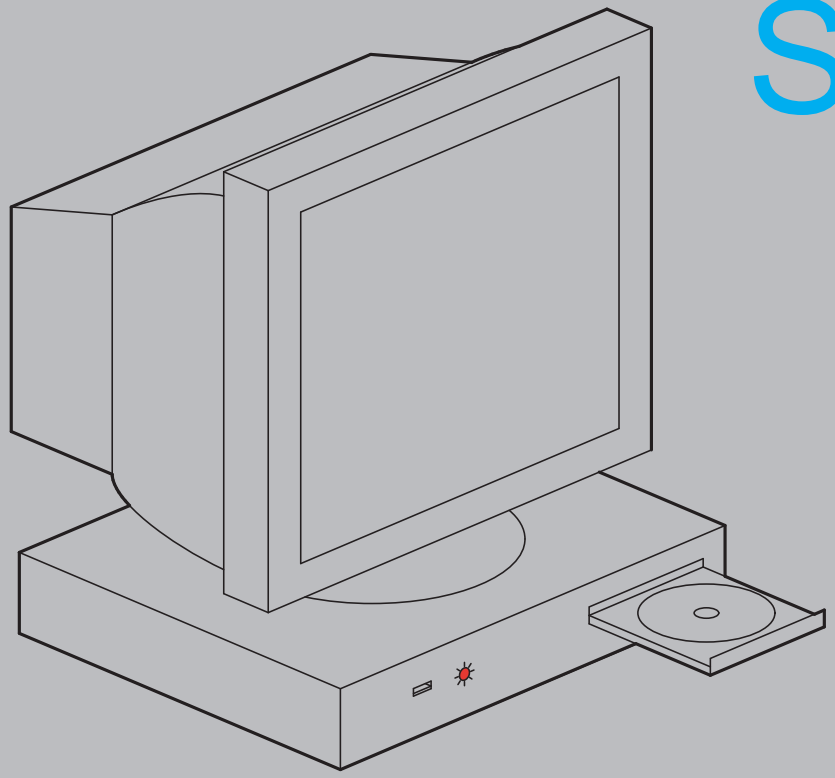
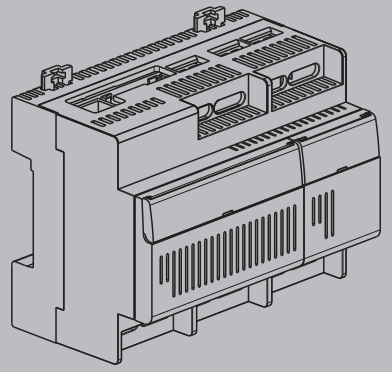
# Legrand Access System Software





USER GUIDE

legrand®

# Introduction

**The Legrand Access System Software package is part of a series of tools developed by Legrand to manage building access control in the tertiary sector.**
**The Legrand Access System Software package comprises the software (with its unlocking key) and a Webcam (useful to customise users), and is the ideal administration tool for a site that has several controllers.**

**This highly complete package will enable you to manage building entry rights, view entry statuses in real time on a plan, define or modify entry rights, and consult the events history for the site.**

**The package can manage up to 10,000 users and 256 doors, using badge readers, code keypads or fingerprint readers.**

**This user guide contains the information you will need to configure your site, as well as details of useful functions that will help you to use the system more effectively.**

**Nota :**

If an installation is managed using LEGRAND ACCESS SYSTEM SOFTWARE, you can no longer manage it using LAS JAVA. The two applications are incompatible and cannot be used together.

