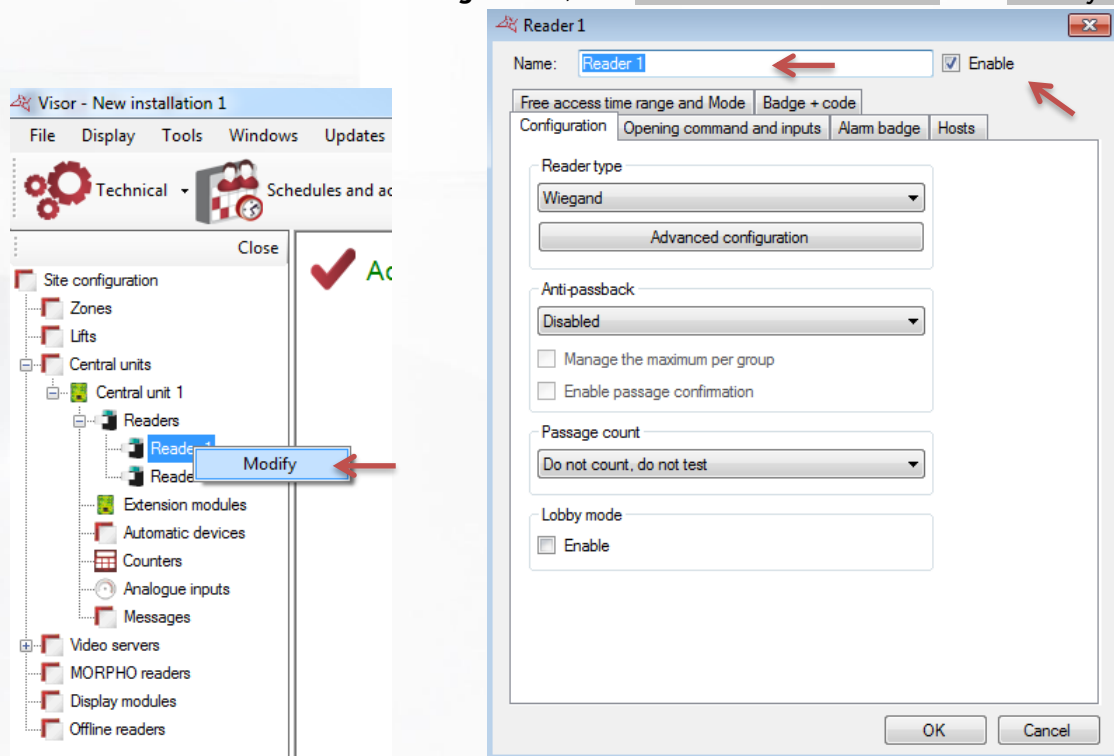


To return to the normal display, click again on the button in the upper right corner and click "Full Screen".

Tip: You can use a shortcut to display your matrix.

CONFIGURING A CENTRAL UNIT READER

From the **Technical** menu then **Site configuration**, click on the central unit reader then "Modify":



From this window, you can:

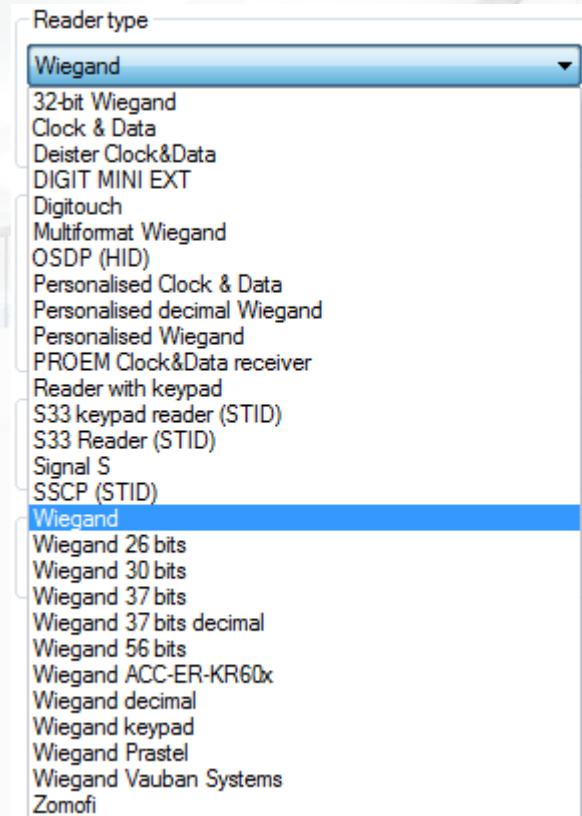
- + Name your reader: enter the name in the "Name" field.
- + Disable the reader (it will no longer be taken into account in the calculation of the license).

Configuration tab

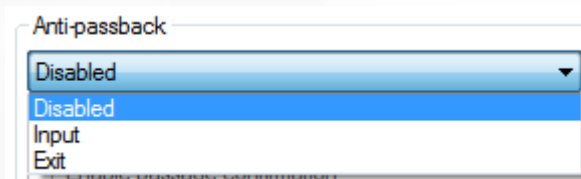
In the Configuration tab, you can:

+ Choose the Type of reader:

- Clock & Data
- Personalised Clock & Data
- Deister Clock&Data
- DIGIT MINI EXT
- Digitouch
- OSDP (HID)
- Personalised Clock & Data
- Personalised decimal Wiegand
- Personalised Wiegand
- PROEM Clock&Data receiver
- Reader with keypad (HID RK40)
- S33 keypad reader (STID)
- S33 reader (STID)
- Signal S
- SSCP (STID)
- Wiegand
- Wiegand 26 bits
- Wiegand 30 bits
- 32-bit Wiegand
- Wiegand 37 bits
- Wiegand 37 bits decimal
- Wiegand 56 bits
- Multiformat Wiegand
- Wiegand ACC-ER-KR60x
- Wiegand decimal
- Wiegand keypad
- Wiegand Prastel
- Wiegand Vauban Systems
- Zomofi



+ Enable the Anti-passback function by selecting the reader either as an "Input" or an "Output".



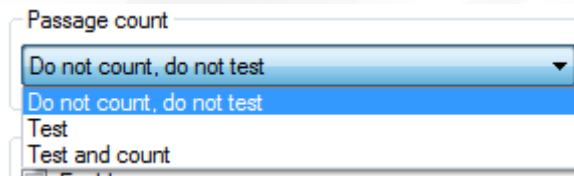
Check the "Manage the maximum per group" box if you wish to restrict the number of users per access group for a given reader. The maximum number is specified in the group - refer to the chapter entitled "Managing access groups".

Enable passage confirmation to validate when users operate a reader. To use this function, the "Door contact" input must be connected to a door contact and the parameter for the input must also be enabled; refer to the "Opening command and inputs" tab.

+ Enable the passage count function. You can select:

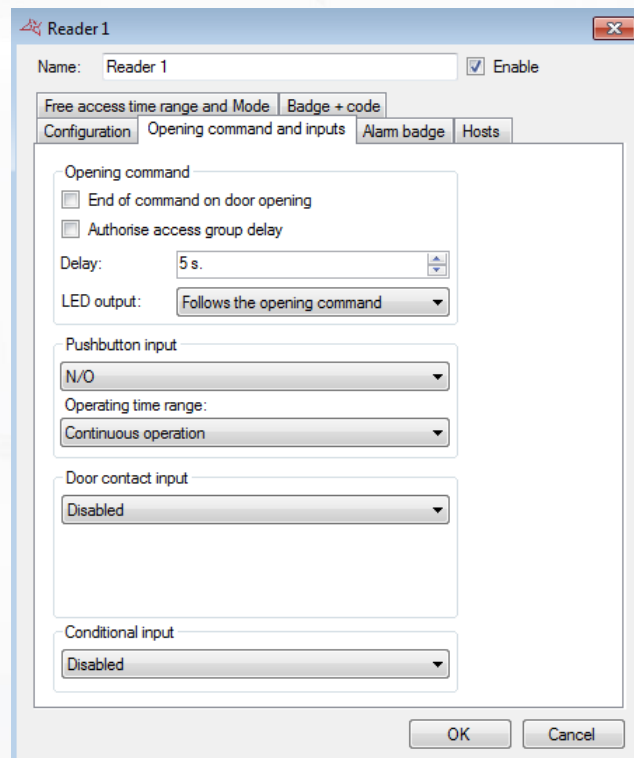
- Test: used to test the number of times that a user has operated a reader without counting and block the user if the reader is equal to 0.

- Test and count: used to test the number of times that a user has operated a reader by counting and block the user if the reader is equal to 0.



- + Enable Lobby mode: used to integrate a reader into a lobby. Only one of the readers belonging to the lobby can be enabled at any one time.

Opening command and inputs tab



From this tab, you can:

+ Configure the Opening command.

- If you check the "End of command on door opening" box (a door contact needs to be connected to the central unit's "Door Contact" input), the relay command will be disabled when the door is opened or the time delay expires.
- If you check the "Authorise access group delay" box, the reader's relay command delay will correspond to the delay specified in the group, which is practical if the time required for a user to operate a reader is long.
- The relay command delay is from 1 to 255 seconds. If you set the value to less than 1, you will switch to **Bistable** command mode (the relay status is reversed for each user accepted or each press of the pushbutton).
- The LED output (generally used to control the reader's LED) may follow the:
 - Opening command (status of the command relay).
 - Door state (status of the "Door contact" input).
 - Opening command and door status (statuses of the command relay and "Door contact" input).

+ Configure the Pushbutton input.

You can choose:

- Between a NO or NC contact.
- Continuous operation or a predefined time range.

Pushbutton input

N/O

Operating time range:

Continuous operation

+ Configure the Door contact input.

You can choose:

- Between a NO or NC contact.
- The blocked door delay function creates a blocked door event in VISOR if the door is not closed within the predefined time.

Door contact input

N/O

Blocked door delay:

Disabled

+ Configure the Conditional input.

You choose:

- NO or NC vehicle detection
When a badge is swiped at the reader, a vehicle must be detected to confirm the opening command.
- NO or NC alarm in service
When a badge is swiped at the reader, users will be refused entry unless they have been assigned the alarm management authorisation.
- Glass break monitoring green NO or NC
This will create a simple event in VISOR for enabling or disabling the break-glass functionality.

Conditional input

Disabled

Disabled

N/O vehicle detection

N/C vehicle detection

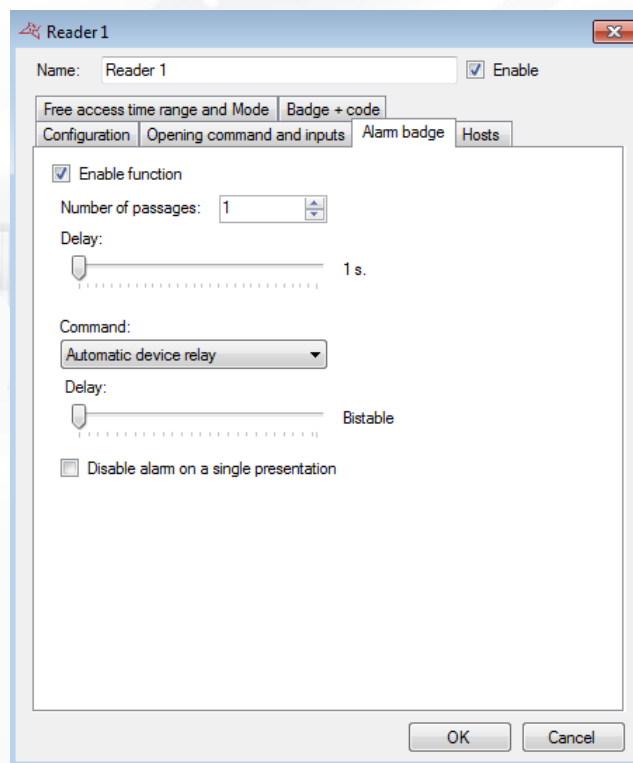
N/O alarm in service

N/C alarm in service

Glass break monitoring green N/O

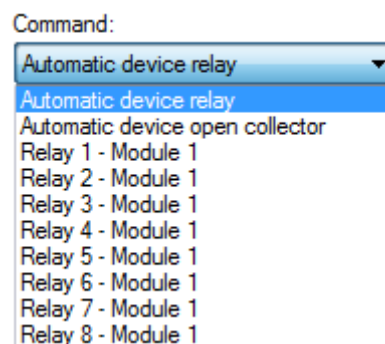
Glass break monitoring green N/C

Alarm badge tab



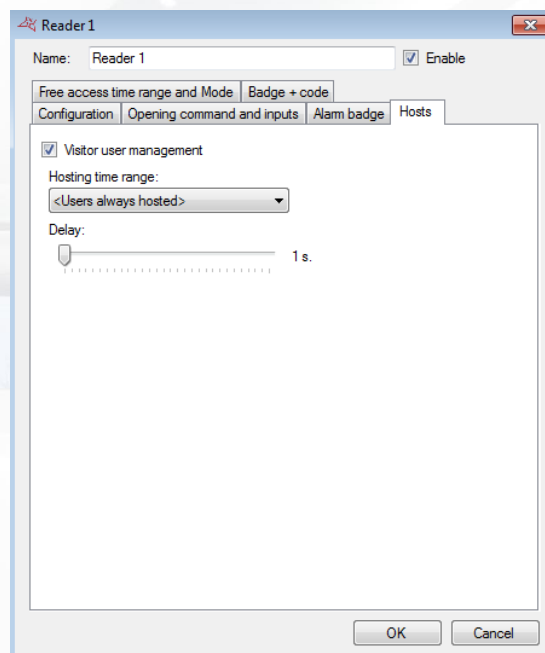
From this tab, you can:

- + Enable the "Alarm badge" function.
- + Enter the number of passages (between 1 and 10) for the badge at the reader to enable the alarm.
- + Specify a delay to reach the number of passages required to enable the alarm.
- + Choose the command:
 - o By the Automatic device relay.
 - o By the Automatic device open collector output.
 - o By a V-EXTIO module relay.



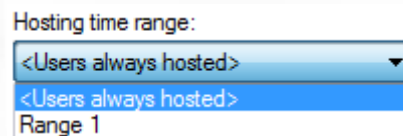
- + Set the bistable or pulse command delay to a value between 1 and 255 seconds.

Hosts tab



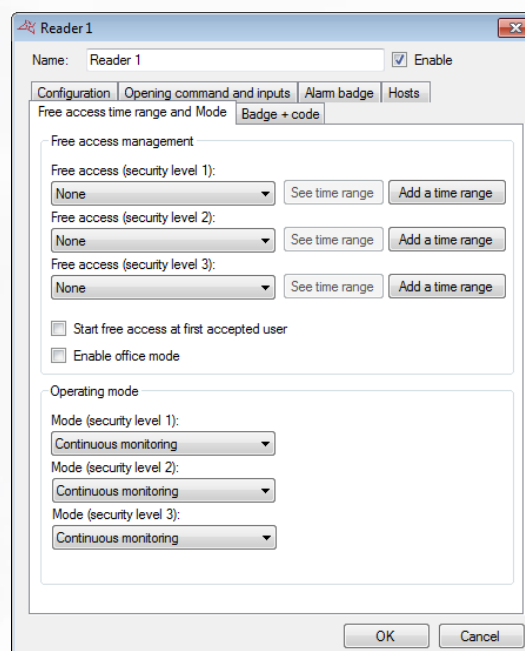
From this tab, you can:

- + Enable the visitor user management function.
- + Select a predefined hosting time range.



- + Set a delay for waiting for the host after the visitor user.

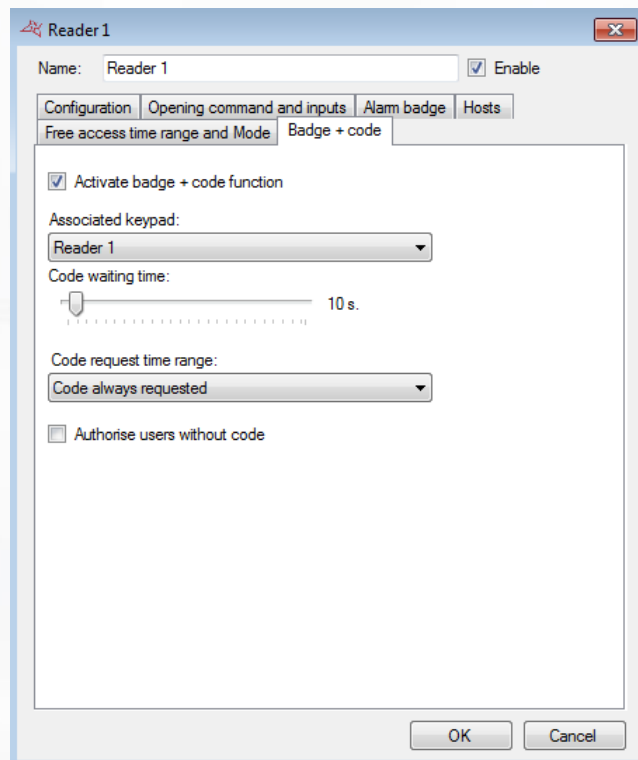
Free access time range and Mode



From this tab, you can:

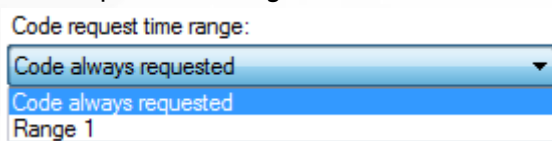
- + Set the free access range for each security level
 - Select <Permanent control> to apply no free access to the reader
 - Select a time range so that the reader will remain opened until the selected range will remained active
 - Click "Add a time Range" to create a new time range
 - Click "See time range" to edit the selected time
- + Start free access at the first accepted user.
- + Enable office mode
- + Select the operating mode for 3 security levels
 - Either continuous monitoring, or
 - Opening maintained, or
 - Closure maintained.

Badge + Code tab



From this tab, you can:

- + Enable the badge + code function.
- + Select the keypad associated with the reader.
- + Set a delay for the code waiting time (between 1 and 255 seconds) after a badge is swiped at the reader.
- + Enter a predefined code request time range.



- + Authorise users without a code.

Autinor lifts tab

Note: This tab only requires one declared Autinor lift to be displayed (see Managing Autinor lifts)

The screenshot shows a configuration window titled 'Lecteur 1'. It has several tabs: 'Configuration', 'Opening command and inputs', 'Alarm badge', 'Hosts', 'Free access time range and Mode', 'Badge + code', and 'Autinor lifts'. The 'Autinor lifts' tab is selected. Inside this tab, there is a checkbox labeled 'Controlling an Autinor lift' which is checked. Below this, there are three fields: 'Autinor lift' with a dropdown menu showing 'Lift Autinor 1', 'Lift floor' with a dropdown menu showing 'R-1', and 'Reader order (indicates its position in the corridor)' with a numeric input field showing '0'. At the bottom right of the window are 'OK' and 'Cancel' buttons.

Via this tab, you can:

- + Specify whether the reader controls an Autinor lift.
- + Choose the Autinor lift controlled by the reader.
- + Choose the floor where the reader is located.
- + Choose the order of the reader corresponding to its position in the corridor.

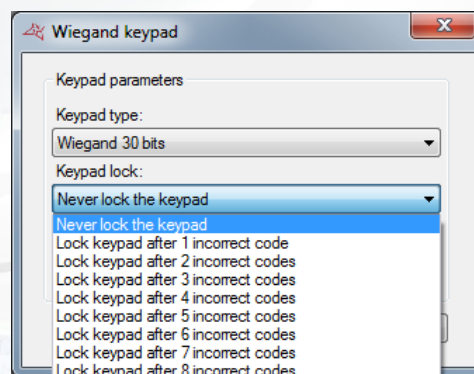
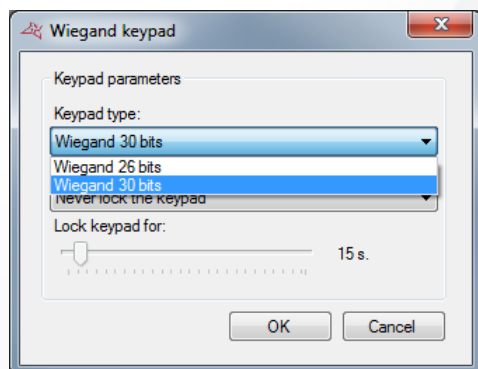
ADVANCED READER PARAMETERS

Depending on the type of reader selected, you can apply advanced settings to the reader.

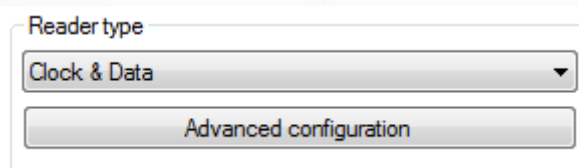
WIEGAND KEYPAD

The screenshot shows a dialog box for 'Wiegand keypad' configuration. It has a 'Reader type' dropdown menu with 'Wiegand keypad' selected. Below the dropdown is an 'Advanced configuration' button.

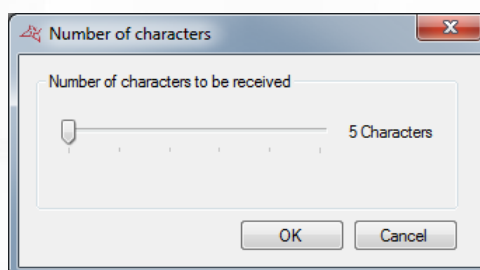
From the advanced configuration, you can choose the type of keypad (Wiegand 26 or 30 bits) and set the keypad lock (from 1 to 255 seconds) depending on the number of incorrect codes.



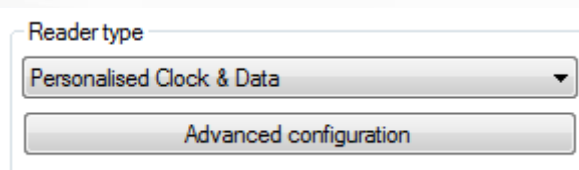
CLOCK & DATA READER



From the advanced configuration, you can configure the number of read characters (5 to 10 characters).

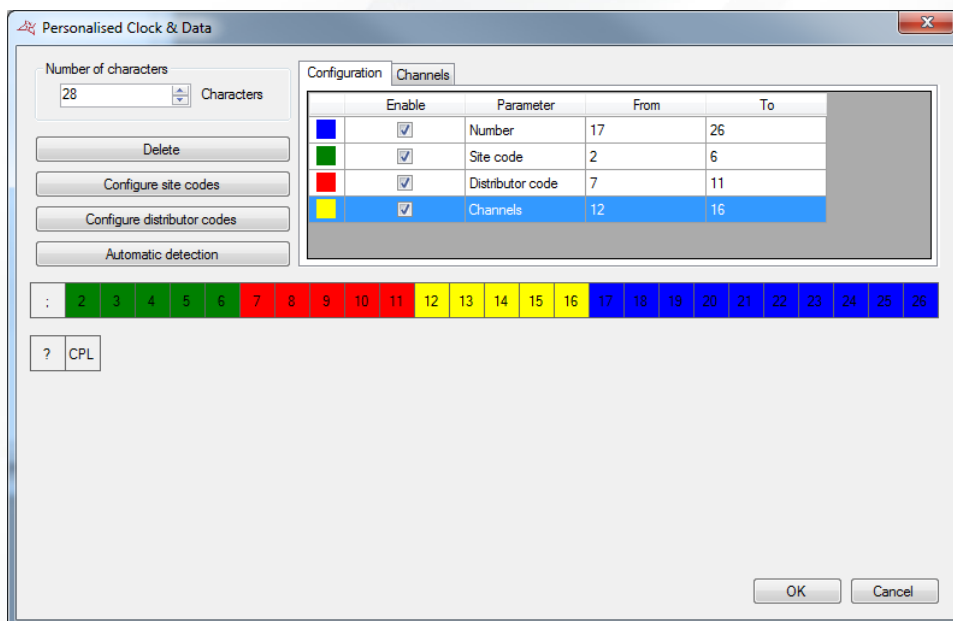


PERSONALISED CLOCK & DATA



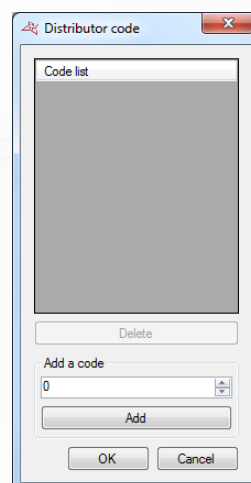
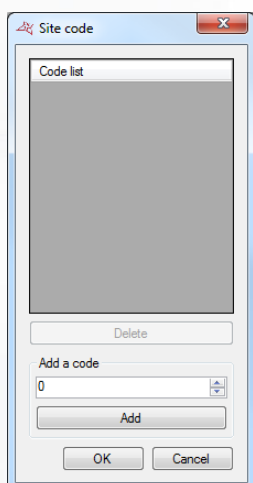
In the advanced configuration, choose the number of characters returned by the reader (10 to 128 characters) and then enter the following parameters:

- + Number: location and size of the badge number read (maximum of 10 characters).
- + Site code: location and size of the site code (maximum of 5 characters).
- + Distributor code: location and size of the distributor code (maximum of 5 characters).
- + Channels: location and size of the channels (maximum of 5 characters) for the radio emitters.