# Contents


## I - INSTALLATION ..... p. 5

Software ..... p. 5

Installing the site ..... p. 8

Creating system users (Administrators or users) ..... p.10

## II - MANAGING THE SITE ..... p. 13

**This section explains the essential functions for using the software**

Creating controllers ..... p. 13

Configuring readers ..... p. 21

Time periods ..... p. 25

Creating a group ..... p. 27

Creating an installation user ..... p. 29

## III - USING THE APPLICATION ..... p. 33

**This section explains the functions used in daily installation management**

Searches and analysis tools ..... p. 33

List of events ..... p. 36

Control and overview ..... p. 37

Opening an installation ..... p. 39

Closing the session ..... p. 39

IP camera ..... p. 39

# Contents


## IV - OPTIONS ..... p. 41

This section presents the additional functions of the software

“Access control” tab ..... p. 41
“Technical” tab ..... p. 43
“Administration” tab ..... p. 45
- Log ..... p. 45
- Personalising users ..... p. 45
- Quick data recovery ..... p. 46

“Extension” tab ..... p. 47
- Learning ..... p. 47
- Creating a printable badge format ..... p. 48
- Site code ..... p. 49
- Configuring automatic backup ..... p. 49

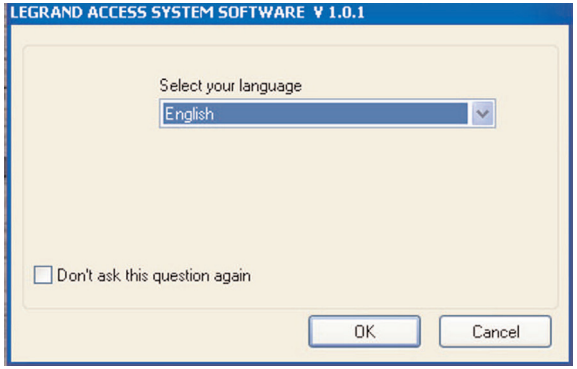
# I - INSTALLATION - Software

## Software

To validate the software for utilisation on your system, you must insert the electronic key supplied with the package into one of the installation controllers (see Legrand Access System Software manual).
Operation without a protection key is visible in the status bar (Demo). In this case, the application cannot be reconfigured and the events recording function is deactivated.
Insert the installation CD, select “Legrand Access System Software” and then click on “Software” to install.
Click on the LAS Software icon on your desktop to run the application.

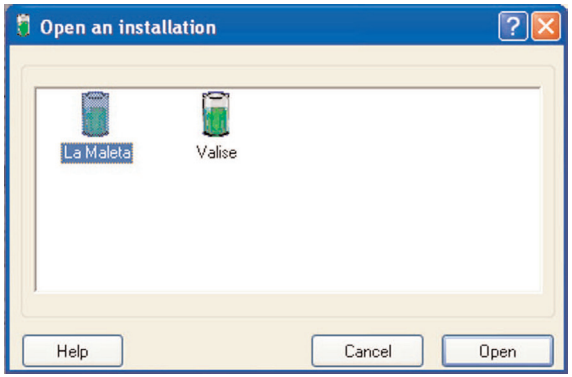
Compatible with Windows 2000, XP, Vista, Seven.
You must have administrator rights to be able to install the software.
The default folder for the installation is C:\Program Files\LAS\LAS Software. You may select another folder.
The software user must have read/write rights for the selected folder.

Select your language.



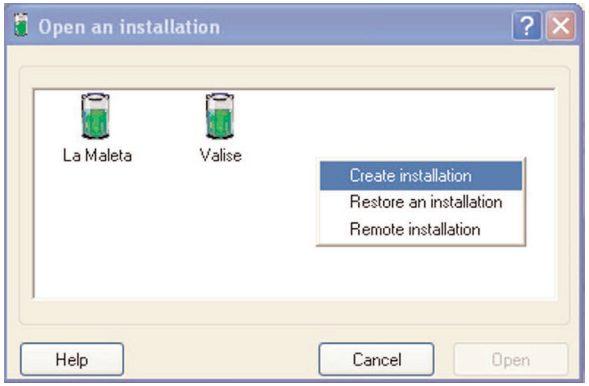
# I - INSTALLATION - Software

This opens the installation creation and management window.