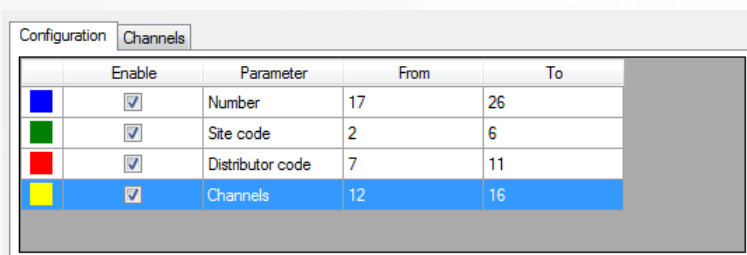


By clicking on "Configure site codes", you can add authorized site codes:

By clicking on "Configure distributor codes", you can add authorized distributor codes:



To configure each item, select them in the list and then check the corresponding box in the "Enable" column. Finally, in the frame, click on each character concerned. Caution: characters for the same item must be consecutive.



In the **Channels** tab, you can choose the value of each channel for each reader (between 0 and 255).

By clicking on "Automatic detection", you can automatically search for the area containing the badge number in the frame received from the reader.

To start the search, enter the badge number to be read by the central unit and then click on "Start". You will then have 15 seconds to present the badge at the selected reader.

If a match is found between the number entered and the number read, after clicking on "OK", the reader type will automatically be configured.

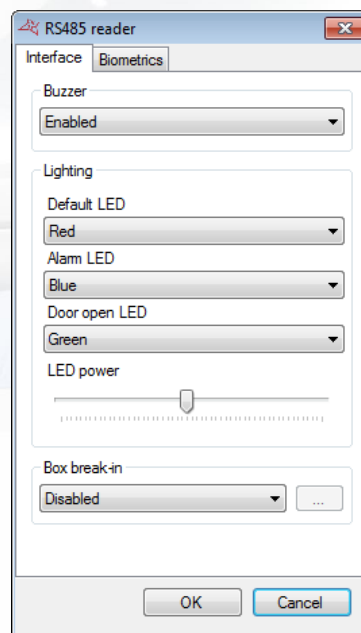
DEISTER CLOCK & DATA READER

The configuration procedure is the same as for a personalised Clock & Data reader.

DIGIT MINI EXT READER

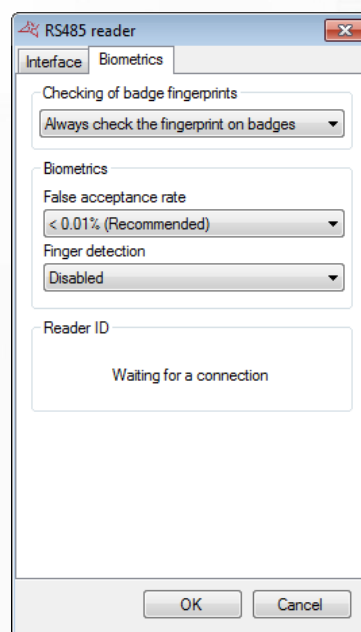
From the advanced configuration, you can:

Interface Tab:



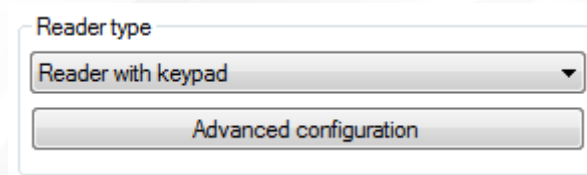
- + Activate or disable Buzzer.
- + Select colours and lighting levels
- + Define box intrusion detection values.

Biometrics Tab:

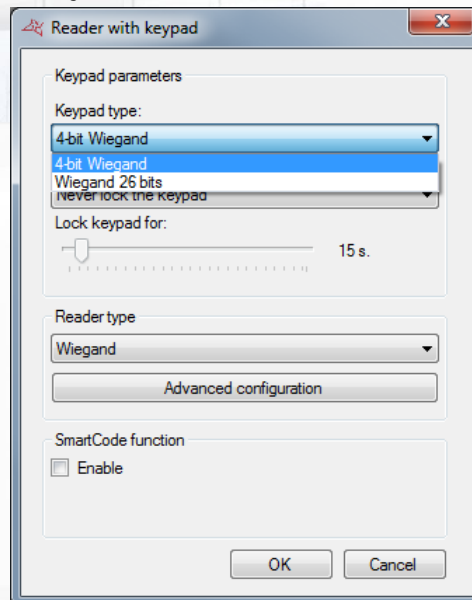


- + Define when biometric prints on cards should be checked
- + Define biometric sensitivity
- + Reset reader ID in the event of a replacement.

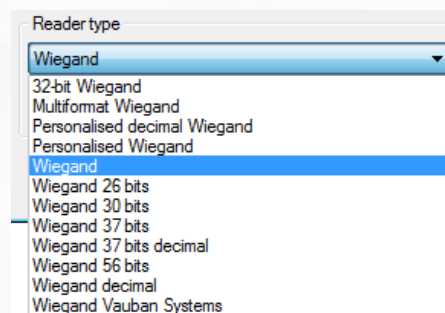
READER WITH KEYPAD (HID RK40 OR OTHER EQUIVALENT PRODUCT)



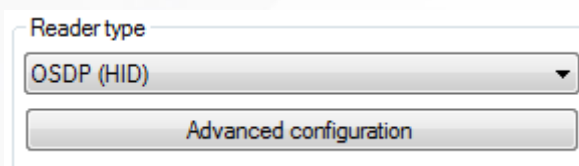
From the advanced configuration, you can:



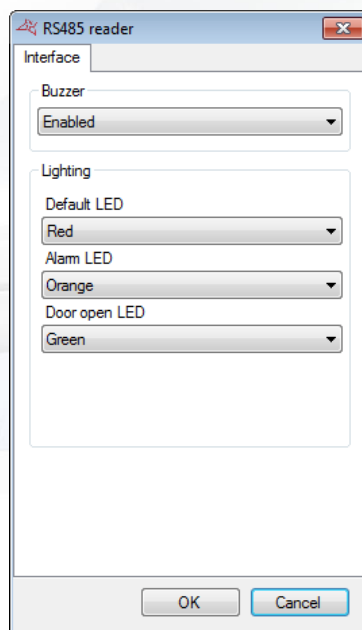
- + Select the type of keypad: 4 or 26-bit Wiegand.
- + Lock the keypad for 1 to 255 seconds following 1 to 10 incorrect codes.
- + Select the type of reader



OSDP READER (HID)

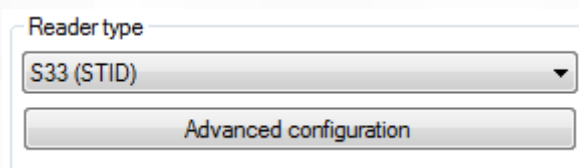


From the advanced configuration panel, you can:



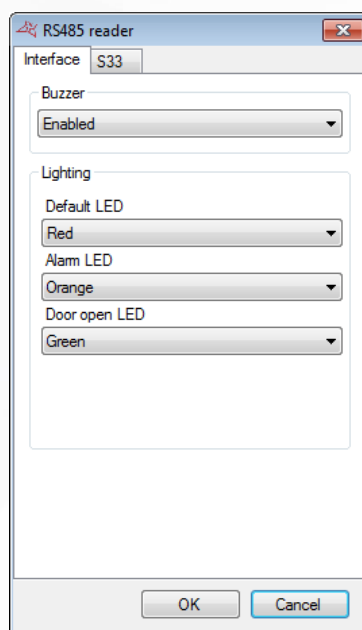
- + Activate or disable Buzzer.
- + Select colours and lighting

S33 READER (STID)



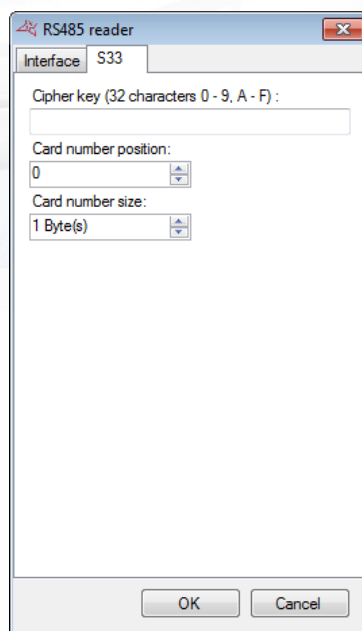
From the advanced configuration panel, you can:

Interface Tab



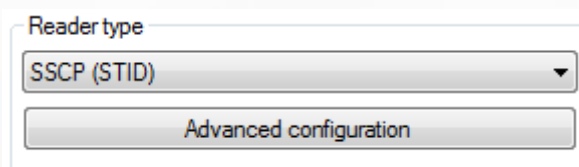
- + Activate or disable Buzzer.
- + Select colours and lighting levels

S33 tab



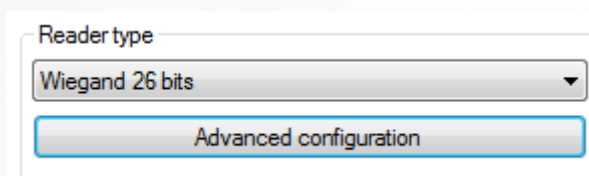
- + Specify encryption key
- + Specify position of card number
- + Define card number size

SSCP READER (STID)

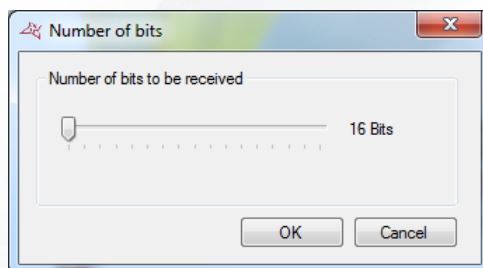


The configuration mode is identical to that of the OSDP reader (HID).

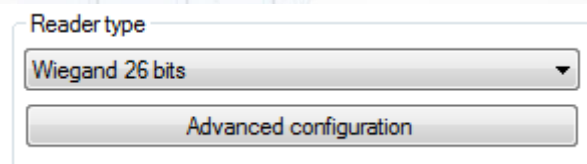
WIEGAND READER



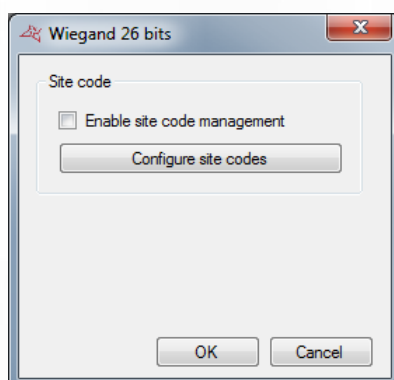
In the advanced configuration, you can choose the number of bits to be received by the central unit (16 to 32 bits).



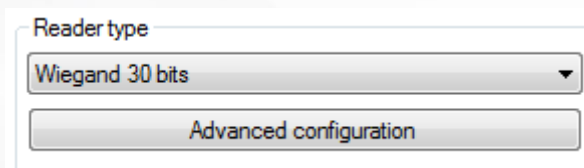
26 BITS WIEGAND READER



From the advanced configuration, you can enable the site code management function. Click on **"Configure site codes"** to add the authorised site codes.

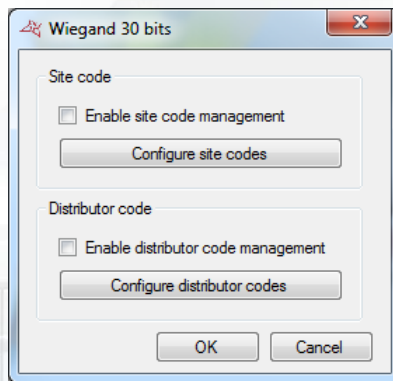


30 BITS WIEGAND READER

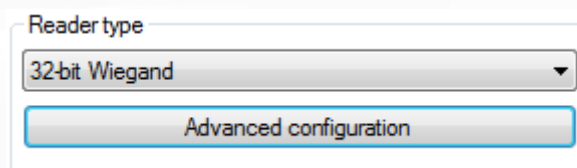


In the advanced configuration, you can:

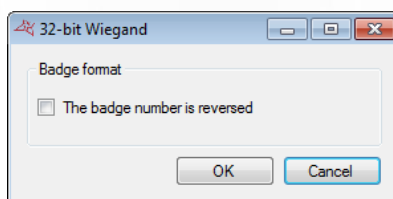
- +** Enable the site code management function. Click on **"Configure site codes"** to add the authorised site codes.
- +** Enable the distributor code management function. Click on **"Configure distributor codes"** to add the authorised distributor codes.



WIEGAND READER 32 BITS

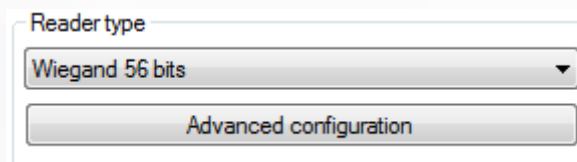


From the advanced configuration panel, you can reverse the badge number.

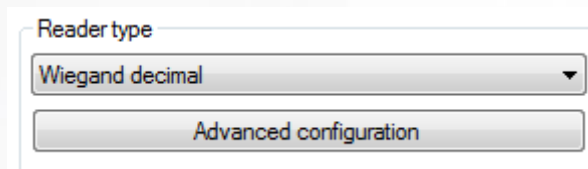


WIEGAND READER 56 BITS

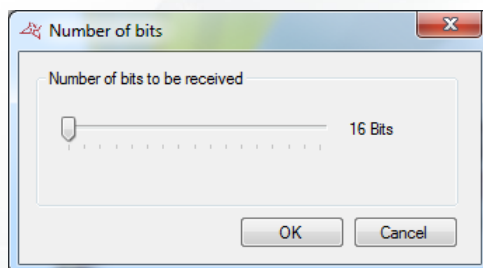
The configuration mode is identical to that of the 32-bit reader.



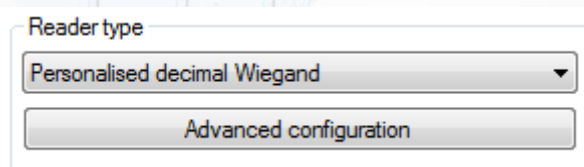
WIEGAND DECIMAL READER



In the advanced configuration, you can choose the number of bits to be received by the central unit (16 to 32 bits).



PERSONALISED DECIMAL WIEGAND

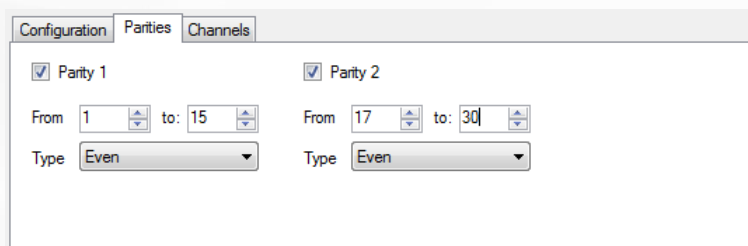


In the advanced configuration, choose the number of bits returned by the reader (16 to 128 bits) and then enter the following parameters:

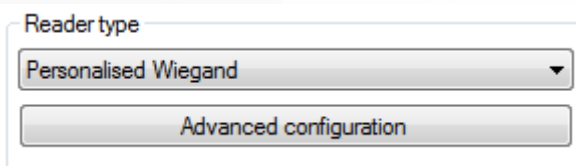
- + Number: location and size of the badge number read (maximum of 32 bits).
- + Site code: location and size of the site code (maximum of 16 bits).
- + Distributor code: location and size of the distributor code (maximum of 16 bits).
- + Channels: location and size of the channels (maximum of 16 bits) for the radio emitters.

You can also:

- + Configure the authorised site codes.
- + Configure the authorised distributor codes.
- + Perform an automatic detection.
- + Configure the channels for each reader.
- + Configure the parities as follows:

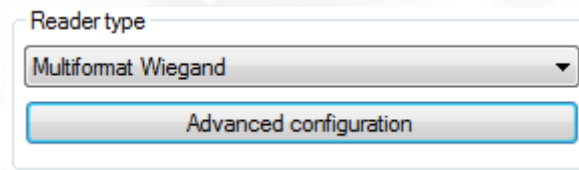


PERSONALISED WIEGAND

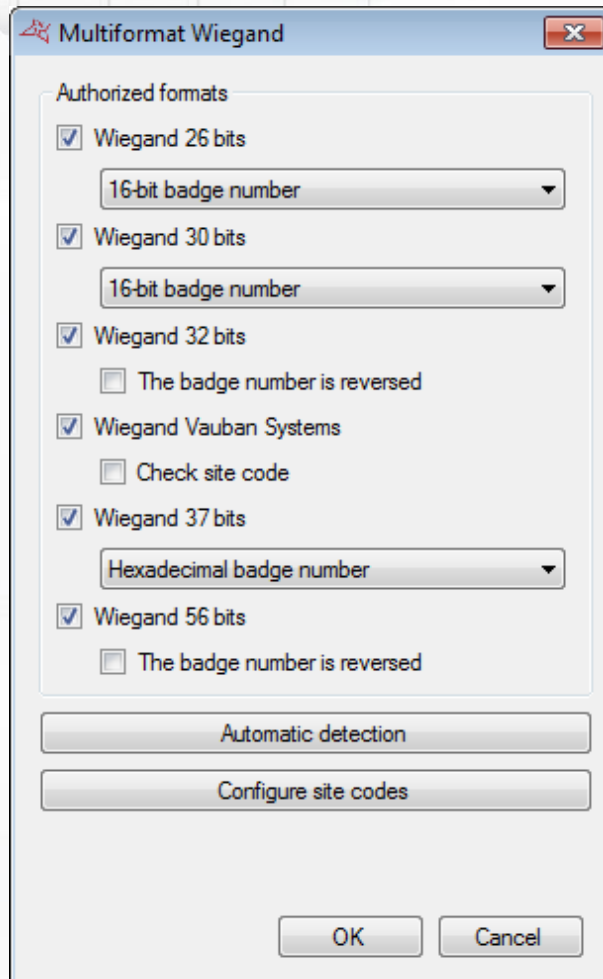


The configuration is the same as for a personalised decimal Wiegand reader.

MULTIFORMAT WIEGAND READER



From the advanced configuration panel, you can choose the formats that will be authorized on the reader, as well as the related site codes



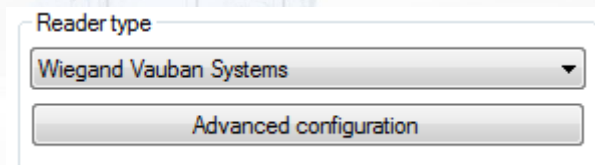
The different authorized formats are:

- +** Wiegand 26 bits
 - 16-bit badge number
 - 16-bit badge number, with site code
 - 24-bit badge number
- +** Wiegand 30 bits
 - 16-bit badge number
 - 16-bit badge number, with site code
 - Prastel format
- +** Wiegand 32 bits
 - Activate or not the reversal of the badge number
- +** Wiegand Vauban Systems
 - Activate or not the verification of the site code
- +** Wiegand 37 bits

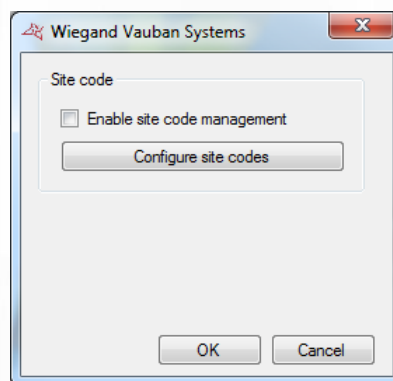
- Hexadecimal badge number
- Decimal badge number
- + Wiegand 56 bits
 - Activate or not the reversal of the badge number

By clicking on "Auto Detect", you can automatically search for the format of the badge presented in front of the reader.

WIEGAND VAUBAN SYSTEMS READER

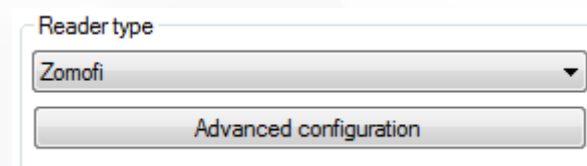


In the advanced configuration, you can enable the site code management function. Click on "Configure site codes" to add the authorised site codes.

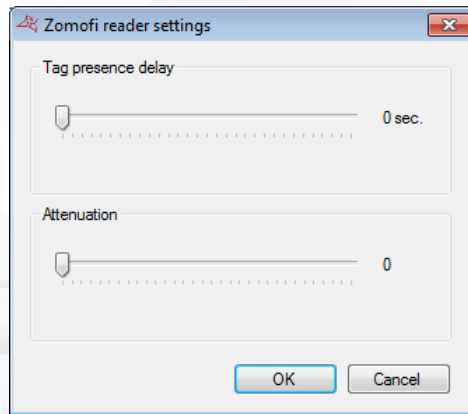


Note: this type of reader is dedicated to the HID iClass® readers associated with HID badges.

ZOMOFI READER



From the advanced settings, you can:

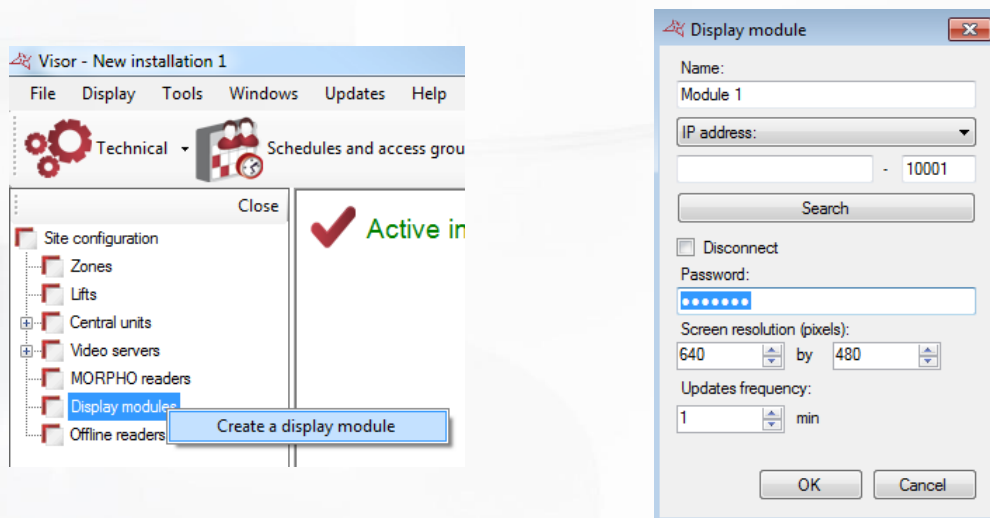


- + Select tag timeout
- + Select attenuation value

DISPLAY MODULES MANAGEMENT

These modules allow you to display information on a screen. A HDMI connection is mandatory on the screen.