There are several ways of creating an installation:

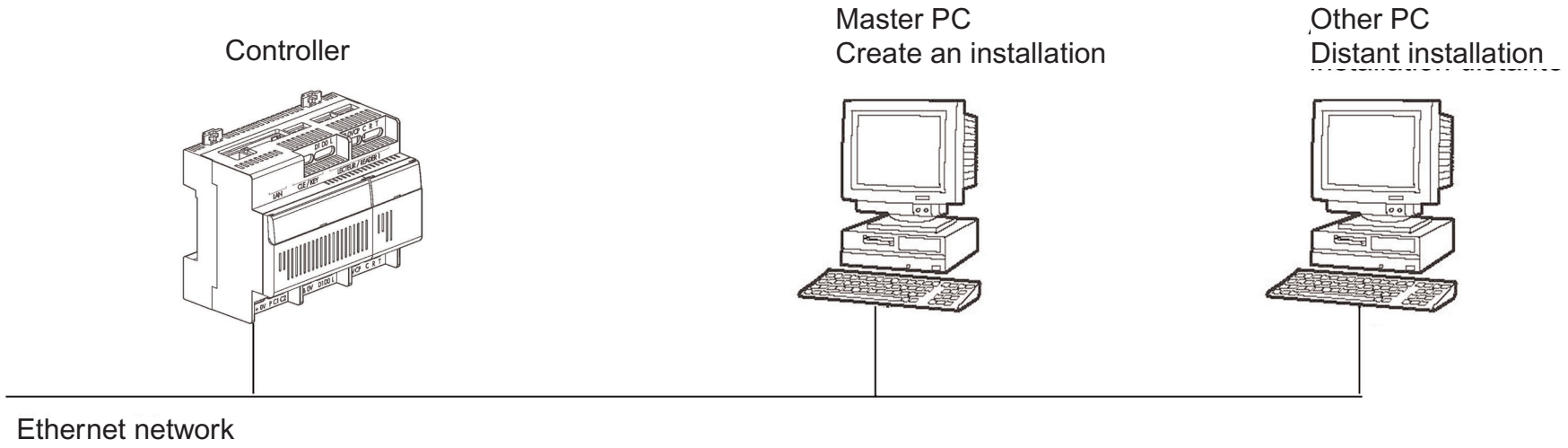
- You can click on “Create a new installation”
- or right-click in the window to open a menu.




- Create an installation: creates a new installation.
- Restore an installation: Opens an installation that has previously been saved.
- Remote installation: A remote installation (e.g. a PC) is connected to a master PC data source and can modify it. This type of installation can only communicate with control units through a master PC that is operational (with LAS Software running). If this is not the case, the changes made by the subscriber terminal will only be sent to the controllers when the master terminal is restarted.

# I - INSTALLATION - Software

If you want to manage an installation from several PCs, you must create an installation on the main PC and open a remote installation on the other PCs. (maximum of 5 remote PCs)

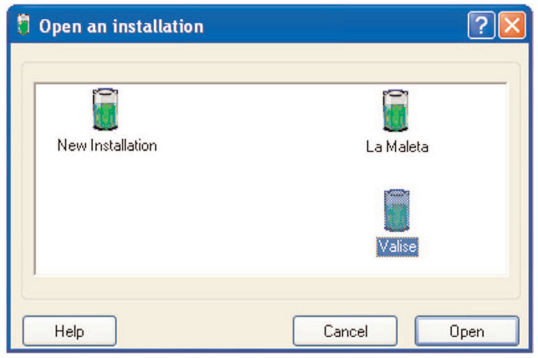



**Note:**

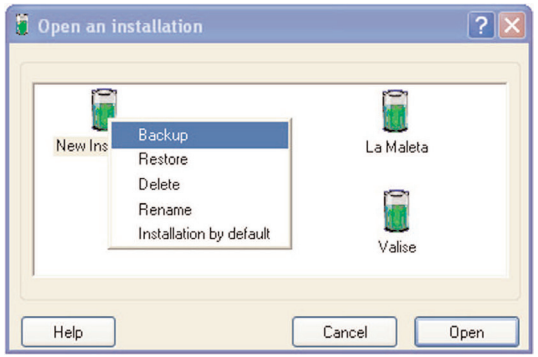
If installing remotely, the main PC must be powered up and connected to the network.

## Installing the site

When the new installation has been created, an icon is displayed in the window.




Right-click on this installation to open a menu.

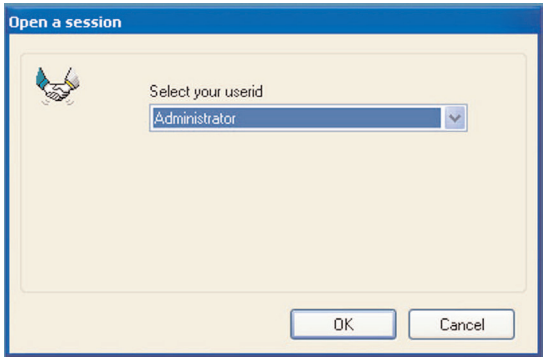



- Save: saves the selected installation in .dbz format, either in local mode or on the company LAN. All the installation data is saved: Controller configuration, groups, users, etc.
  Caution: the file name must be the same as the name of the installation.
- Restore: Opens an installation that has been previously saved.
- Delete: Deletes the selected installation.
- Rename: Renames the selected installation.
- Default installation: Defines the default installation. In this case, after a delay of 10 seconds, the software starts up automatically with this installation.

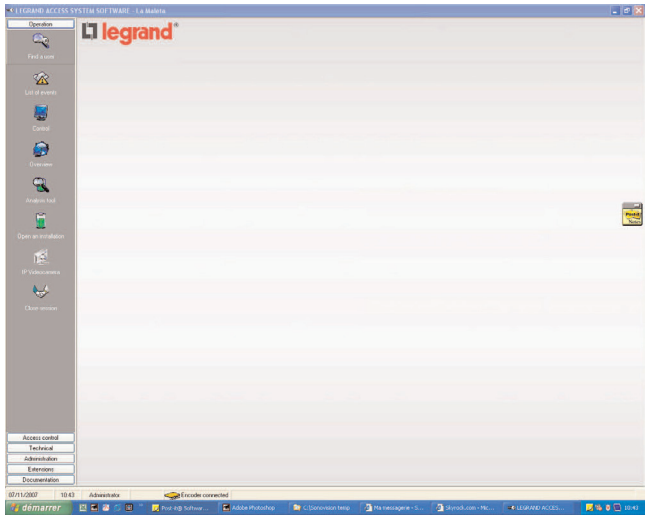
Click on the “Open” button to open the selected installation.

# I - INSTALLATION - Installing the site

This leads to a prompt to open a session. On first login, only the Administrator session will be available. Once users have been created, these will also be displayed in the session opening prompt.



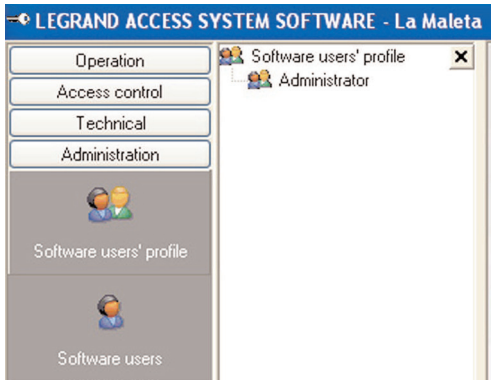

Click on OK to open the session.

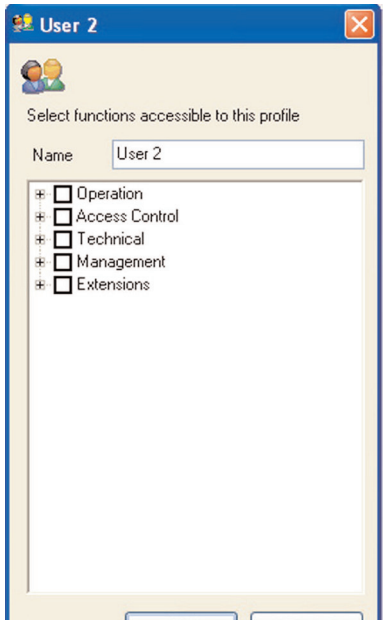


# Creating system users (Administrators or users)

## Creating a software user profile

Select the “Administration” tab, and then click on the “User profiles” icon.




Then click on “User profiles” and on “Create a profile”.