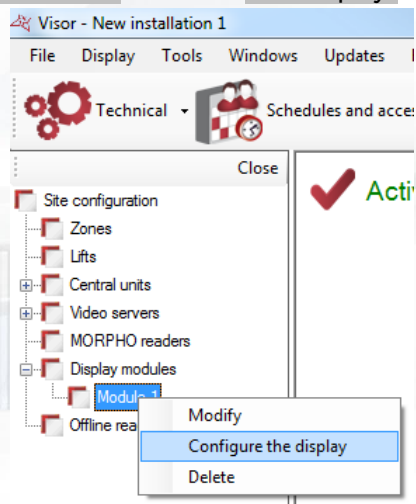
To add a new module, click "Display modules" and then "Create a display module" as follows:



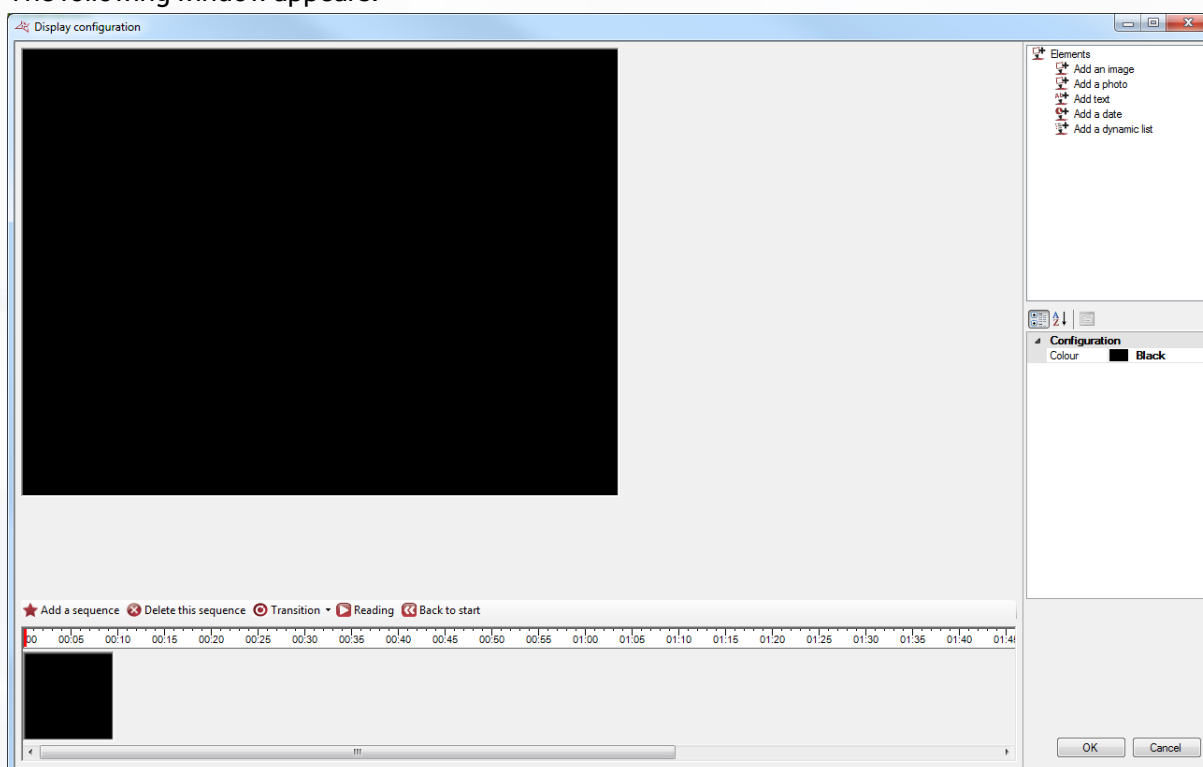
From this window, you can:

- + Give a name to your module, type it in the "Name" field
- + Configure the IP address or DNS address of your module
- + Search your module on the network
- + Disconnect the module: stops all communication with the module.
- + Set a password: the password is used to prevent access to the module's configuration by another computer
- + Set the resolution of the screen connected to the module (in pixels)
- + Configure the update frequency (from 1 to 65535 minutes) if you display dynamic lists (eg past events, present list ...)

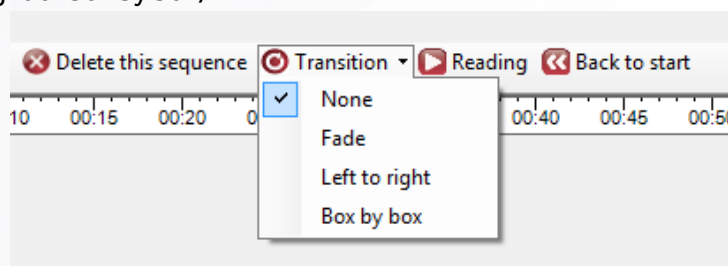
To configure the display, click **your module** then click "Set display" as follows:



The following window appears:



It is possible to add several sequences, configure each display time as well as each mode of transition (fade from left to right or box by box).



For each sequence, you can:

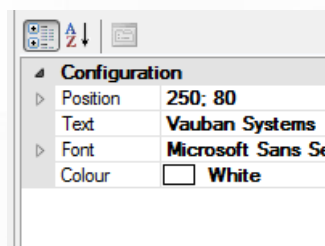
- +** Change the time: Present the mouse cursor over the right edge of the preview until a double arrow appears. Then move the mouse to the desired length.



- + Add a text
- + Add a date and time
- + Add a picture (example: display the logo of the company)
- + Add a user's picture (example: wish a colleague birthday)
- + Display the result of SQL query on the database (examples: last events, list of user present in a zone, personalized query without any limitation). **Caution:** if you use this type of display, VISOR will manage the update of the displayed datas. In this case, ensure VISOR will always run on your computer.

To add an item, select it in the list on the right and drag it on the sequence.
You can move an item in the sequence by clicking on it and then moving the mouse over the sequence.

To configure an item, select it on the sequence and then change its settings from the list on the right bottom of the window.



To remove an item, change the display order, or change the alignment, **right-click the item** and **click the desired**.

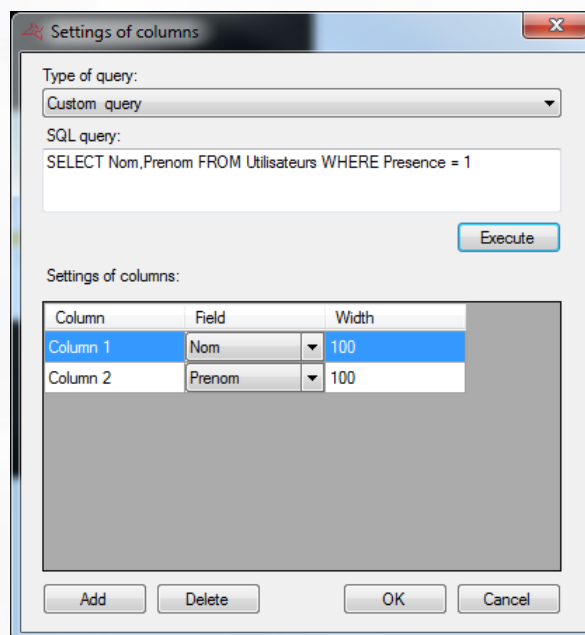
Please note that the updated data from the dynamic lists will be managed by VISOR. In this case, make sure VISOR is constantly running on your computer.
Using the Windows service is highly recommended in this case.

Example of sequence:

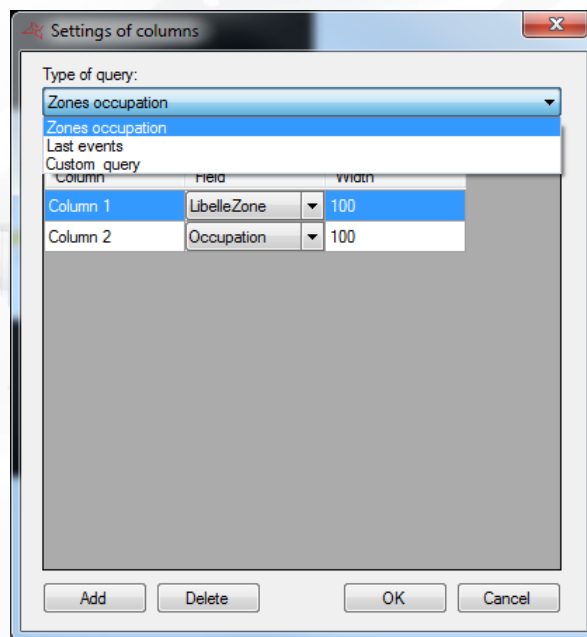


Example of personalised query:

Personalised SQL query:



Pre-parametered query:



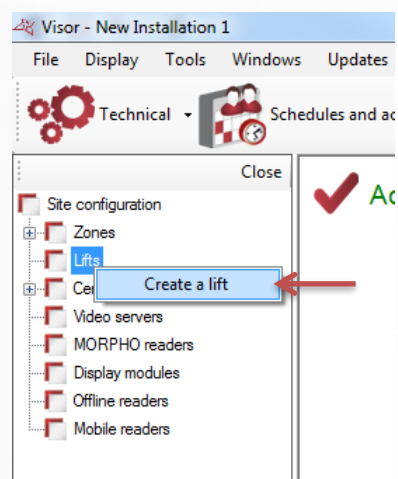
Please note that the updated data from these dynamic lists will be managed by VISOR. In this case, make sure VISOR is constantly running on your computer.

Using the Windows service is highly recommended in this case.

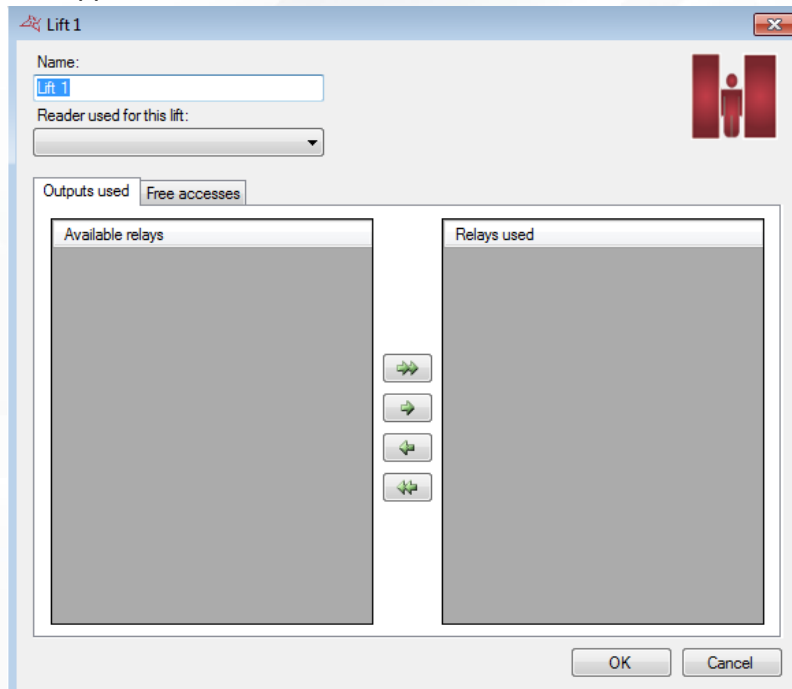
LIFTS MANAGEMENT

The lifts are managed by the V-EXTIO extension modules. These must be declared before you can set up your lifts.

To add a lift, click "Lifts" and then "Create a lift" as follows:

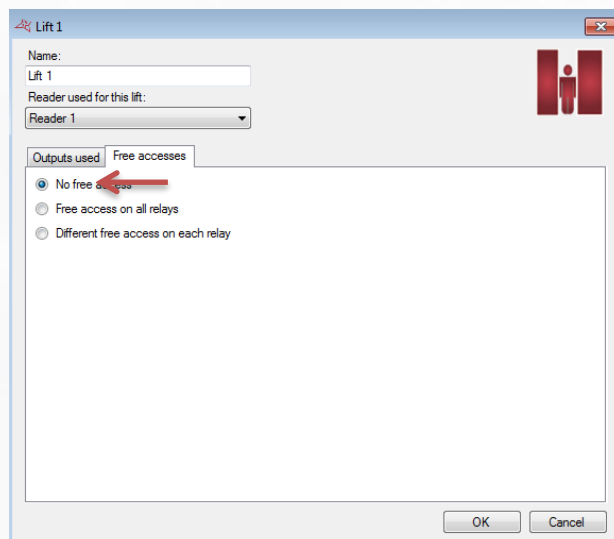


The following window appears:

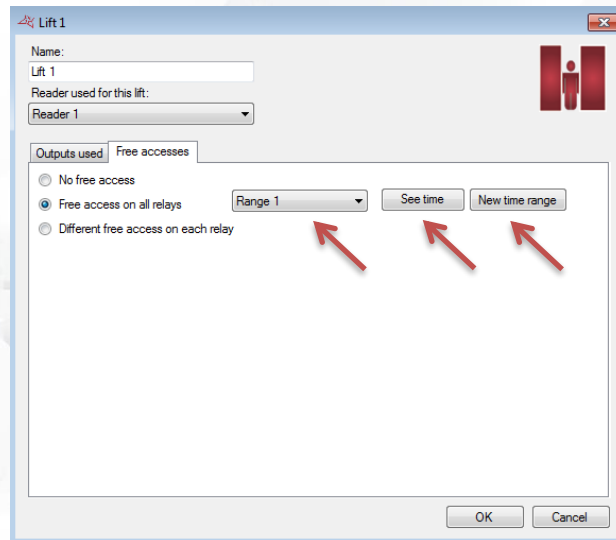


From this window, you can:

- + Give a name to your lift: type it in the "Name" field
- + Select the reader associated to the lift
- + From the "Outputs used" tab, select the relay that will be used to activate the buttons in the lift: use the arrows for it
- + From the "free accesses" tab, set the free access to each floor as follows:
 - o **No free access:** the floors will only be released when a user is accepted

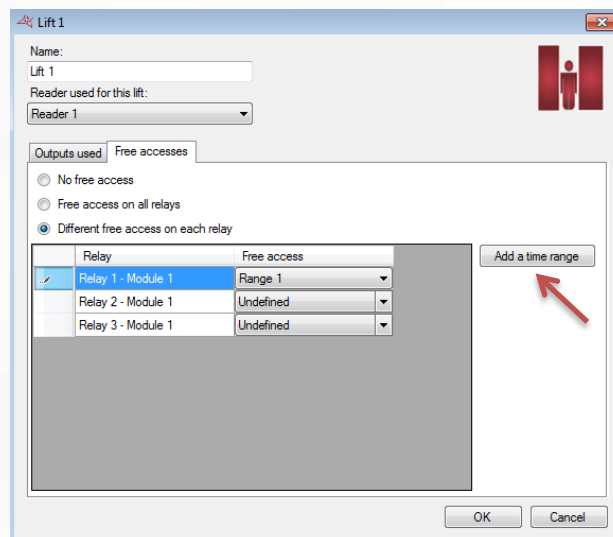


- o **Free access on all relays:** the floors will be released until the selected time range will remain active.



Also you can edit the selected time range by clicking **"See time"** or add a new time range by clicking **"New time range"**.

- **Different free access on each relay:** you can set a free access time range for each floor.



Also you can add a new time range by clicking **"Add time range"**.

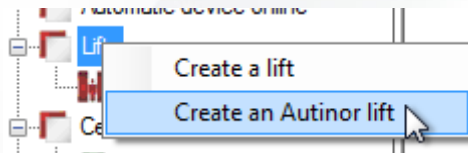
Then you will be able to grant users access on each floor using the access groups.

AUTINOR LIFTS MANAGEMENT

In order to manage Autinor lifts, the function must be activated in the Preferences/Functions menu. An Autinor lift is an electronic interface card between the software and one or more physical lifts.

Adding an Autinor lift

To add an Autinor lift, click on **"Lifts"** and then on **"Create an Autinor lift"**



The following window is displayed:

Lift Autinor 1

Name: Lift Autinor 1

IP address: -

☒ Disconnect

Number of floors: 13 Frequency of the life signal: 1 s

Floor number	Floor name
0	R-1
1	R
2	R+1
3	R+2
4	R+3
5	R+4
6	R+5
7	R+6
8	R+7
9	R+8
10	R+9

OK Cancel

Via this window, you can:

- + Name your lift – enter this in the Label field.
- + Set the IP address and port number of the interface card.
- + Disconnect the lift.
- + Choose the number of floors.
- + Choose the life signal frequency.
- + Name each floor.

Note: each reader must be configured before it can control lifts (see Configuring a reader from the centre / Autinor lifts tab)

Note: the authorisations must be configured based on access groups (see Managing access groups / Autinor lifts tab)

SCHEDULES AND ACCESS GROUPS MENU

MANAGING TIME RANGES

From the menu



Schedules and access groups ▾

click on "Time ranges". The list of time ranges is

displayed.

Click on "Add" to add a new time range.

Click on "Modify" to modify the selected time range.

Click on "Delete" to delete the selected time range.

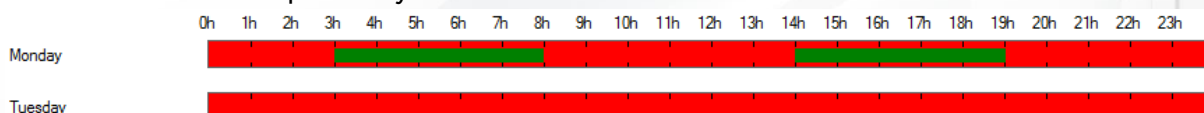
Time range management:

In this window, you can:

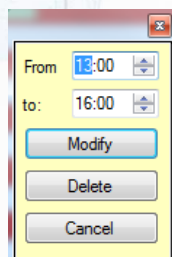
- + Name your time range. Caution: the name must be unique (the same name cannot be used for more than one time range).
- + Configure the type of display:
 - Every day: if your times are different every day.
 - Monday to Friday / Weekend: if your times are identical from Monday to Friday, but different at the weekend.
 - Monday to Sunday: if your times are identical from Monday to Sunday.
 - Monday to Saturday/Sunday: if your hours are the same from Monday to Saturday, but different on Sunday.

+ Enter your schedules

○ Graphic entry



- Adding a time slot: click in a red area and hold down the left mouse button while moving the pointer until the required time slot is obtained.
- Modifying a time slot: click on the time slot and move it. You can also double-click on a time slot and then click on "Modify to enter schedules manually".



- Deleting a time slot: click on the time slot and then press the "Delete" key on your keyboard or double-click on the time slot and then click on the "Delete" button.

○ Manual entry:

Graphic entry
Manual entry

	Time slot 1	Time slot 2	Time slot 3	Time slot 4	Time slot 5	Time slot 6
Monday	From 03:00 to: 08:00	From 14:00 to: 19:02				
Tuesday						
Wednesday	From 13:00 to: 16:00					
Thursday						
Friday						
Saturday						
Sunday						
Public holidays						

Modify the selected time slot

From: 03:00 to: 08:00

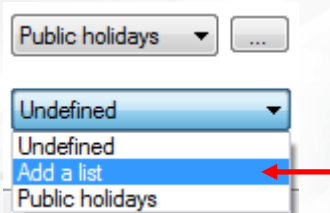
Delete Apply

- Adding a time slot: click on an empty time slot, enter your times in the "Modifying the selected time slot" area and then click on the "Apply" button.
- Modifying a time slot: click on the time slot to be modified, enter your new times in the "Modifying the selected time slot" area and then click on the "Apply" button.
- Deleting a time slot: click on the time slot to be deleted and then click on the "Delete" button.

For each time range, you can define a day of the week as well as choose from a list of public holidays.

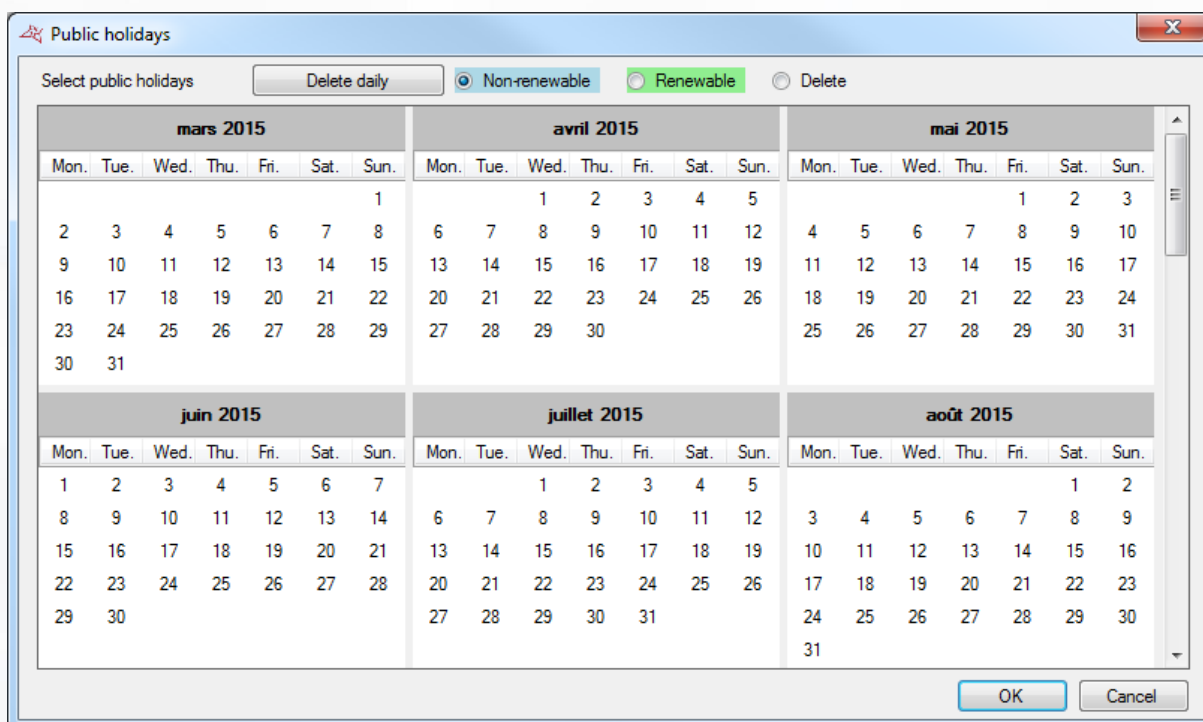
To configure the list, click on the button after "Public holidays". A new window is displayed where you can configure the list of public holidays.

You can also define another list of specific days. To do so, click on the "Add a list" option from the drop-down menu:



MANAGING PUBLIC HOLIDAYS

From the menu  Schedules and access groups, click on "Public holidays". The list of public holidays is displayed.




In this window, you can:

- + Add renewable public holidays (automatically renewed from one year to the next by the central units and software). To do so, select "Renewable" and then click **on the days** that you wish to add. These days will then take the selected colour.
- + Add non-renewable public holidays (automatically deleted at the end of their validity period). To do so, select "Non-renewable" and then click **on the days** that you wish to add. These days will then take the selected colour.
- + Delete public holidays: select "Delete" and then click **on each day** that you wish to delete.
- + Delete all public holidays: click on the "Delete daily" button.
- + Import public holidays from Outlook: automatically import public holidays from your Outlook calendar. Caution: to use this function, Outlook 2007 or earlier must be installed on your computer.

MANAGING SPECIAL DAYS

In addition to special days, you can add up to eight additional lists of special days.

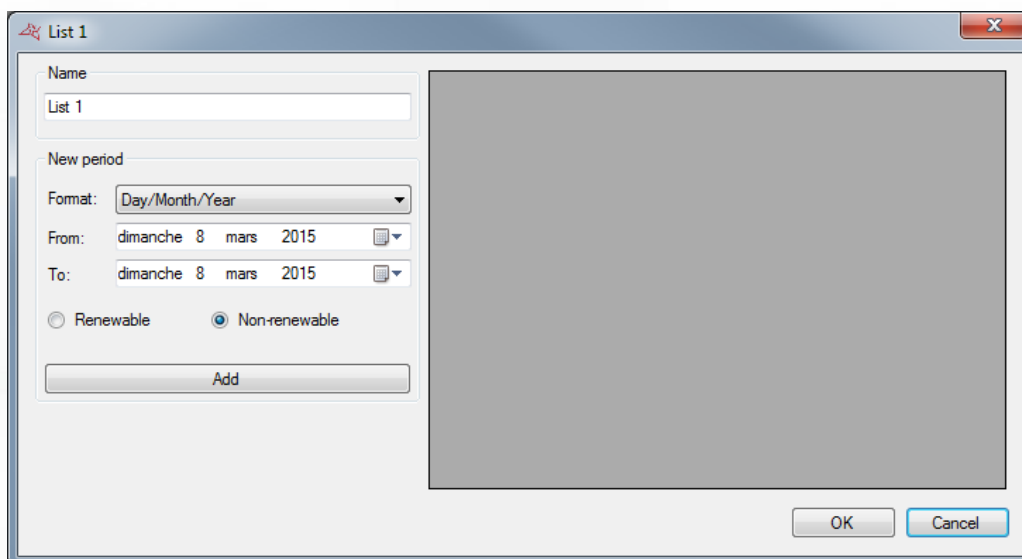
In the  Schedules and access groups menu, click on "Special days". The list of special days is displayed.

Click on "Add" to add a new list of special days.

Click on "Modify" to modify the selected list.

Click on "Delete" to delete the selected list.

Managing a list:



The screenshot shows a dialog box titled "List 1". It contains a "Name" field with the text "List 1". Below this is a "New period" section with a "Format" dropdown set to "Day/Month/Year". The "From" field is set to "dimanche 8 mars 2015" and the "To" field is also set to "dimanche 8 mars 2015". There are two radio buttons: "Renewable" (unselected) and "Non-renewable" (selected). An "Add" button is at the bottom of the form area. To the right of the form is a large empty rectangular area. At the bottom right of the dialog are "OK" and "Cancel" buttons.

From this window, you can:

- + Name your list (in the "Name" area).
- + Add, modify and delete days according to two formats (Day/Month/Year or Day/Month/Year/Hours/Minutes).

MANAGING ACCESS GROUPS

From the menu  Schedules and access groups, click on "Access groups". The list of groups is displayed.

Click on "Add" to add a new group.

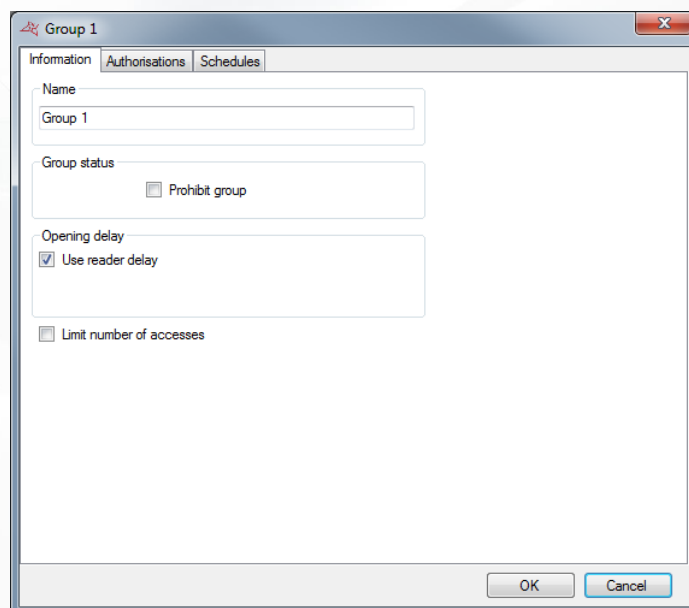
Click on "Modify" to modify the selected group.

Click on "Delete" to delete the selected group.

Click on "Export" to export the configuration report:

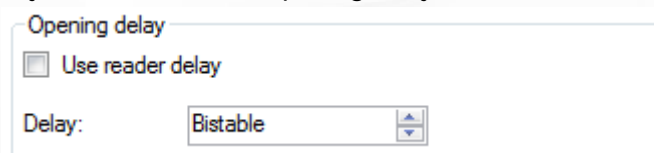
MANAGING AN ACCESS GROUP

Information tab

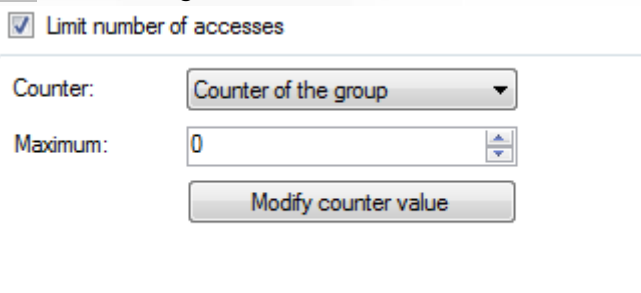


From this tab, you can:

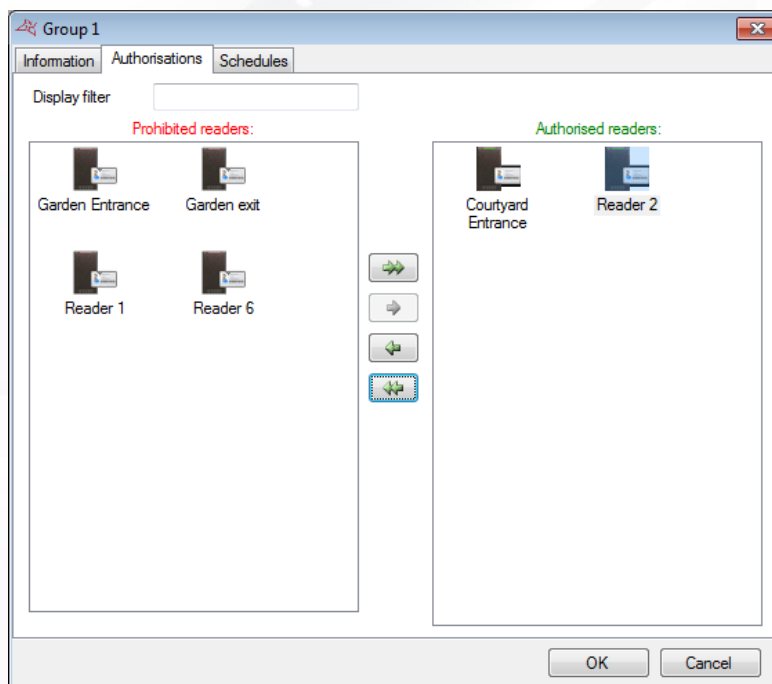
- + Name your access group.
- + Determine your group's status: check the "Prohibit group" box to refuse all users belonging to this group.
- + Choose an opening delay which will replace the reader setting. To do this, uncheck the box "Use reader delay" then set the new opening delay.



- + Restrict the number of accesses for group users to the readers. You can choose the counter that will be used (the group counter or a counter previously created on the unit). If you use the group counter, you can change its current value by clicking on the button "Modify counter value" and entering its new value.

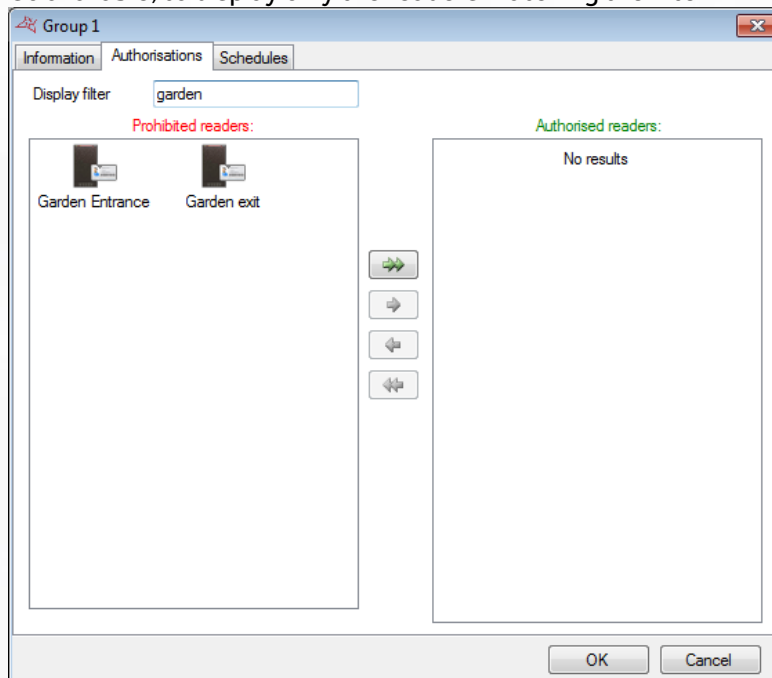


Authorisations tab

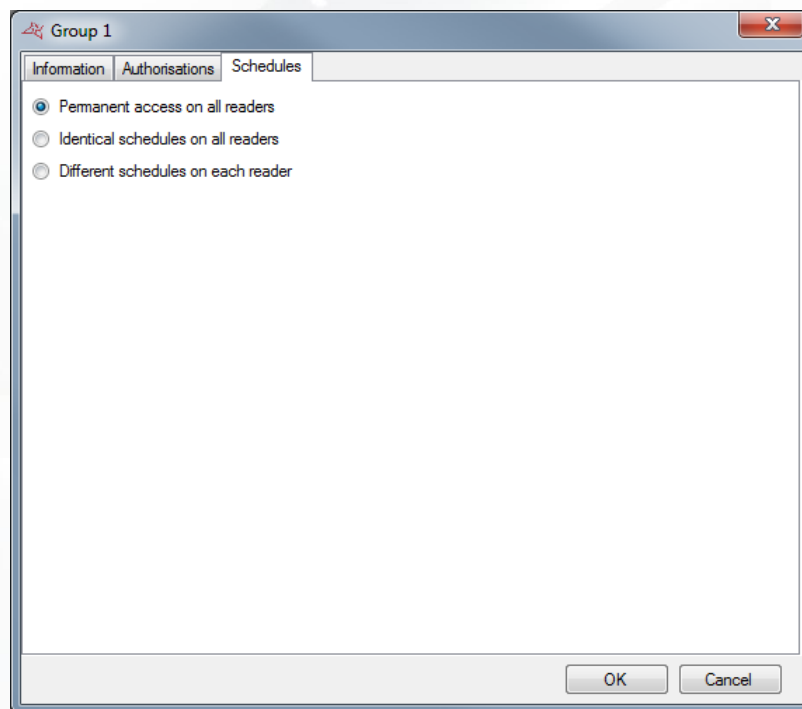


From this tab, you can select the readers to which you want to grant users access. Double-click on a reader in the left-hand list (list of prohibited readers) to authorise it or double-click on a reader in the right-hand list (list of authorised readers) to deny access. You can also use the arrows in the centre of both lists to switch the selected readers.

A display filter is also available, to display only the readers matching the filter.



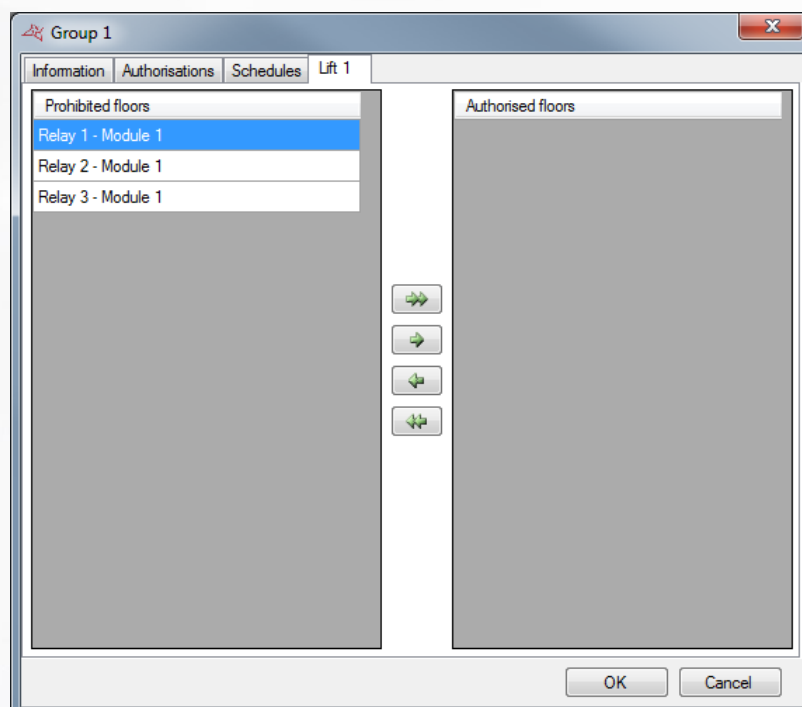
Schedules tab



From this tab, you can define access schedules on the readers authorised for your group. In particular, you can:

- +** Choose to not restrict the access schedules for your users.
- +** Define identical access schedules on all readers: to do so, select or create a time range.
- +** Configure different schedules on each reader: to do so, select a time range opposite each reader.

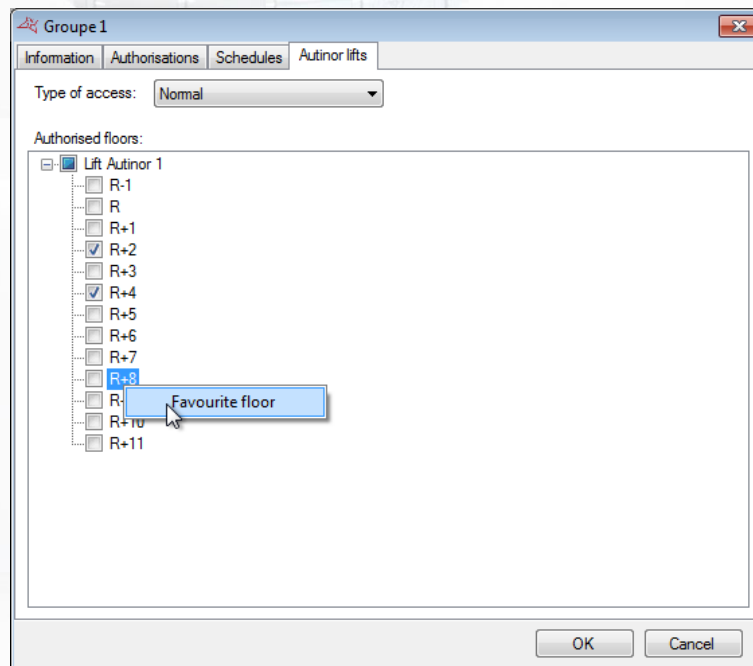
Lift tab



If you manage lifts and if a reader associated to a lift is granted in the group, a new tab with the name of your lift appears.

Then you can select the floors to which you want your users to be granted. Double click on one floor of the left list (list of prohibited floors) to authorize or double click on a floor of the right list (list of authorized floors) to prohibit it. You can also use the arrows in the center of the two lists to toggle the selected floors.

Autinor lifts tab

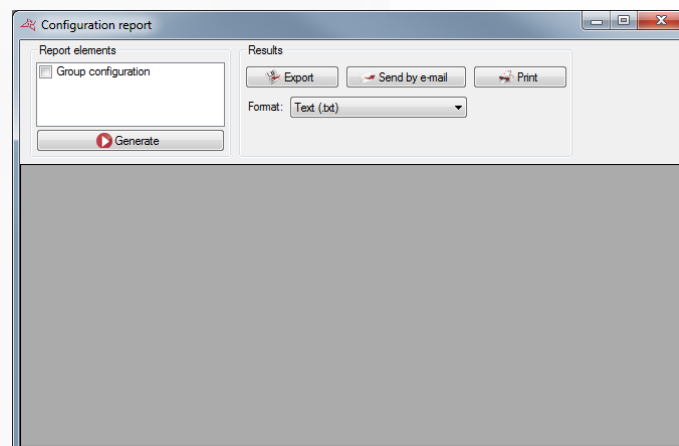


Via this tab, you can:

- + Choose access type (Normal or President).
- + Choose authorised floors.
- + Choose a favourite floor by right-clicking it.

EXPORTING THE ACCESS GROUPS SETTINGS

To export your group access configuration, from this group list, click on "export" button




From this window, you can:

- +** Choose to include the configuration of the groups in the report by checking the "Group Configuration" box.
- +** After generating the report:
 - Export it.
 - Email it to a contact selected in a list or enter the contact directly with the option of zipping the file. This option depends on the email settings in Tools > Preferences > Emails.
 - Print it.
- +** Choose the format for the report:
 - Text (.txt).
 - Comma-separated text (.csv).
 - Access 2007 (.accdb).
 - Excel (.xls).
 - XML (.xml).
 - PDF (.pdf).

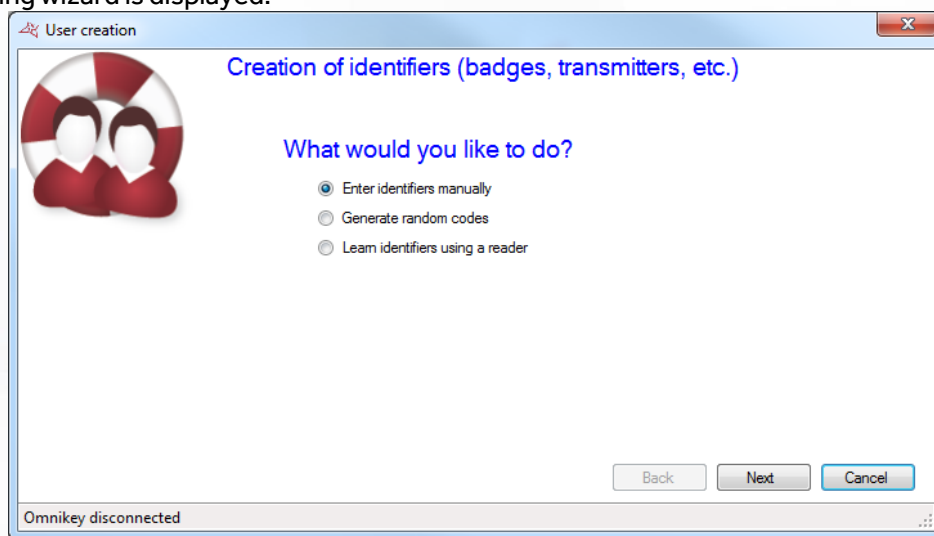
USERS MENU

CREATING USERS

The first method for creating users involves using a wizard, which will create the identifiers (badges, emitters, application badges, and so on), users (physical people accessing the site) and access groups (schedules and access rights for the site's different readers).

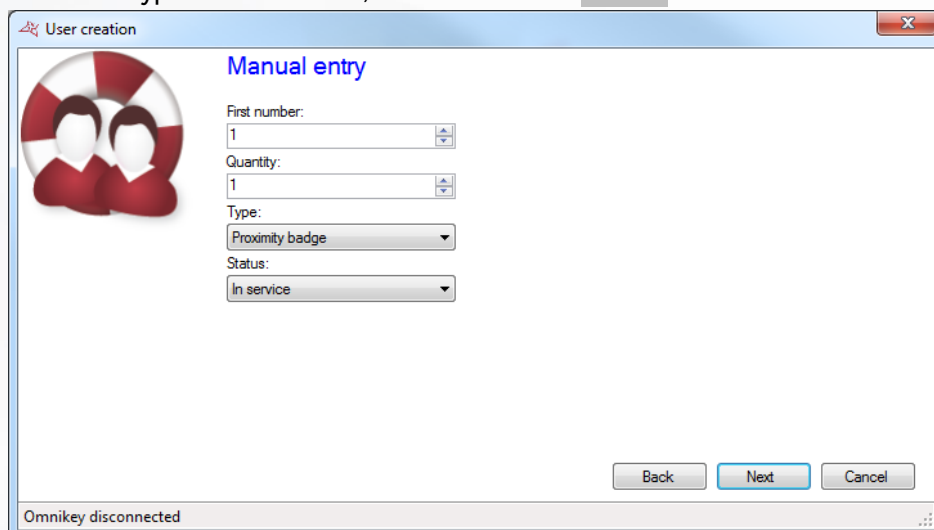
To do so, click on  and then "Create users".

The following wizard is displayed:

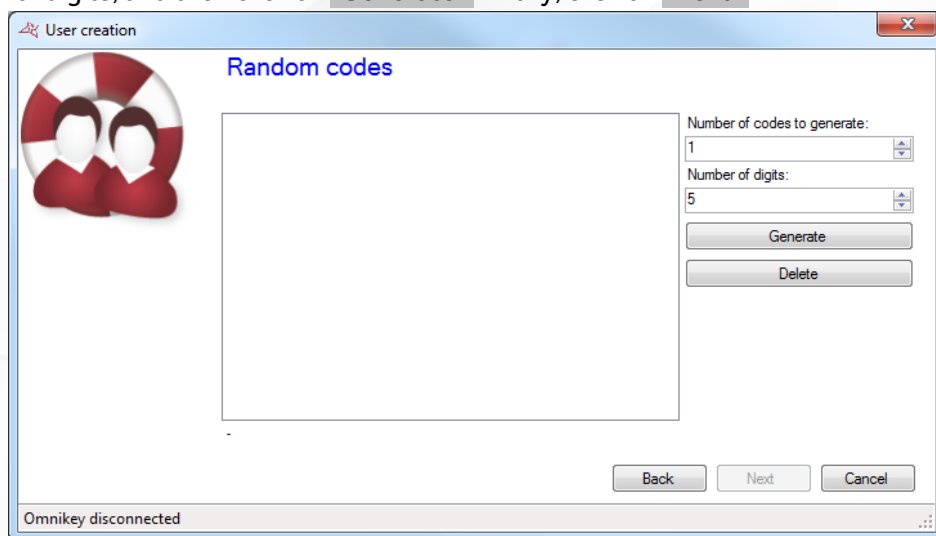


There are three different ways to enter your identifiers:

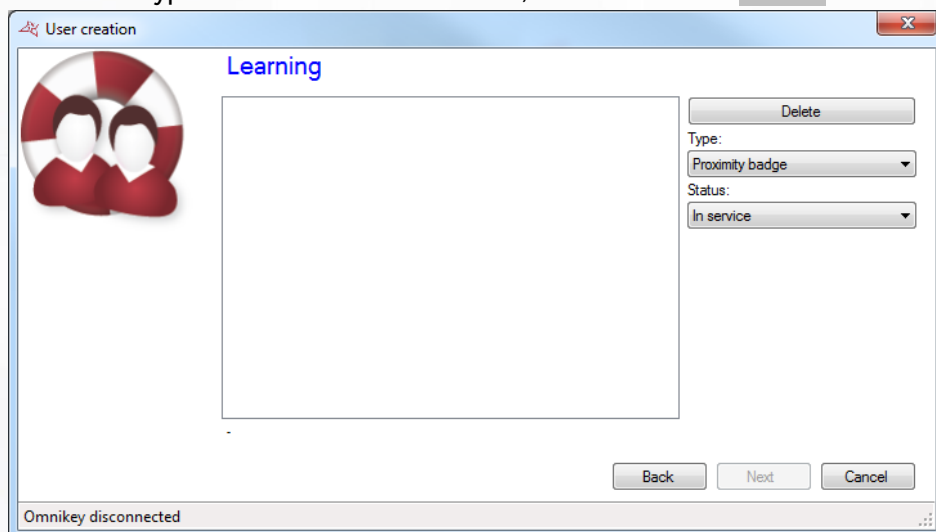
- + **Manual entry:** enter the first number of your identifiers, the quantity to be created, the identifier type and the status, and then click on "Next".



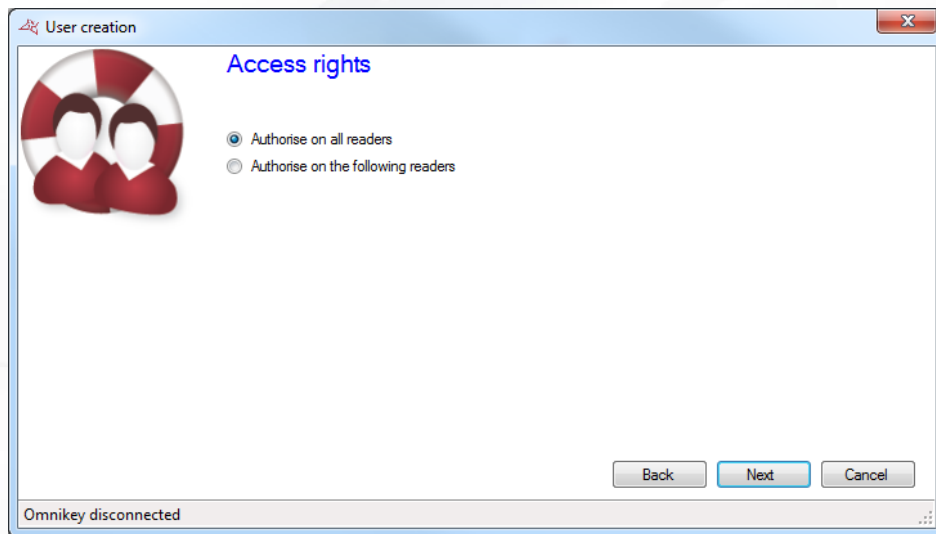
- + Generation of random codes: chooses the quantity of codes to be created and the number of digits, and then click on "Generate". Finally, click on "Next".



- + Learning: click on "Learning" and then pass your identifiers one-by-one to any reader in your installation. If you have a DIGIUSB (Mifare CSN card reader), swipe your badges one-by-one. Select the type of identifier and the status, and then click on "Next".



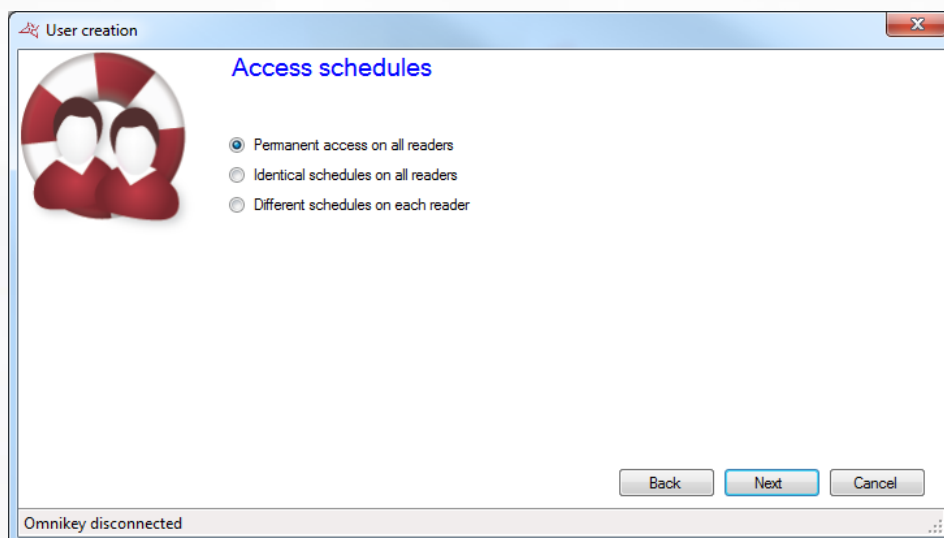
Enter the access rights to be created for your users (authorisations for the site's different readers).



To do so, you can:

- + Use an existing access group (caution: this option is only available if groups have already been created in your installation).
- + Grant users access to all readers.
- + Grant users access to a selection of readers: the list of all readers will then be displayed, and you must check the readers to which users will have access.

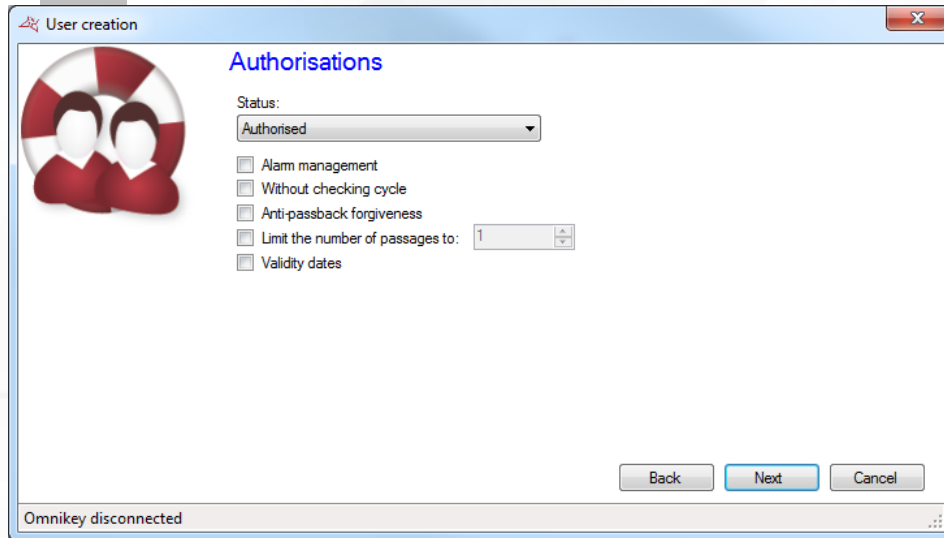
Then click on "Next":



Enter the access schedules for your new users. To do so, you can:

- + Use the schedules for the selected access group: if you have chosen an existing access group, your only option will be to use the schedules for that group.
- + Choose to not restrict the access schedules for your users.
- + Define identical access schedules on all readers: to do so, select or create a time range.
- + Configure different schedules on each reader: to do so, select a time range opposite each reader.

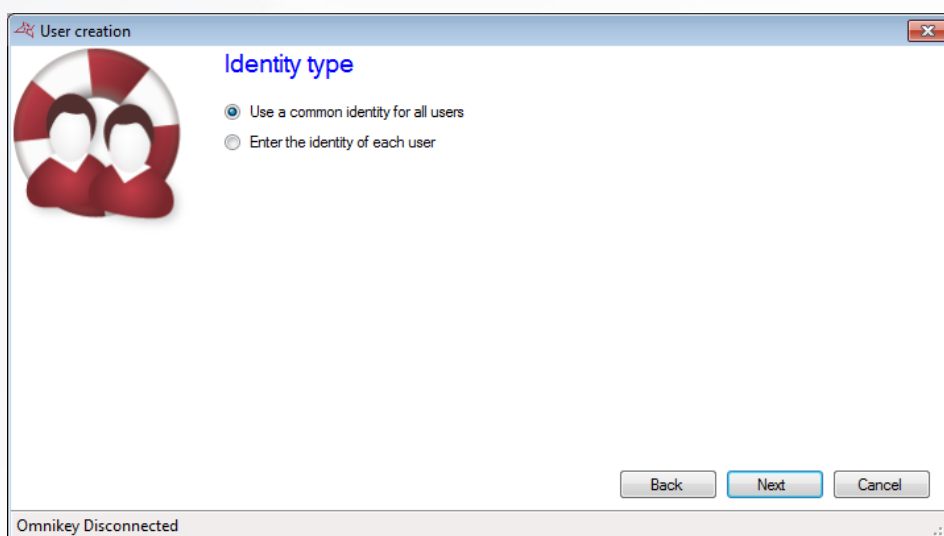
Then click on "Next":



Enter the different options for your users:

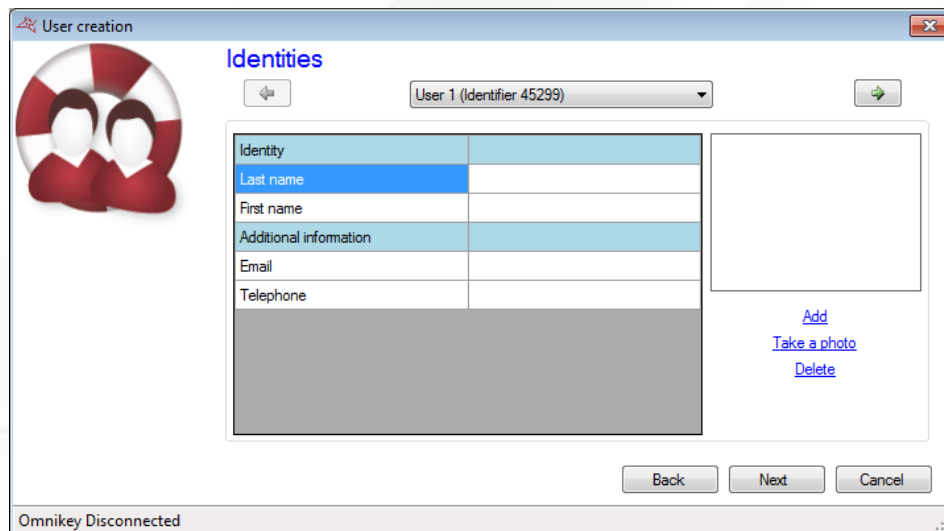
- + Their status (Authorised or Suspended).
- + The "Alarm management" option: users authorised to activate / deactivate an alarm system connected to the central unit (your installation must already be correctly configured).
- + The "Without checking cycle" option: if your installation is configured to use the Anti-passback function and this box is checked, all users created with this option will not be subject to the Anti-passback mechanism.
- + The "Anti-passback forgiveness" option: whenever users operate a reader, all anti-passback cycles for all users will be cleared (all users can enter or exit again).
- + The "Limit the number of passages to" option will restrict a user's maximum number of passages to the value entered.
- + The validity start and end dates.

Then click on "Next":



Use this window to choose the identity type of each user: common or separate identity.

Then click on "Next":



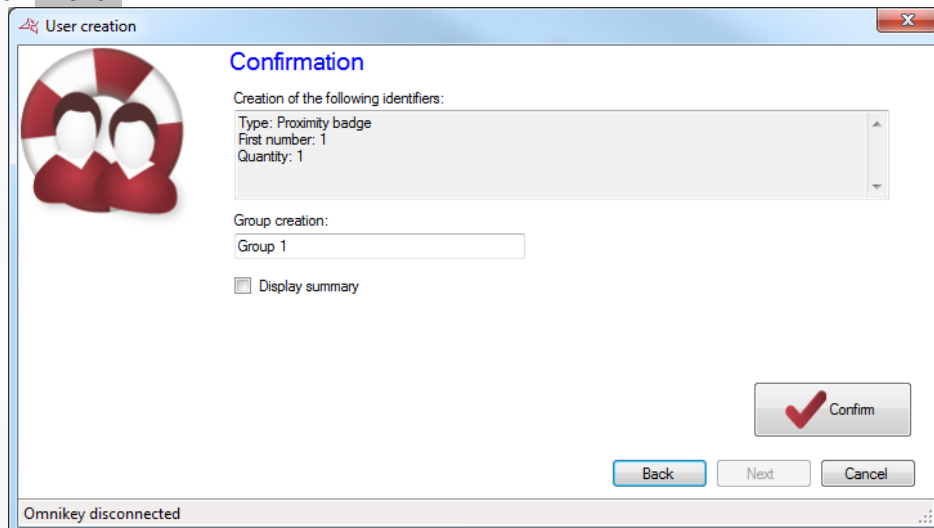
The "User creation" window shows the "Identities" tab. On the left is a circular icon with two stylized figures. The main area contains a dropdown menu set to "User 1 (Identifier 45299)". Below it is a table for user details:

Identity	
Last name	
First name	
Additional information	
Email	
Telephone	

To the right of the table is a large empty box with three links: "Add", "Take a photo", and "Delete". At the bottom are "Back", "Next", and "Cancel" buttons. The status bar at the bottom says "Omnikey Disconnected".

Use this window to define user identities. To proceed to the next step, all fields marked with * must be filled in.

Then click on "Next":



The "User creation" window shows the "Confirmation" tab. On the left is the same circular icon. The main area displays the following information:

Creation of the following identifiers:


- Type: Proximity badge
- First number: 1
- Quantity: 1

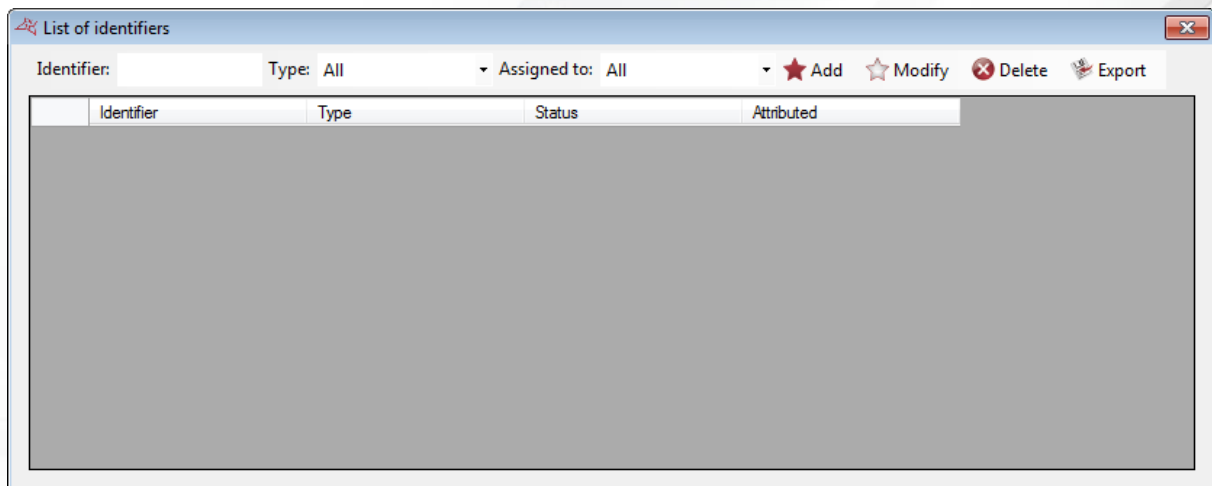
Below this is a "Group creation:" section with a text box containing "Group 1". There is a checkbox labeled "Display summary" which is currently unchecked. At the bottom right is a "Confirm" button with a red checkmark icon. Below it are "Back", "Next", and "Cancel" buttons. The status bar at the bottom says "Omnikey disconnected".

Ensure that all the information displayed is correct. If the wizard needs to create a new access group, you can change its name. Then click on "Confirm" to finish creating your users.

MANAGING IDENTIFIERS

To display the list of identifiers (proximity cards, application tag, transmitters, codes, ...), click on

"Identifiers" in the menu.  Users ▾

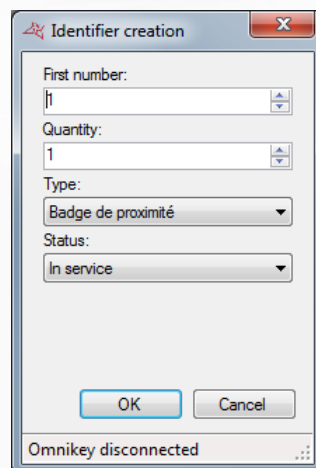


From this window, you can:

- + Search for an identifier by entering the number in the box "Identifier"
- + Select the type of identifiers to display
- + Select if you want to display only the attributed identifiers, not attributed identifiers or both
- + Press "Add" to create a new identifier
- + Press "Modify" to edit an identifier
- + Press "Delete" to delete an identifier
- + Press "Export" to export the list of identifiers

ADDING AN IDENTIFIER

From the previous menu, press "Add"



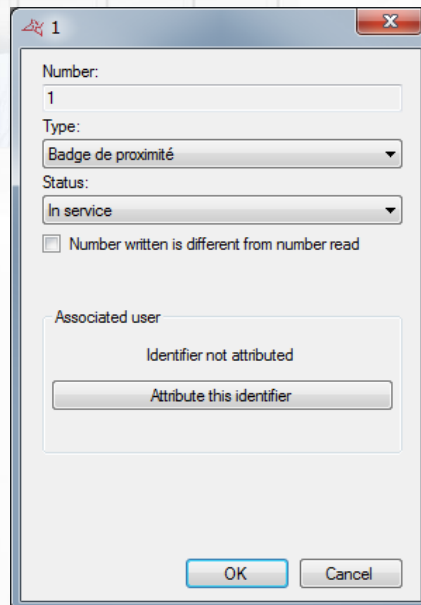
From this window, you can:

- + Enter the number of the first identifier
- + Enter the quantity of identifiers to create in case of several identifiers
- + Select the type of the identifiers
- + Select the status
- + If you use an Omnikey USB reader, swipe the first card in front of the reader

Note: The identifiers created using this window do not have attributed user. That means you have to create users then select the appropriate identifier for each of them. If you want to create identifiers and users at a time, use the "Create users" menu.

MODIFYING AN IDENTIFIER

From the identifiers list, select the identifier to modify then press "Modify" or double click on it.



From this window, you can:

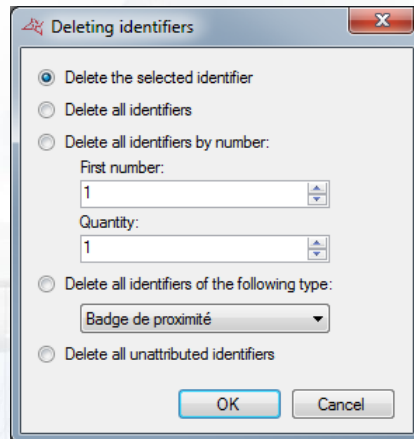
- + Select the type of the identifier
- + Select the status
- + Enter the logical number: if the number written on the identifier is different than the read number. To enable this option, press "Display numbers written on identifiers" from the "Favorites" menu.
- + Attribute or not the identifier to an user
- + Edit the user (if the identifier is attributed)
- + Press **OK** to save the configuration.

DELETING AN IDENTIFIER

From the identifiers list, select the identifier to delete then press "Delete".

Confirm the deletion then confirm if you want to delete the according user (if the identifier is attributed).

If you have authorized multiple modification of identifiers from the "Favorites" menu, the following window appears by pressing "Delete":



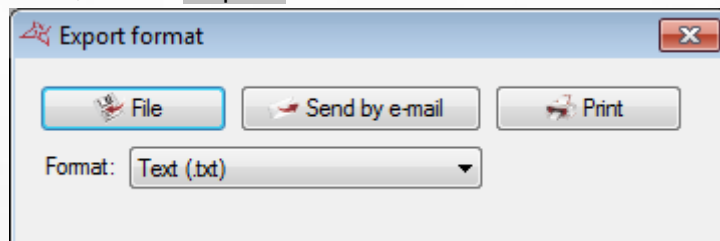
From this window, you can:

- + Delete only the selected identifier
- + Delete all identifiers at a time
- + Delete all identifiers matching with the number and quantity entered
- + Delete all identifiers according to the selected type
- + Delete all identifiers unattributed

Press **OK**, confirm the deletion then confirm if you want to delete the according user (if the identifiers are attributed).

EXPORT THE IDENTIFIERS

From the list of identifiers, click on "Export".

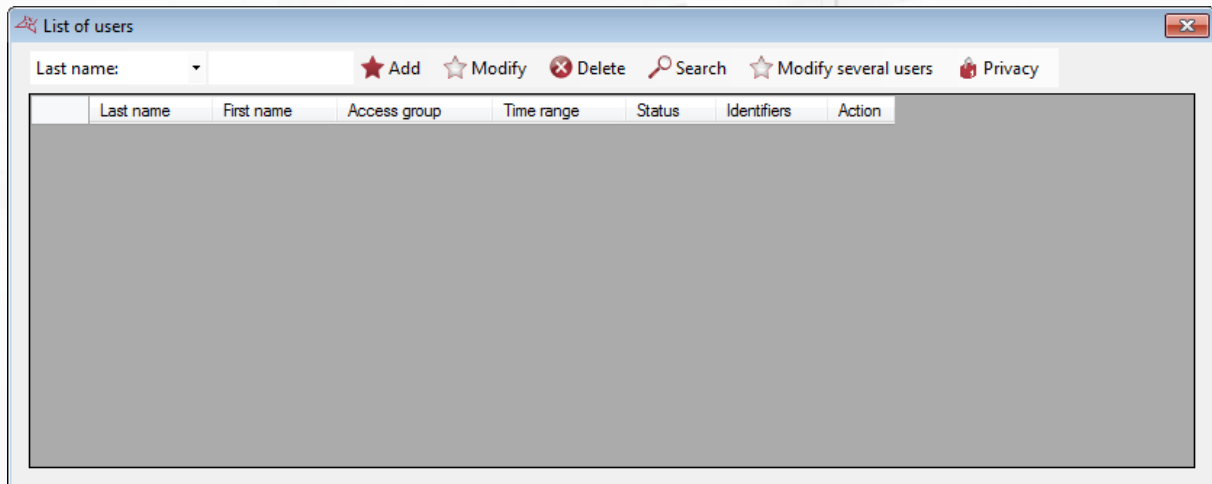


From this window, you can

- + Export the list of identifiers to a file
- + Email the list of identifiers
- + Print the list of identifiers
- + Choose the operating format of the report:
 - o Text (.txt).
 - o Comma-separated text (.csv).
 - o Access 2007 (.accdb).
 - o Excel (.xls).
 - o XML (.xml).
 - o PDF (.pdf).

MANAGING USERS

To display the list of users, click on "Users" in the menu.



From this window, you can:

- + Search for an user by entering his last name or first name or press "Search" for more criteria
- + Press "Add" to create a new user
- + Press "Modify" to edit an user
- + Press "Delete" to delete an user
- + Press "Modify several users" to modify several users. To enable this option, check the box "Authorize multiple modification of users and identifiers" from the "Favorites" menu.


ADDING OR MODIFYING A USER

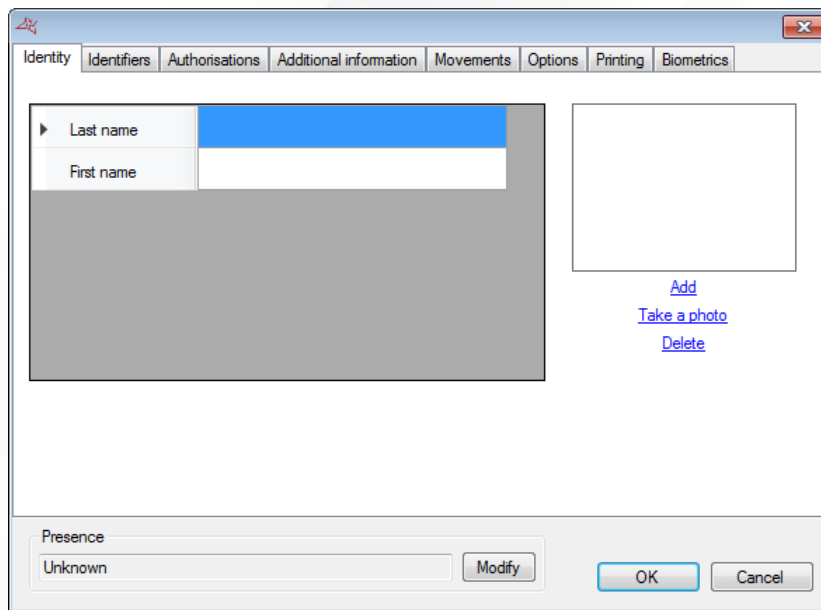
To add a user, press "Add" from the previous window.

To modify a user, you must first open his record.

To find a user, click on "Users" in the menu



The list of users is displayed. Double-click on one of the users in the list or click on  Search to find a user based on their last name, first name or identifier.
The user's record is then displayed:



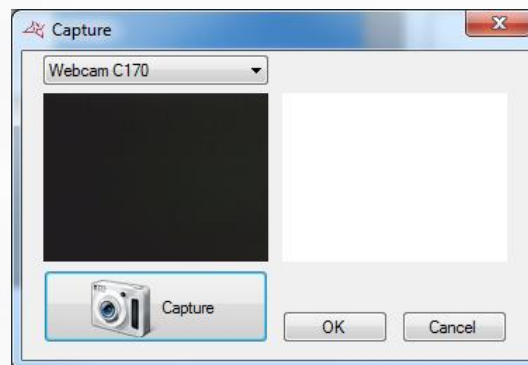
Tip: at the bottom of the window, you will see information about the user's presence (Unknown if your site has not implemented the anti-passback function or if the user has not yet operated one of your site's readers, in or out, the date of his last passage and the zone in which he is if you manage the zones).

Identity tab

From this tab, you can:

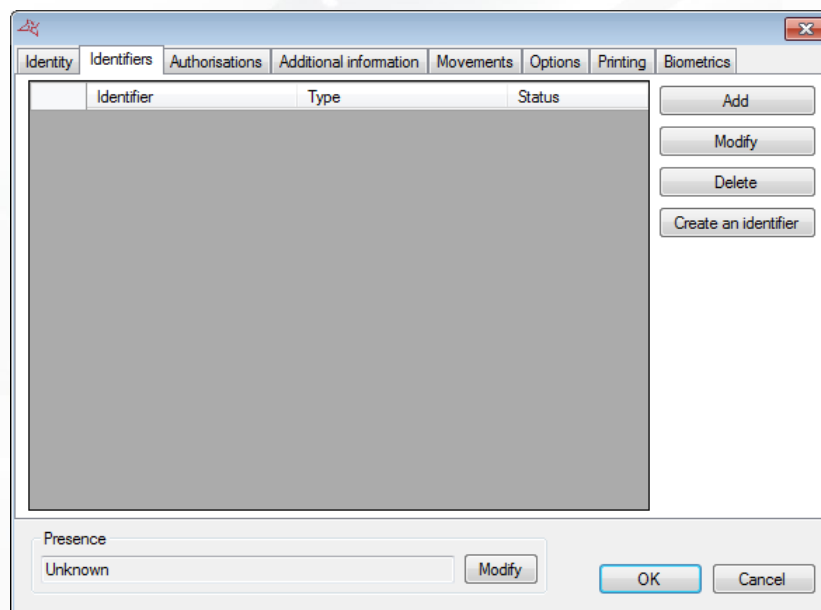
- + Configure a last name and first name for your user.
- + Add an image file that has already been saved on your computer or network.
- + Take a photo using a webcam connected to your computer.
- + Delete the user's photo.

If you click on "Take a photo", the following window is displayed:



Select the required webcam from the list in the top-left corner. Click on the "Capture" button to take a photo. Finally, when the photo suits you, click on "OK".

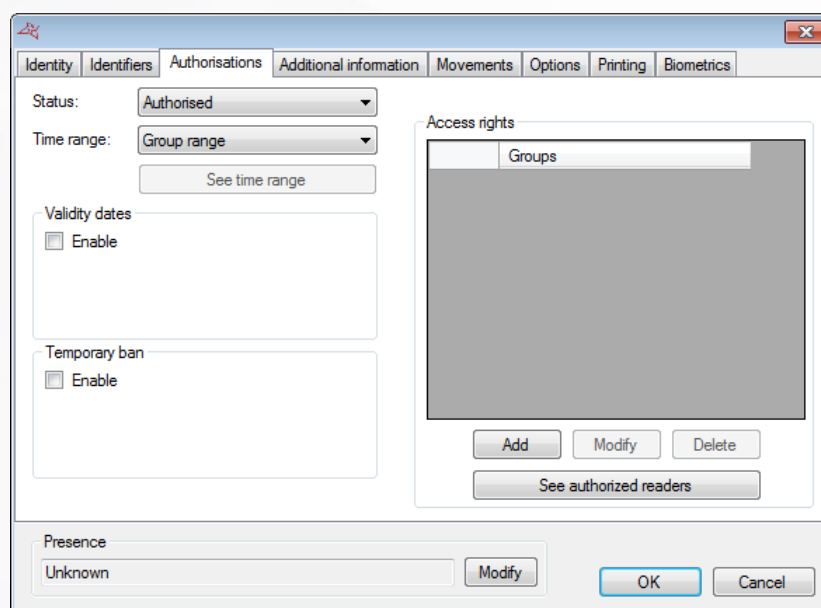
Identifiers tab



From this tab, you can:

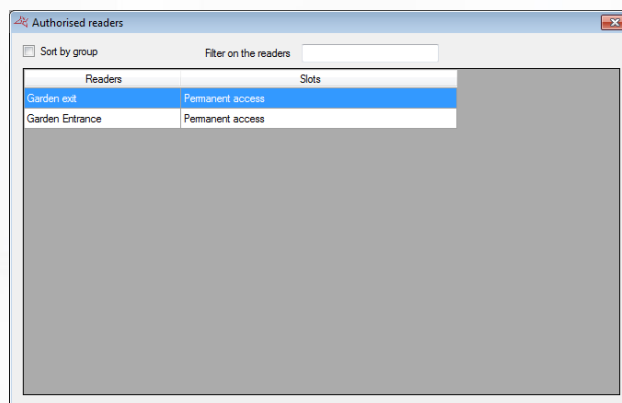
- + Add new identifiers to your user (for example, your users can use an emitter to access a car park and a badge to access their office). You can assign as many identifiers to the user as required (maximum of 15,000). Caution: the same identifier cannot be assigned to more than one user. Click on the "Add" button. The list of identifiers (only those that have not yet been assigned) is displayed. Then double-click on the identifier that you wish to assign to the user
- + Modify an already assigned identifier: select an identifier in the list and then click on "Modify". You can then modify the type of identifier (proximity badge, etc.) and the status (In service, Suspended or Stolen).
- + Remove an identifier from your user: select an identifier in the list and then click on "Delete".

Authorisations tab



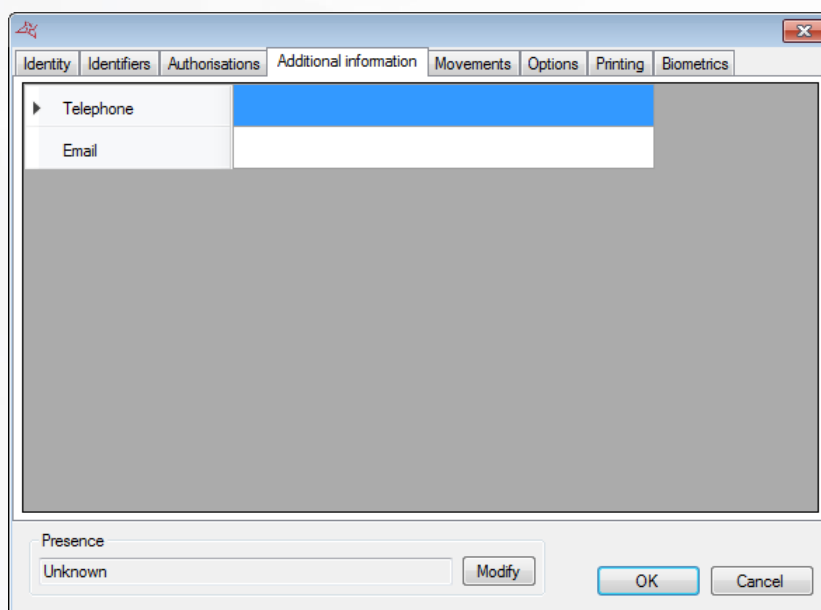
From this tab, you can:

- + Select the user's status (Authorised or Suspended).
- + Configure the access schedules:
 - Group range (use the schedules configured in the access groups).
 - Permanent access: no schedule restrictions for all readers, regardless of the schedules configured for your access groups.
 - Predefined time range: use this time range for all readers, regardless of the time ranges configured for your access groups.
- + Configure the validity start and end dates and times.
- + Configure start and end dates and times for temporary bans. A user who is temporarily banned cannot access the site during the specified period
- + Configure the access groups:
 - Add a group from those already created: click on the "Add" button. The list of groups is displayed. Double-click on the required access group. You can add up to three access groups for the same user.
 - Modify the access group selected in the list.
 - Delete the selected access group.
 - See authorized readers:



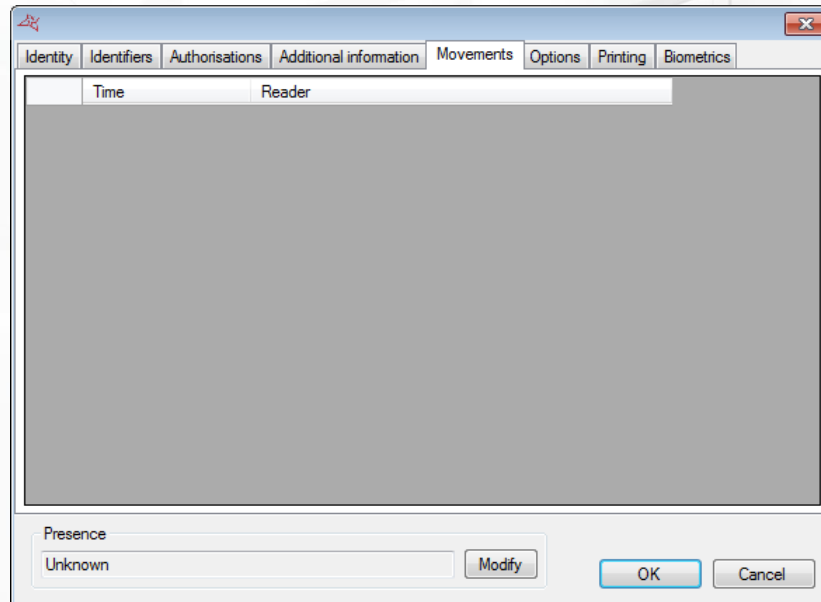
It is possible to display the readers in groups, and to filter the displayed readers.

Additional information tab



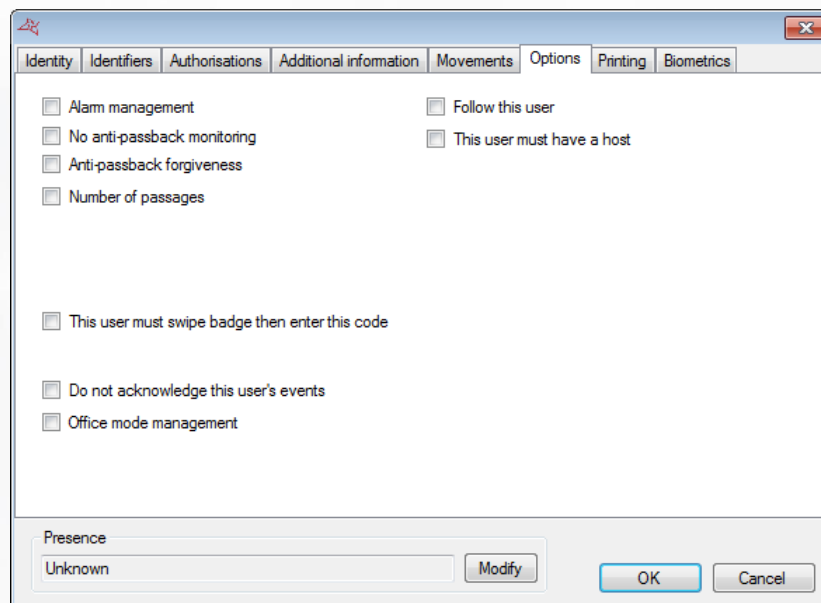
From this tab, you can add other types of information to your user (e.g. telephone number, parking space, etc.). To add new fields, use the "Preferences" menu from the "Tools" menu at the top of the software's interface.

Movements tab



In the "Movements" tab, you can see the user's last 50 passages. The first line in the list corresponds to the most recent passage.

Options tab



From this tab, you can modify the different options for your user:

- +** The **"Alarm management"** option: users authorised to activate / deactivate an alarm system connected to the central unit (your installation must already be correctly configured).

- + The **"No anti-passback monitoring"** option: if your installation is configured to use the Anti-passback function and this box is checked, all users created with this option will not be subject to the Anti-passback mechanism.
- + The **"Anti-passback forgiveness"** option: whenever users operate a reader, all anti-passback cycles for all users will be cleared (all users can enter or exit again).
- + Number of passages: users will have a restricted number of passages for the readers configured to support this function.
- + Option "Track this user" enables you to send an email and/or an SMS to managers if the feature was activated in the settings. Cf. Email preferences and SMS preferences.
- + The **"This user must have a host"** option: on readers configured to support this function, users must be accompanied by a specific user or a user belonging to an access group in order to be authorised. Check this box and then choose the type of host:

☒ This user must have a host

Host

☒ User
 ☐ User group

Search

Delete

- **"User"**: click on "Search" and then double-click on the host in the list displayed.
 - **"User group"**: click on "Search" and then double-click on the host access group (any user belonging to the selected access group can accompany the user).
- + The "This user must swipe badge then enter this code" option: on readers configured to support this function, users must enter the specified code.

☒ This user must swipe badge then enter this code

1234

- + The "Do not acknowledge this user's events" option: the acknowledgment window will not be displayed for this user
- + The "Office mode management" option: allows the user to manage office mode on configured readers.

Printing tab

Identity

Identifiers

Authorisations

Additional information


Movements

Options

Printing

Biometrics

Preview



Last name :

Printing template:
Template 1

Printer:
Default printer

Identifier:
1

Send by email

Print

Presence
Unknown

Modify

OK

Cancel

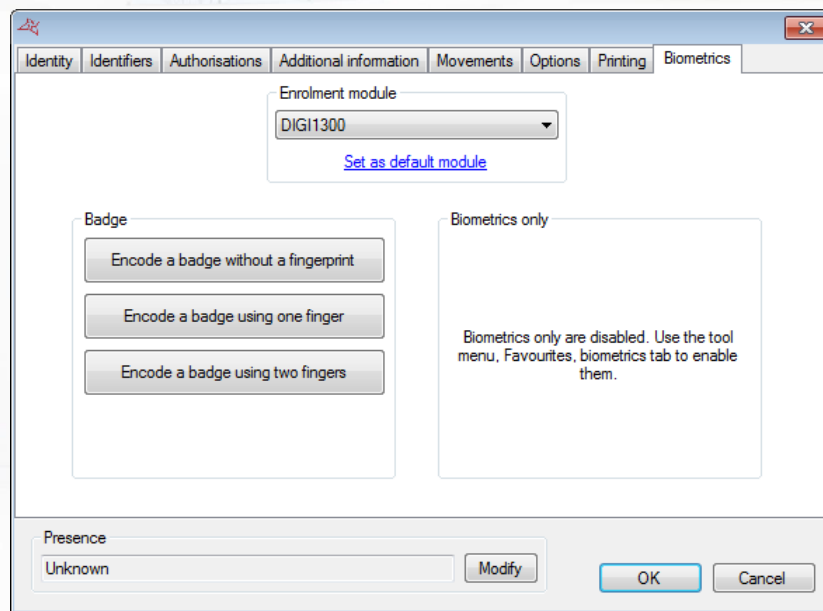
In the "Printing" tab, you can select:

- + The predefined printing template. Refer to "Badge printing templates".
- + A printer.
- + An identifier.

To finish, click on:

- + "Send by email" to send the card as an attachment to an email
- + "Print" to print the card.

Biometrics tab



From this tab, you can:

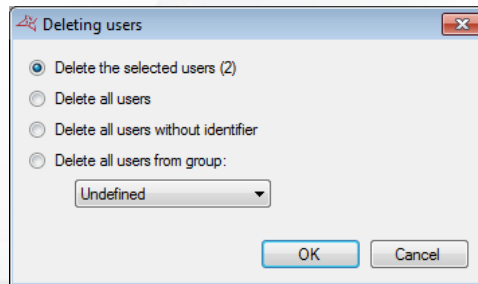
- + Choose the enrolment module (click "Set as default module" to remember the used module)
- + Encode a card with or without fingerprints
- + Enrol the user's fingerprints (to activate this function, use the "Preferences" menu if you are sure to be allowed to use fingerprints only in your current country)

DELETING USERS

From the users list, select the user to delete then press "Delete".

Confirm the deletion then confirm if you want to delete the according identifiers (if the user owns one or more identifiers).

If you have authorized multiple modification of users from the "Favorites" menu, the following window appears by pressing "Delete":



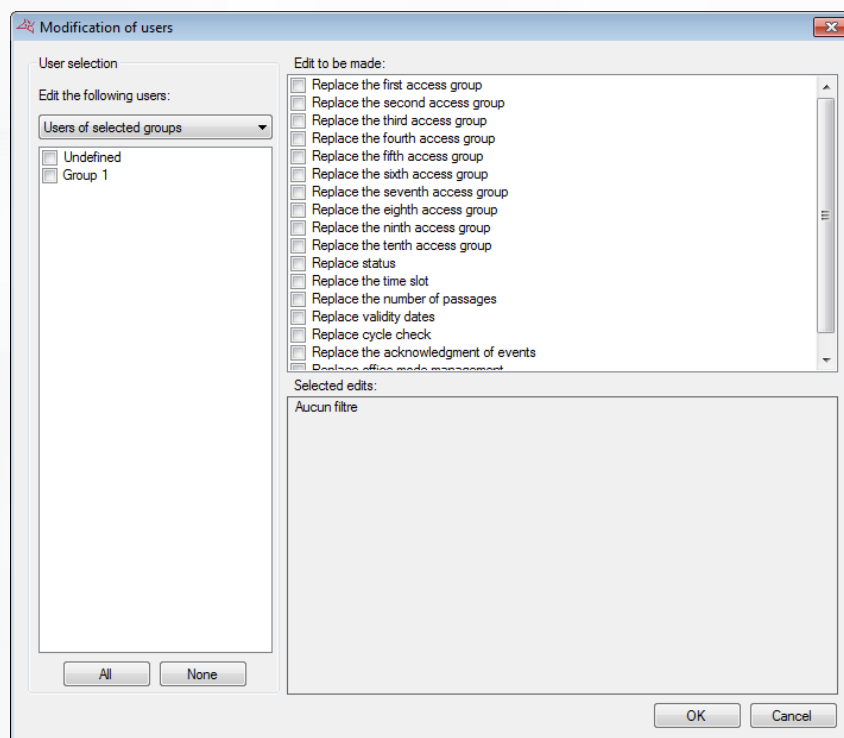
From this window, you can:

- + Delete only selected users
- + Delete all users
- + Delete all users without identifier
- + Delete users belonging to a group

Press **OK**, confirm the deletion then confirm if you want to delete the according identifiers (if the user owns one or more identifiers).

MODIFYING SEVERAL USERS AT A TIME

From the users list, press **"Modify several users"**. This option is only available if the box "Authorize multiple modification of users and identifiers" is checked from the "Favorites" menu.



From this window, you can:

- + Choose to only edit selected users
- + Select the groups of users to modify
- + Select to replace the ten groups of the corresponding users
- + Select to replace the status of the corresponding users
- + Select to replace the time zone of the corresponding users
- + Select to replace the number of passages of the corresponding users
- + Replace the company of the corresponding users
- + Select to replace the validity dates of the corresponding users

- + Replace the cycle verification of the corresponding users
- + Replace the acknowledgment of events of the corresponding users
- + Replace the office mode management of the corresponding users

Press **OK** to modify all users according to selected group(s).

Warning: this operation cannot be undone.

USER PRIVACY

This function makes it possible to anonymise the traces of deleted users in accordance with European personal data protection regulations.

In the User list, click on "Privacy".

Via this window, you can:

- + Set the user's surname.
- + Set the user's forename.

Validate the action by clicking on **OK**. VISOR will display a confirmation request. Confirm the modification by clicking on **Yes**.

Warning: this action cannot be undone and it has an impact on the results of history searches.

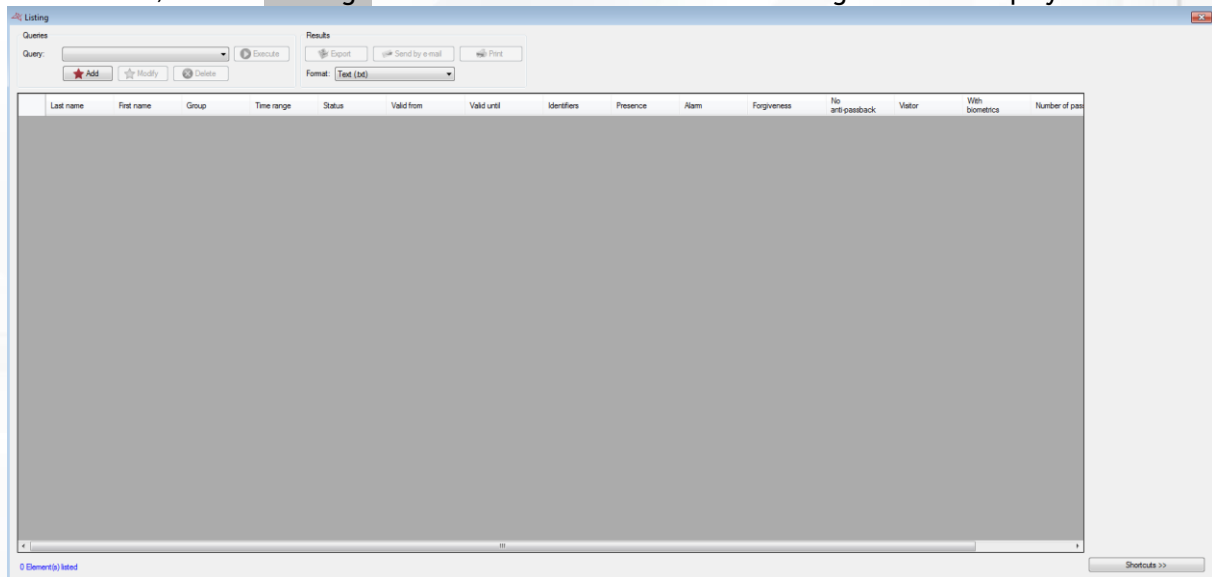
CUSTOM LIST OF USERS

You can generate user lists by configuring the fields to be displayed and filtering according to different criteria.

To sort a list, click on "Listing" in the menu.



The following window is displayed:

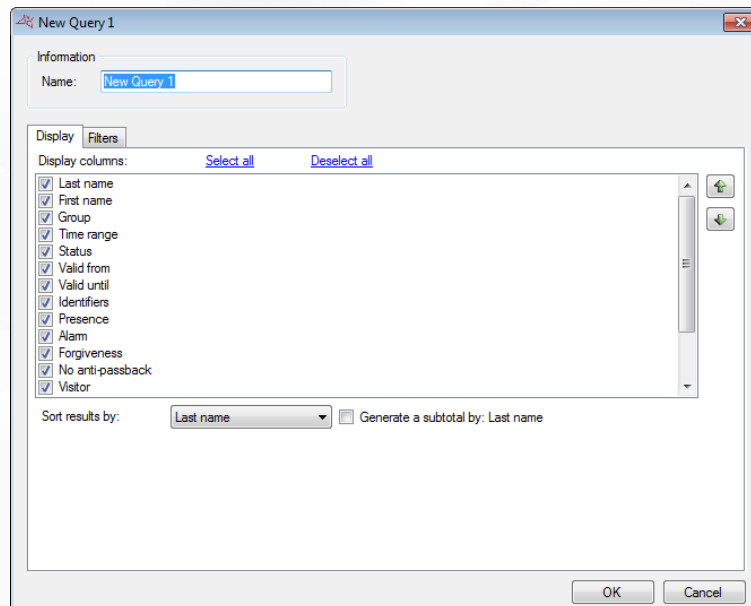


From this window, you can:



- + **Add a query:** click on the "Add" button and then configure your query.
- + **Modify a query:** select your query in the list and then click on the "Modify" button.
- + **Delete a query:** select your query in the list and then click on the "Delete" button.
- + **Execute a query:** select your query in the list and then click on the "Execute" button. The results will then be displayed.
- + **Export the results of a query:** after executing a query, select a format in the list (text file, comma-separated text, Access 2007 database, Excel, XML or PDF) and then click on the "Export" button.
- + **Send the query results by email:** after executing a query, select a format in the list (text file, comma-separated text, Access 2007 database, Excel, XML or PDF) and then click on the "Send by e-mail" button. Select or enter a recipient and choose whether to zip the file. Caution: to use this function, you must have configured the email settings in the software's "Preferences" menu.
- + **Print the query results:** after executing a query, click on the "Print" button.
- + Open the selected user's record by double-clicking on it or by clicking on the "Modify" button in the bottom-right corner if shortcuts are displayed (to show or hide shortcuts, click on the "Shortcuts" button).

MANAGING A QUERY

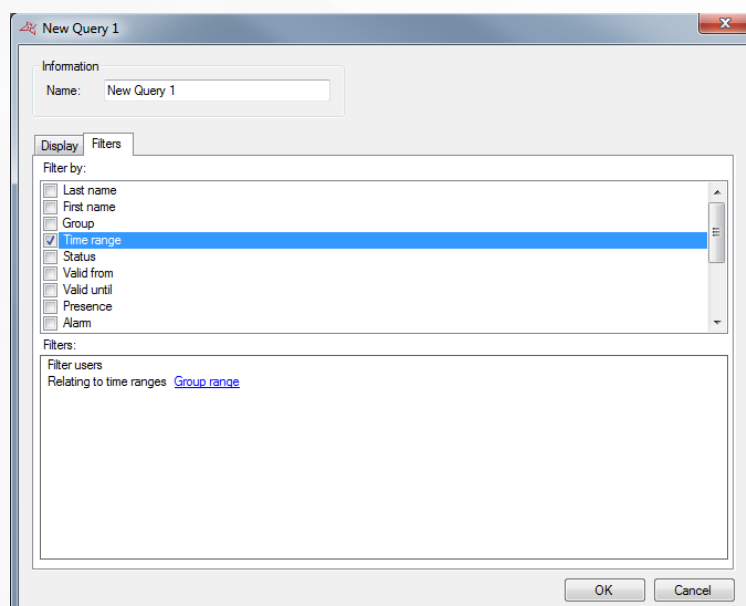
Display tab



From this tab, you can:

- + Name your query: enter the name in the "Name" field.
- + Check the fields that you wish to display in the list.
- + Note that additional fields can be selected provided that they have previously been added via Tools > Preferences > Additional information.
- + Use buttons  and  to change the order in which the result columns are displayed.
- + Select a sort for the results.
- + Check the "Generate subtotal" box to generate a subtotal depending on the selected sort criteria.

Filters tab



To filter the users to be displayed, click on the "Filters" tab. In this tab, you can define the following filters:

- + By last name: filter users whose last name starts with / ends with / contains your text.
- + By first name: filter users whose first name starts with / ends with / contains your text.
- + By group: filter users whose group is part of your list.
- + By time range: filter users whose time range is part of your list.
- + By status: filter users whose status matches the selected status.
- + By validity start and end date: filter users whose validity dates are later than / earlier than / between the dates entered.
- + By credentials: filter users with specific credentials.
- + By presence: filter users whose presence matches the presence selected.
- + By Alarm, Forgiveness, Password confirmation (without any anti-passback cycle check), Visitor, and With biometrics: filter users whose options match the options selected.
- + By number of passages: filter users whose passages are equal to / greater than or equal to / less than a number or between two numbers.
- + By the presence of biometric data: filter users according to whether they have been enrolled.
- + By number of passages: filter users whose number of passages is equal to / greater than or equal to / less than or between the values entered.
- + By inactivity: filter users who have not logged in for a while
- + By acknowledgment: filter users for which the acknowledgment window will or will not be displayed
- + By Office mode management: filter users with or without Office mode management.
- + By presence of a photo: filter users based on whether or not their credentials have a photo.
- + By authorised readers: filter users according to the authorised readers.
- + If you have defined additional fields: filter users whose information starts with / ends with / contains your text.

To add a filter, simply check it. A new window is displayed, where you can fine-tune your search criteria.

To modify a filter, go to the list of filters (at the bottom of the window) and click on the [blue link](#) (example: [Group range](#)). A new window is displayed, where you can fine-tune your search criteria.

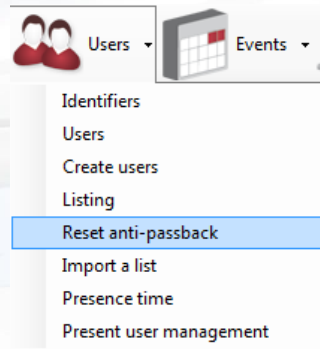
To delete a filter, simply uncheck it.

To filter users by last name or first name, check the "Ask on execution" box, so that the software prompts you to enter your text when executing the query.

Once you have entered your filters, click on "OK". In the previous window, click on "Execute". The results will be displayed.

RESET USERS ANTI-PASSBACK

To reset all users anti-passback cycle, click "Reset anti-passback" as follows:

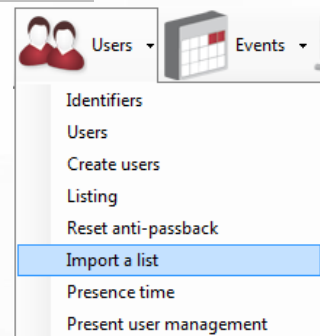


Click "Yes" when prompted.

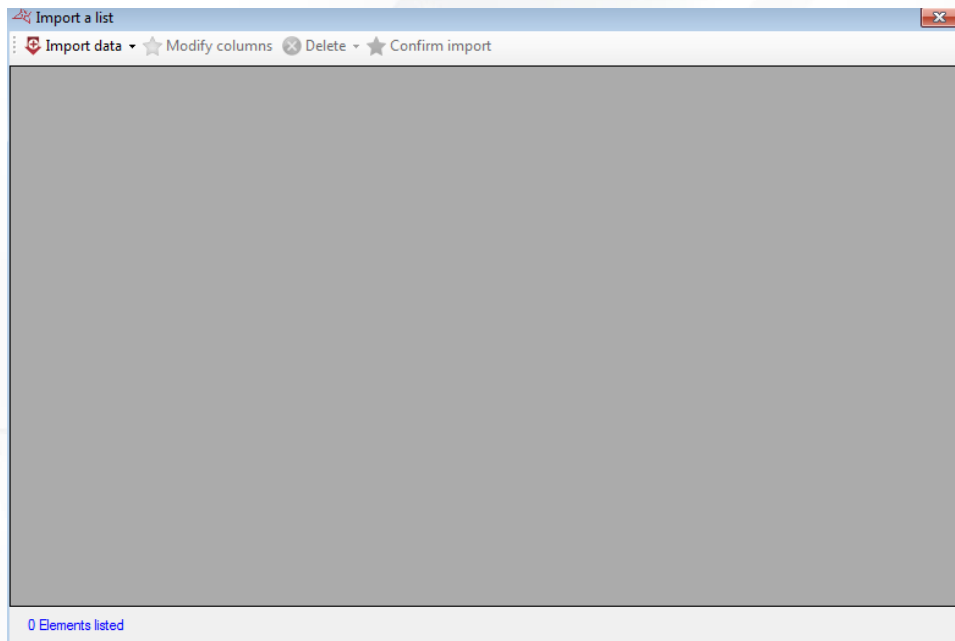
The current presence of all users will be erased and they will be able to go in or out again.

IMPORTING A LIST OF USERS

To import a list of users, click "Import a List" as follows:

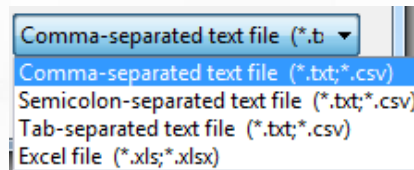


The following window appears:

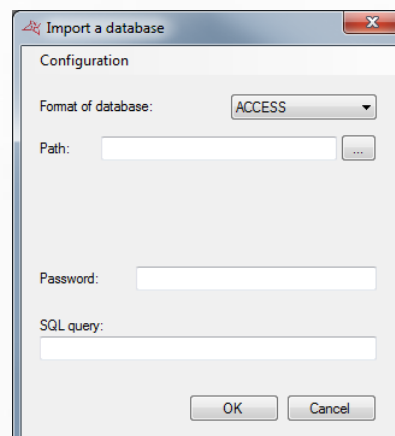


To import your list, click **"Import Data"** and then select your data type:

- + From the clipboard: you must first have copied data
- + From a file: Then select your file format and click **"Open"**. The following formats are available:

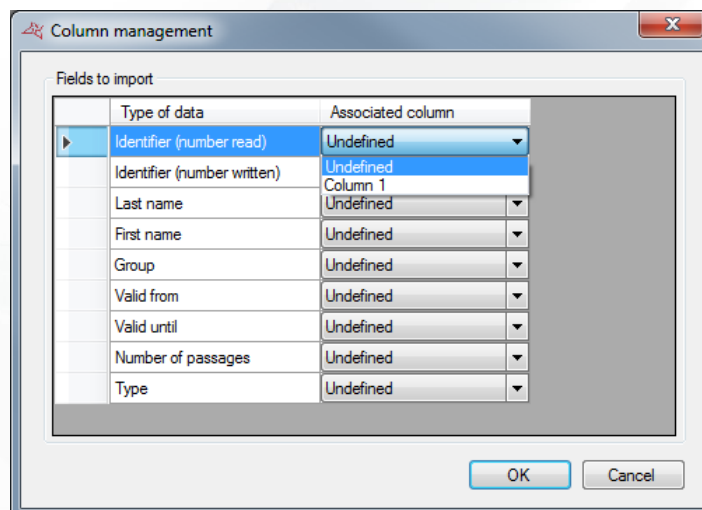


- + From a database:



- Select the format of the database (ACCESS or SQL SERVER)
- Enter the path to the database
- Enter the authentication mode, the login and password if necessary
- Specify the query to retrieve the data to import
- Use the "Settings" button to export or import the configuration

Once your data is imported, you must configure the various columns as follows:



For each field type to import, configure the column number based on the data in your file. If your file does not contain some columns, leave them as "Undefined".

Tip: You can import multiple credentials per user. To do this, in the identifier column, enter the list of user IDs separated by commas.

To return at any time on this column settings, click "Modify Columns".

To remove the lines you do not want to import, select them from the list and click "Remove".

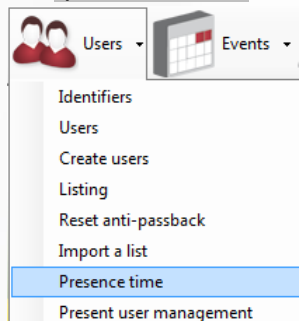
To start importing and creating users, click "Confirm Import".

If you have set a "Group" column, make sure that the access groups were created previously with the same spelling. You can then choose whether to create non-existent groups.

Otherwise, you can choose an access group that will be automatically assigned to all imported users. These last two options will be required upon confirmation of import.

PRESENCE TIME

To calculate the user presence time, click "presence time" as follows:



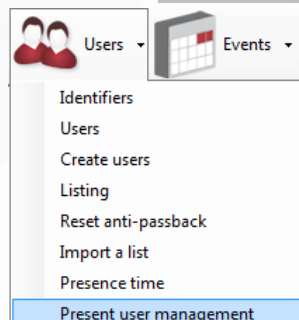
The following window appears:

From this window, you can:

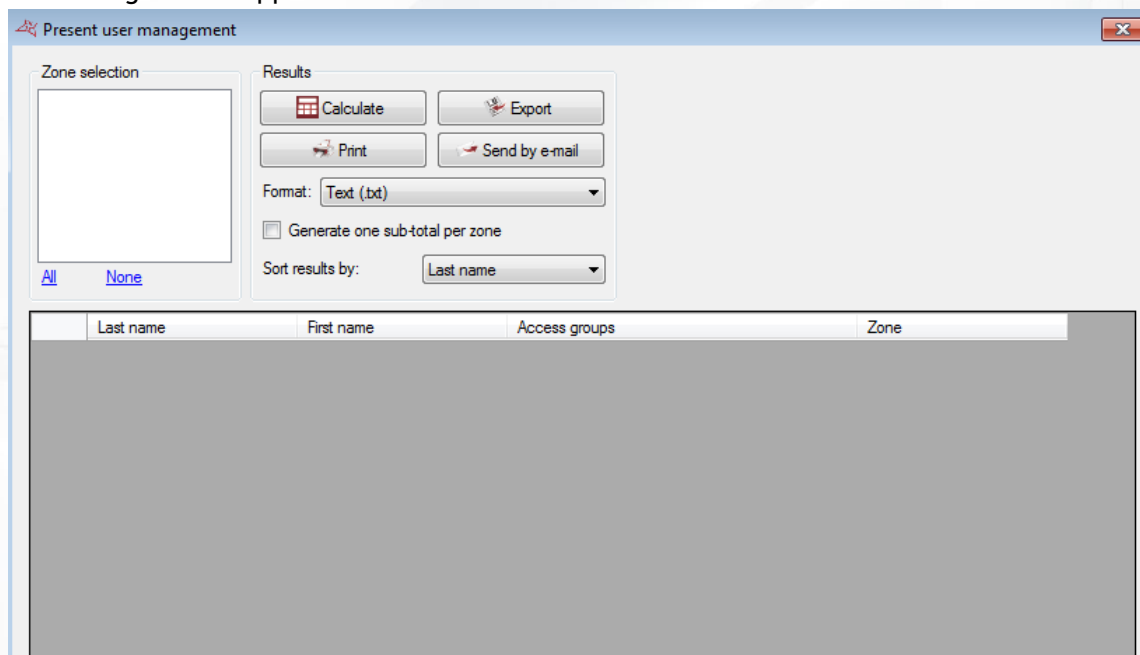
- + **Select the entries and exists readers.** You can also use the shortcuts "All" and "None" to check or uncheck all readers within one click.
- + **Select the calculation period:** month predefined or custom period
- + **Select users to calculate** either the users of all groups, users of a group or a specific user
- + **View the details of the user passages** by checking the box "Display passages"
- + **Start the calculation** by clicking on "Calculate"
- + **Export results:** after running the calculation, select a format from the list (text file, text separated by commas, Access 2007 database, Excel, XML or PDF) and click the "Export" button.
- + **Send results by email:** after running the calculation, select a format from the list (text file, text separated by commas, Access 2007 database, Excel, XML or PDF) then click "Send by e-mail". Select or enter a recipient and choose whether to compress the file. **Caution:** to use this feature, you must have configured the mail settings from the "Preferences" menu of the software.
- + **Print the results:** after running the calculation, click the "Print" button

MANAGING THE PRESENT USER

To view the list of users in one or more areas, click "Present user management" as follows:



To use this feature, you must have configured your areas first.
The following window appears:



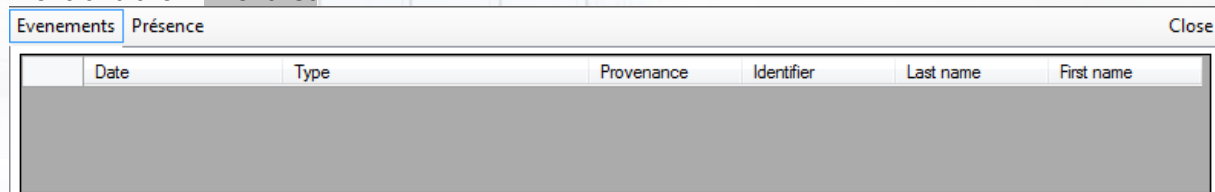
From this window, you can:

- + **Select the areas used for the report.** You can also use the shortcuts "All" and "None" to check or uncheck all zones in one click.
- + **Start the calculation** by clicking on "Calculate"
- + **Export results:** after running the calculation, select a format from the list (text file, text separated by commas, Access 2007 database, Excel, XML or PDF) and click the "Export" button
- + **Send results by email:** after running the calculation, select a format from the list (text file, text separated by commas, Access 2007 database, Excel, XML or PDF) and then click "Send by e-mail". Select or enter a recipient and choose whether to compress the file. **Caution:** to use this feature, you must have configured the mail settings from the "Preferences" menu of the software.
- + **Print the results:** after running the calculation, click the "Print" button
- + **Select to generate a subtotal per area** in the report by checking the box "Generate one subtotal per area"
- + **Select the sort criterion of users** by selecting it in the list (Name or Access Group)

EVENTS MENU


EVENTS DISPLAY

You can display a list of events in real time at the bottom of your screen by clicking on the "Display" menu and then "Event list".

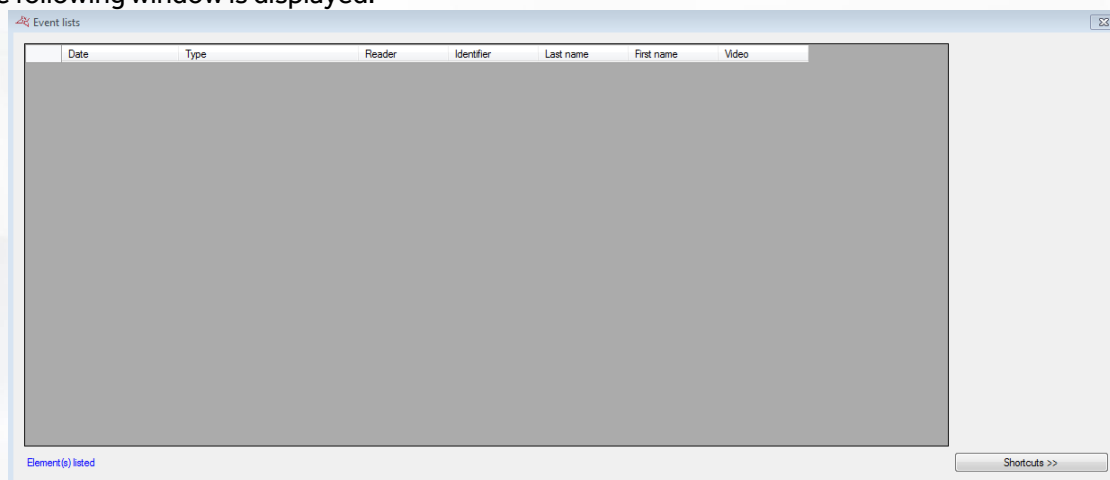


Date	Type	Provenance	Identifier	Last name	First name
------	------	------------	------------	-----------	------------

Caution: this list only contains events that have occurred since you started VISOR. To close the list, click on the "Close" button at the top-right of the list.

To view the last 2,000 events, click on the menu  and then "See list".
Note: to display more events, refer to the "History" tool.

The following window is displayed:



Date	Type	Reader	Identifier	Last name	First name	Video
------	------	--------	------------	-----------	------------	-------

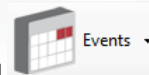
In this window, you can:

- + View the last 2,000 events.
- + Double-click on a user-related event to open its record.
- + Double-click on an identifier-related event to open its record.
- + Consult a recorded video (requires compatible video server and a setup of VISOR according to the recordings, refer Video Servers section)

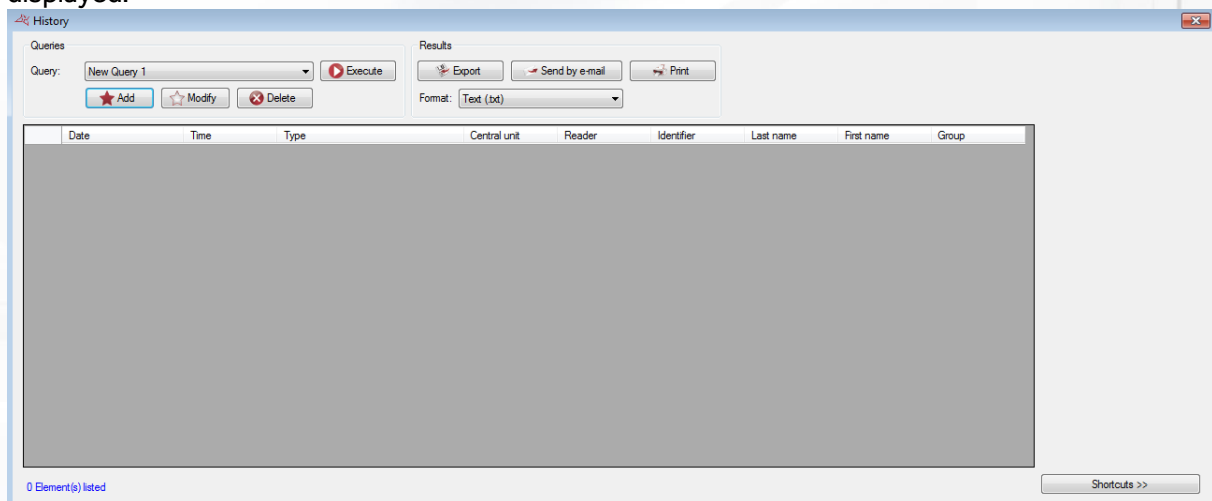
EVENT HISTORY AND REPORTS

You can sort the event history by configuring the fields to be displayed and filtering according to different criteria.

To sort the history, click on "History and reports" in the menu



. The following window is displayed:

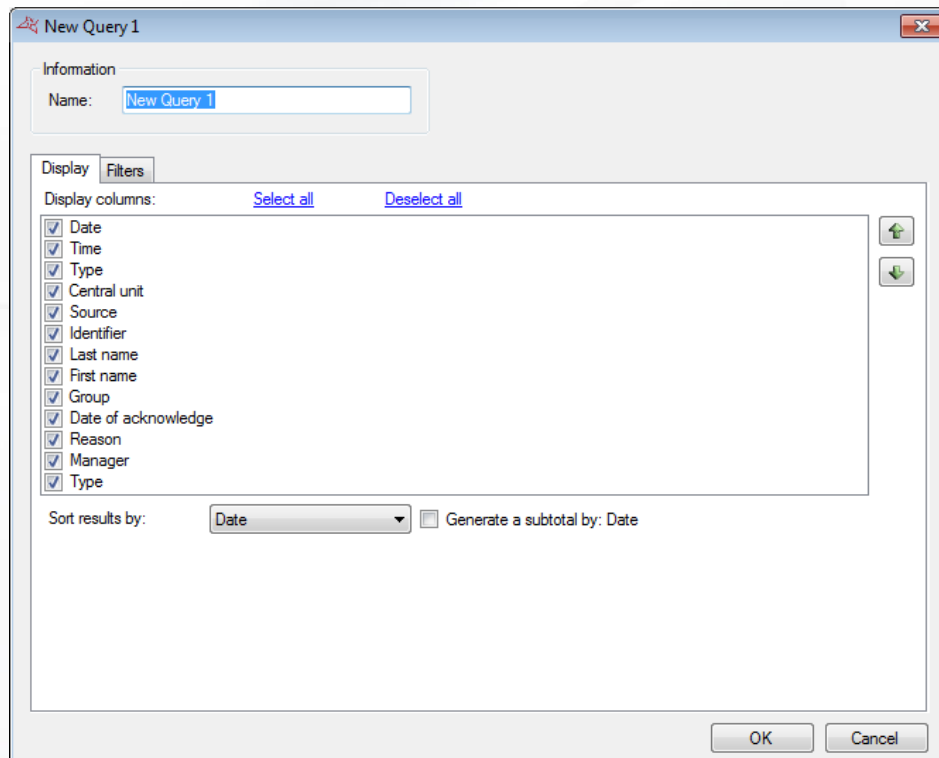


In this window, you can:



- + Add a query: click on the "Add" button and then configure your query.
- + Modify a query: select your query in the list and then click on the "Modify" button.
- + Delete a query: select your query in the list and then click on the "Delete" button.
- + Execute a query: select your query in the list and then click on the "Execute" button. The results will then be displayed.
- + Export the results of a query: after executing a query, select a format in the list (text file, comma-separated text, Access 2007 database, Excel, XML or PDF) and then click on the "Export" button.
- + Send the query results by email: after executing a query, select a format in the list (text file, comma-separated text, Access 2007 database, Excel, XML or PDF) and then click on the "Send by e-mail" button. Select or enter a recipient and choose whether to zip the file. Caution: to use this function, you must have configured the email settings in the software's "Preferences" menu.
- + Print the query results: after executing a query, click on the "Print" button.
- + If the selected event concerns a user, open the record by double-clicking on it or by clicking on the "Modify" button in the bottom-right corner if shortcuts are displayed (to show or hide shortcuts, click on the "Shortcuts" button).
- + If the selected event concerns an identifier, open the record by double-clicking on it or by clicking on the "Modify" button in the bottom-right corner if shortcuts are displayed (to show or hide shortcuts, click on the "Shortcuts" button).

MANAGING A QUERY

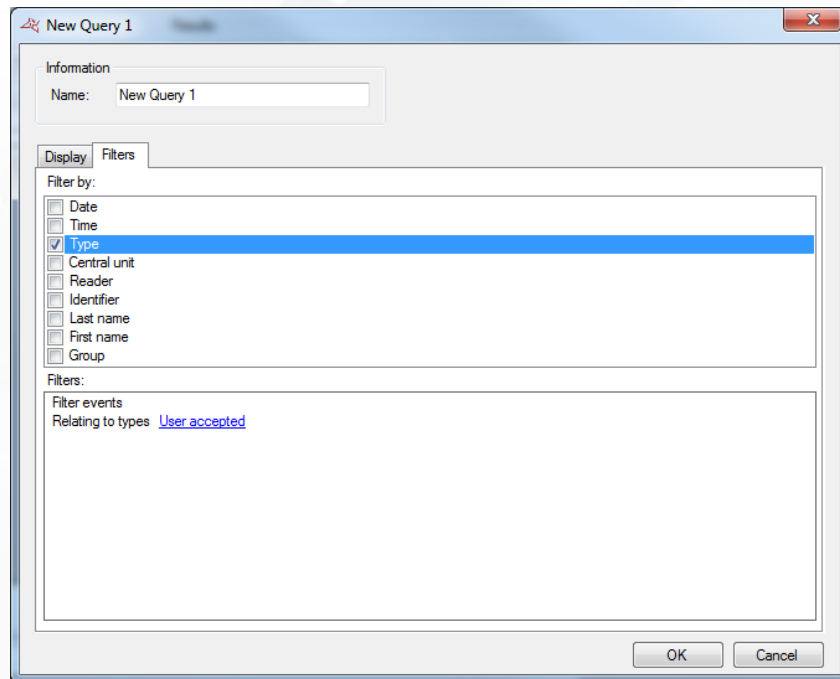
Display tab



From this tab, you can:

- + Name your query: enter the name in the "Name" field.
- + Check the fields that you wish to display in the history.
- + Use buttons  and  to change the order in which the result columns are displayed.
- + Select a sort for the results.
- + Check the "Generate subtotal" box to generate a subtotal depending on the selected sort criteria.

Filters tab



To filter the events to be displayed, click on the **"Filters"** tab. In this tab, you can define the following filters:

- + **By date:** filter events whose date is later than / earlier than / between the dates entered.
- + **By time:** filter events whose time is between the times entered.
- + **By type:** filter events whose type is part of your list.
- + **By central unit:** filter events whose central unit is part of your list.
- + **By Associated Source:** filter events to view events from your list of Associated sources (Readers, LPR server, Groups intrusion, Zones intrusion).
- + **By identifier:** filter events whose identifier is part of your list.
- + **By last name:** filter events where the last name starts with / ends with / contains your text.
- + **By first name:** filter events where the first name starts with / ends with / contains your text.
- + **By group:** filter events whose group is part of your list.
- + **By Acquittal date, by Cause, by Manager**
- + **By additional information** (if this feature has been activated in the "Event Configuration" menu).

To add a filter, simply check it. A new window is displayed, where you can fine-tune your search criteria.

To modify a filter, go to the list of filters (at the bottom of the window) and click on the **blue link** (example: [User accepted](#)). A new window is displayed, where you can fine-tune your search criteria.

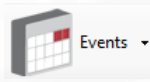
To delete a filter, simply uncheck it.

To filter users by last name or first name, check the "Ask on execution" box, so that the software prompts you to enter your text when executing the query.

Once you have entered your filters, click on **"OK"**. In the previous window, click on **"Execute"**. The results will be displayed.

DAYBOOK MENU

From the menu, click on



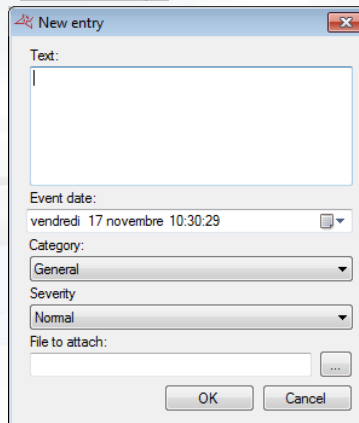
"Daybook".

From this window, you can:

- + **Add a new entry:** Click on "New entry".
For further information, Cf. chapter "Adding an entry"
- + **Define categories:** Click on "Categories".
For further information, Cf. chapter "Category management"
- + **Select display filters:** you can filter categories, managers or entry severity
- + **Select display period:** select the period during which the desired entry took place.
- + **Display results:** click on "View" to show the entries matching the selected criteria
- + **Export displayed results:** once you have displayed results, select a format from the list (text file, CSV file, Access 2007 database, Excel, XML or PDF) then click on "Export"
- + **Send displayed results by email:** once you have displayed results, select a format from the list (text file, CSV file, Access 2007 database, Excel, XML or PDF) then click on "Send by email" Select or type a recipient, and specify whether or not to compress the file. Note: In order to be able to use this feature, you need to have configured the email settings in the "Preferences" menu of the software.
- + **Print query results:** once the results are displayed, click on "Print"

ADDING AN ENTRY

From the "Daybook" window, click on "New entry".



The 'New entry' dialog box contains the following fields and controls:

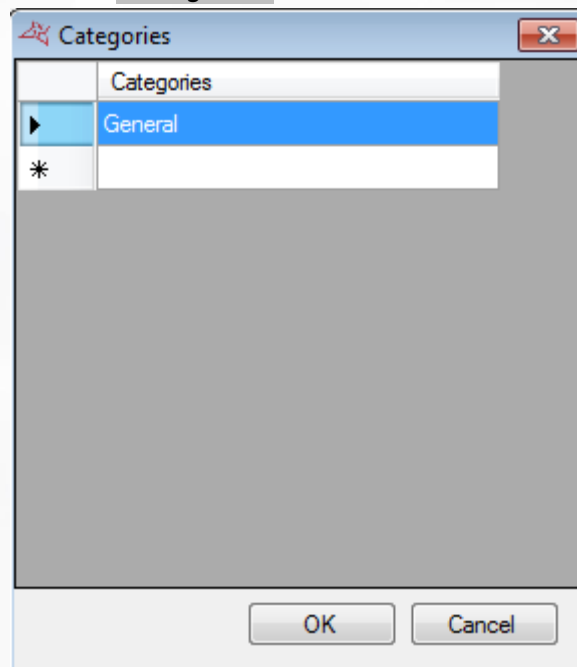
- Text:** A large text area for entering the event description.
- Event date:** A date and time selector showing 'vendredi 17 novembre 10:30:29'.
- Category:** A dropdown menu with 'General' selected.
- Severity:** A dropdown menu with 'Normal' selected.
- File to attach:** A text field with a browse button ('...').
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

From this window, you can:

- + Specify the title of the event
- + Select the date at which the event took place
- + Select the category of the event
- + Select the severity of the event
- + Add an attachment when applicable: the attachment must not exceed 1Mo.

CATEGORY MANAGEMENT

From the "Visitors" window, click on "Categories".



The 'Categories' dialog box features a list box with the following items:

	Categories
▶	General
*	

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

From this window, you can:

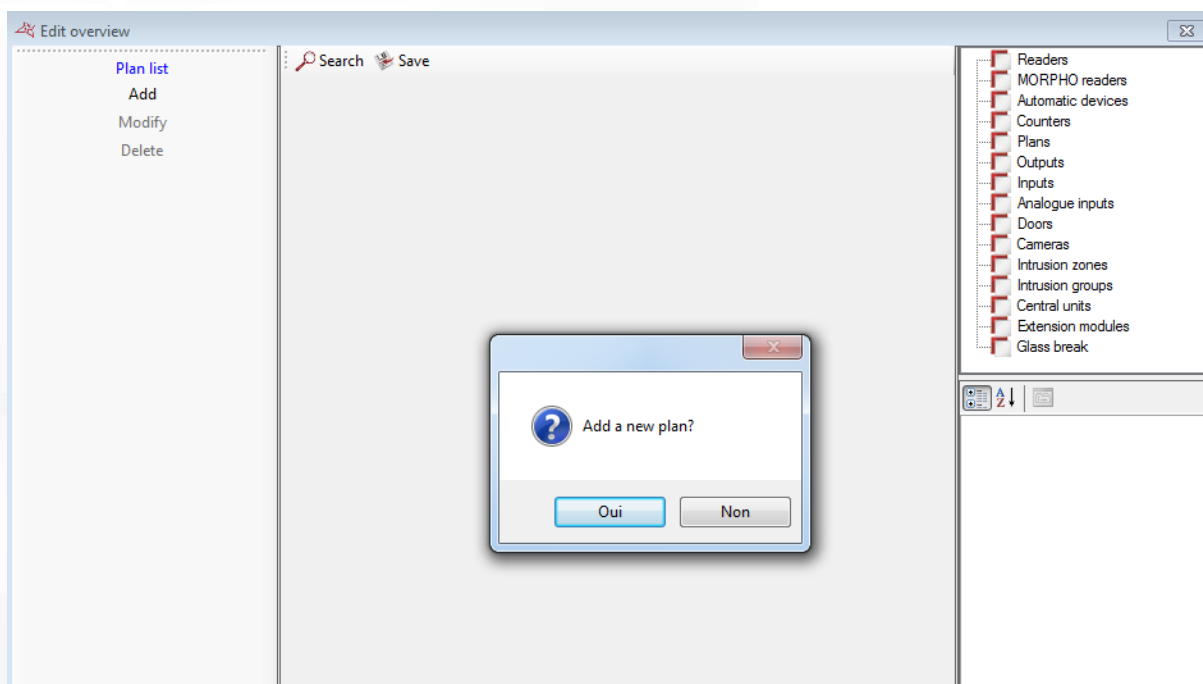
- + Add, modify or delete categories.

MAPS MENU

The overview allows you to view your installation's status in real time and in plan format.

EDITING THE MAPS

From the menu  select **"Edit"** to create your maps.

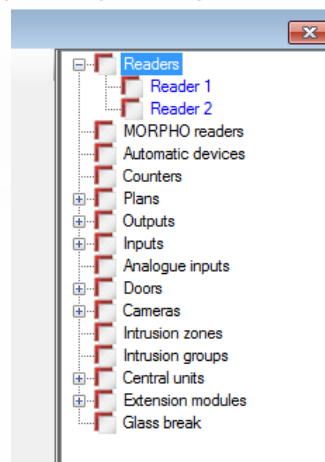


Your overview must have a plan. The first time, you are prompted to add a plan via a specific window or click on **Add** in the left-hand column and then search for a plan in jpg, bmp, gif or png format.

To add items to a plan, select the item in the list of items on the right side of the window and drag into the plan.

In the plan, you can **right-click on the icon** to see a preview of the item's different statuses or delete the item.

By selecting an icon in the plan, you can edit its parameters in the lower part of the right-hand column.



For a reader, you can:


- + Choose a background colour.
- + Show or hide an event window as soon as an event occurs on the reader.
- + Select the window position:

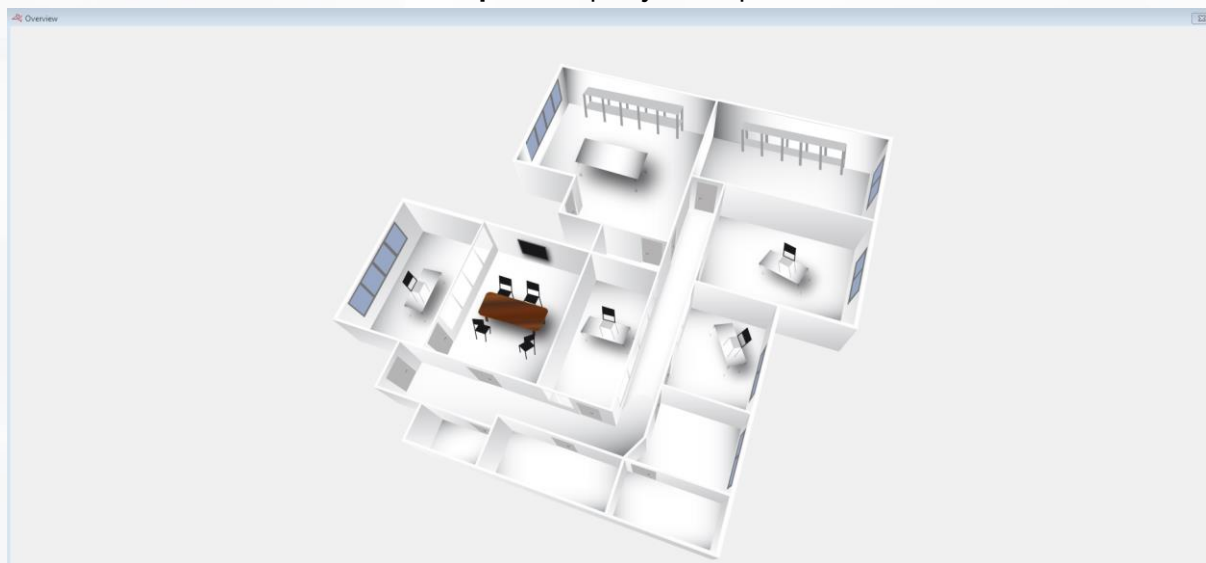


- + Change the image size.
- + Change the image.
- + Change the name.
- + Change the font.

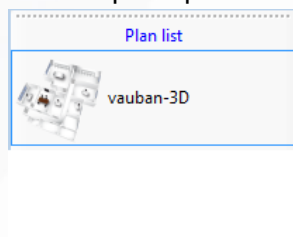
Configuration	
Colour	<input type="checkbox"/> 0; 255; 255; 255
Event Window	
Display	Yes
Window Position	Bottom / Right
Images	
Image Size	48; 48
Normal	<input type="checkbox"/> None
Break-in	<input type="checkbox"/> None
Door Blocked	<input type="checkbox"/> None
Free access	<input type="checkbox"/> None
Opening Maintain	<input type="checkbox"/> None
Closure Maintain	<input type="checkbox"/> None
Name	
Text	Reader 1
Text Colour	<input type="checkbox"/> 0; 0; 0
Font	Microsoft Sans Serif; 8
Supervision	
First plan	No

OPENING THE MAPS

From the menu  select **"Open"** to open your maps.




If you have several plans, you can select the required plan in the left-hand column:

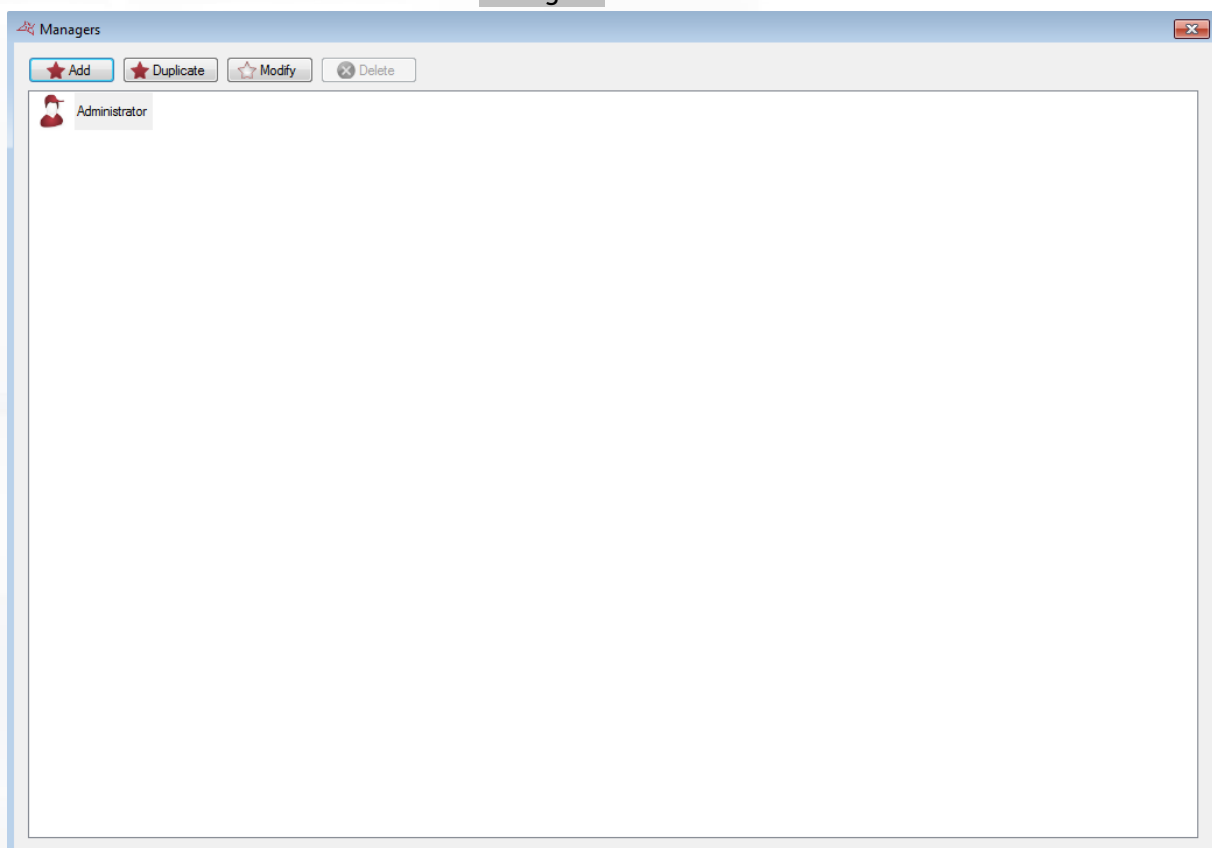


ADMINISTRATION MENU

The administration function is used to organise the software's managers. You can then adjust the access rights for each manager. A log is also available and provides a record of all events occurring between the start and end of a given session.

CREATING A MANAGER

In the menu  Administration ▾ click on **Managers.**



You can **add**, **duplicate**, **modify** and **delete** managers. The Administrator is the default manager and cannot be modified or deleted, since the Administrator represents the top-level manager.

Click on **"Add"** to create a manager.

From this window, you can enter the:

- + Last name.
- + First name.
- + Email address.
- + Phone number
- + Password.

Check "**The password may be changed**" to allow managers to change their password.

Check "**The password must be changed**" to force managers to change their password when opening a session.

Check "**Manager prohibited**" to ban the manager.

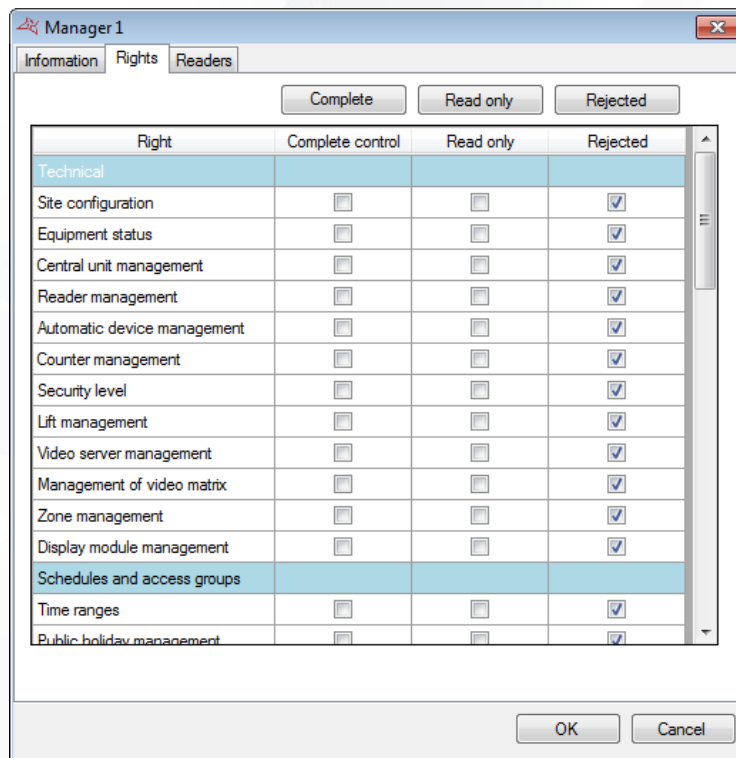
Check "**Manager using the SmartPhone application**" to allow managers to use the iPhone application (if this function is enabled).

Check "**Receive e-mail alerts**" so that managers will receive events by email. An email address must be provided.

Check "**Operator able to acknowledge**" to indicate that the acknowledgment window may be displayed for this operator.

Check "**Enable default window**" to choose a window to open when logging in.

All managers have rights determining their access and management of the software. To configure their rights, go to the "Rights" tab.



From this window, you can check all of the following columns with a **single click**:

- + Complete control: managers have no restrictions and complete access to all software functionality as the administrator.
- + Read only: managers have access to all software functionality, but cannot make any changes to the software.
- + Rejected: managers will be denied access to all software functionality and all their rights will be deleted.

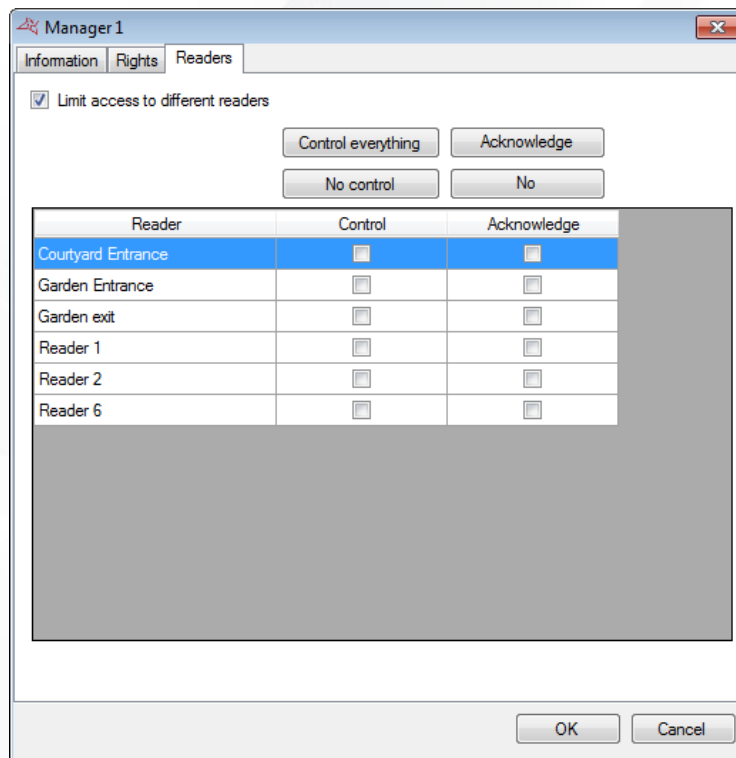
You can also reorganise managers' rights if they are not part of the same column. The rights available are as follows:

- + **Technical**
 - Site configuration
 - Equipment status
 - Central unit management
 - Reader management
 - Automatic device management
 - Counter management
 - Security level
 - Lifts management
 - Video server management
 - Video matrices management
 - Zones management
 - Display modules management
- + **Schedules and access rights**
 - Time ranges
 - Public holiday management
 - Lists of special days

- Access groups
- + Users**
 - Credentials
 - Users
 - Create users
 - User privacy
 - User movements
 - List of users
 - Re-cycle users
 - Data import
 - Attendance time
 - Attendance management
- + Events**
 - Event display
 - History and reports
 - Daybook
- + Maps**
 - Edit the maps
 - Open the maps
- + Administration**
 - Managers
 - Managers log
- + Updates**
 - Units, extension modules and software updates
- + Tools**
 - Event settings
 - Card printing templates
 - Preferences
 - Modules management
 - Company management
 - Automatic import
 - Shortcuts management
- + Software management**
 - Software closure

If you have additional modules, you will also find the different access rights to these modules in this window.

You can limit the control or acknowledgment on the readers. To set these permissions, go to the "Readers" tab



Check "Limit access to different readers" to filter the actions of this operator.

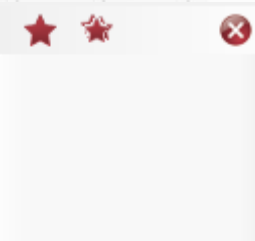
For each reader, you can indicate:

- If the operator can control the reader; in this case, it the reader can be opened from a synoptic, for example.

If the operator can acknowledge the reader: the acknowledgment window will be displayed for this reader.

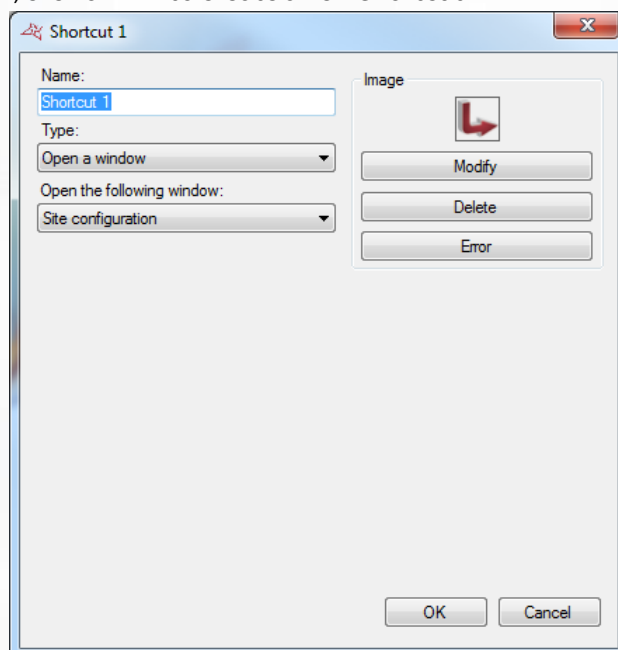
MANAGING SHORTCUTS

Shortcuts provide a very quick way of using the software both easily and effectively. You can carry out pre-programmed tasks with just a single click.



CREATE A SHORTCUT

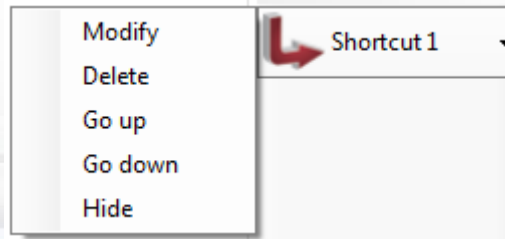
In the right-hand column, click on  to create a new shortcut:



From this window, you can:

- + Change the name.
- + Choose the type of shortcut.
- + Modify, delete or reset the shortcut image.

SHORTCUT CONFIGURATION



From this window, you can:

- + Modify a shortcut
Warning, changes apply to all managers
- + Delete a shortcut
Warning, deletions apply to all managers
- + Move a shortcut up or down
- + Hide shortcuts that you are not going to use.

Warning, Modify and Delete buttons apply to all managers. Up/Down/Hide buttons apply only to the current Manager.

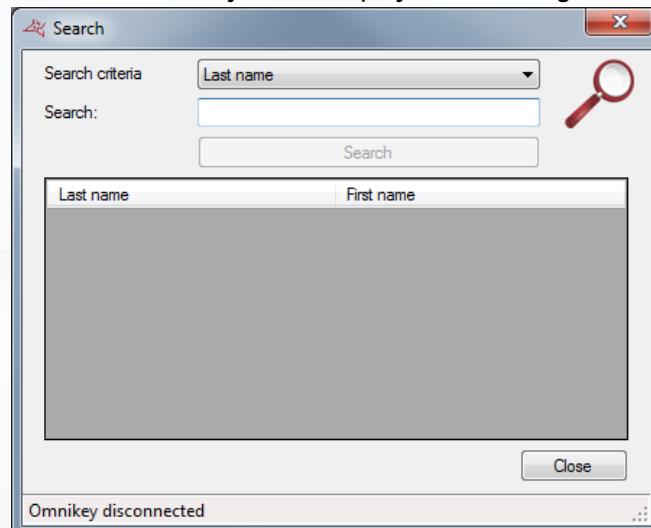
TYPES OF SHORTCUTS

1. **Open a window:** with this shortcut, you can open the following functions:
 - + Site configuration
 - + Equipment status
 - + Time ranges
 - + Public holidays
 - + Special days list
 - + Access groups
 - + Identifiers
 - + Users
 - + User creation
 - + User list
 - + Event list
 - + History and report
 - + Edit overview
 - + Overview
 - + Presence time
 - + Managers
 - + Security level
 - + Data import
 - + Video switcher
 - + Attendance management
2. **Create: with this shortcut, you can create:**
 - + A group.
 - + A time range.
 - + A list of special days.
 - + An identifier.
 - + A user.
 - + A manager.
3. **Creating users:** from this shortcut, you can open the user creation window.
4. **History:** with this shortcut, you can execute a predefined query in the Event history. This shortcut enables you to:
 - + Display the results.
 - + Print the results.

- + Export the results in the following format: Text (.txt), Comma-separated text (.csv), Access (.accdb), Excel (.xls) XML (.xml), PDF (.pdf).
 - + Define the location of the results on your PC.
 - + Email the file to a recipient. The file can be zipped and/or deleted after sending.
5. **User list:** with this shortcut, you can execute the same operations as the **History**, and the query must be predefined in the Listing.
 6. **Control readers:** with this shortcut, you can control one or more readers:
 - + Simple opening
 - + Return to Normal mode
 - + Opening maintained
 - + Closure maintained

The command can be executed on all readers or just specific readers.

7. **Search for a user:** with this shortcut, you can display the following window:



In this window, you can select one of the following search criteria:

- Last name
- First name
- Identifier

Then click on "Search". In case of search results, you can double-click on users to edit them.

8. **Video servers:** with this shortcut, you can **Display a camera** that has been selected in a list or a **Global event** from a Digifort video server that has been pre-declared in your site's configuration.
9. **Launch a program:** with this shortcut, you can launch another program on your PC. To do so, define the path pointing to the program.
10. **Force the importing of a module:** with this shortcut, you can automatically import a module. To do so, first configure the settings in Tools > Automatic import.

11. **Drive an output:** with this shortcut, you can control the output for a V-EXTIO module relay. The command is either to enable the relay or disable the relay.
12. **Change security level:** with this shortcut, you can change the software security level. You can choose between security levels 1, 2 and 3.
13. **Force automatic export:** with this shortcut, you can automatically export a module. To do so, first configure the settings in Tools > Automatic export.
14. **Set the display of a module:** with this shortcut, you can set the display of a module that has been selected in a list.
15. **Manage daybook:** display list or add new entry
16. **Drive an input:** with this shortcut, you can execute the same operations as the "**Drive an output**".
17. **Force database maintenance:** starts the database maintenance process, without waiting for noon or midnight.
18. **Present user management:** Allows you to start displaying, exporting or printing the presence user list for a specific area.

APPENDICES

LIST AND VERSION OF SDK INTEGRATED IN VISOR

Video stocker model	SDK version
Dahua	V 3.4.4
Digifort	V 7.0 or V7.2.1
Gigamédia	V 1.0.44
Hik	HCNetSdk V 5.3.5.25
Milestone	EngineManager V 3.8.0.3
Nuuo	V 3.1
Samsung (Hanwha)	V 1.44.0

SQL SERVER COMPATIBILITY

Visor is compatible with the following SQL server versions:

- + SQL Server 2005
- + SQL Server 2008
- + SQL Server 2012
- + SQL Server 2014