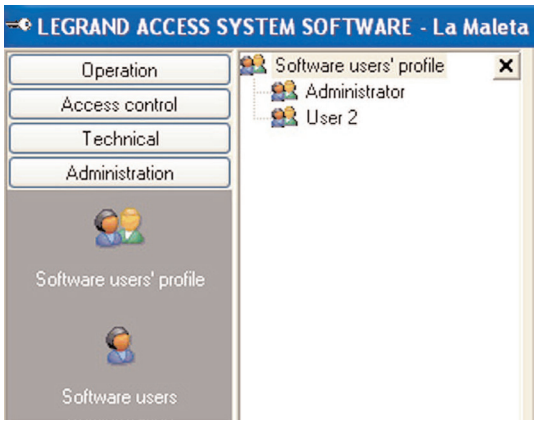
- Name: Name of profile or action level on site.

Next select the rights attached to this profile by selecting the corresponding boxes in the list.
Creating a profile also involves creating a first user for this profile.
Deleting a profile also deletes all users that have this profile.

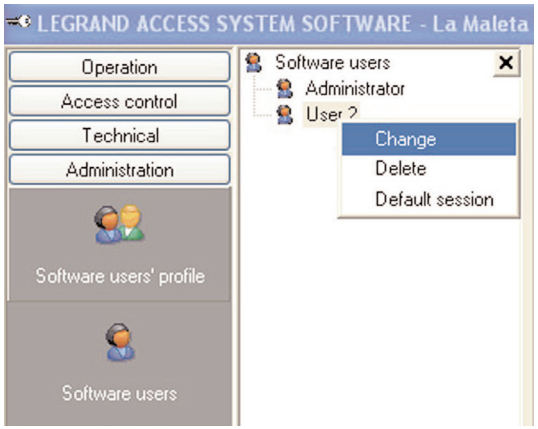
# I - INSTALLATION - Creating system users (Administrators or users)

## Creating a software user profile

Select the “Administration” tab, and then click on the “User profiles” icon.

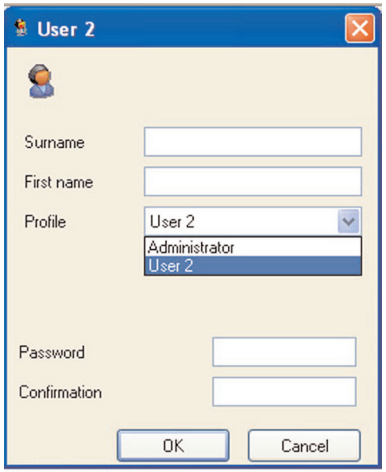



Then click on “User profiles” and on “Create a profile”.



# I - INSTALLATION - Creating system users (Administrators or users)

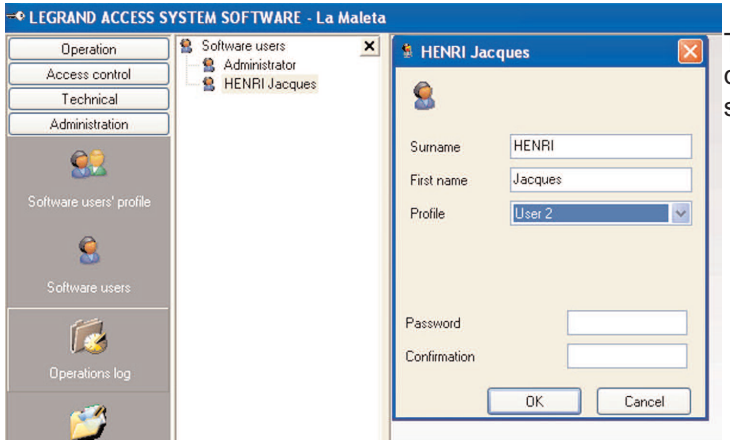
Click on “Change”.




- Name and first name: Name and first name of user being created.
- Profile: Select the profile for this user.
- Password: A password can be assigned to this user if desired.

The basic “Administrator” profile can only be changed by the administrator himself.
The basic “Administrator” user has all the rights defined for the installation. It is therefore recommended that a password be defined for this user whenever a new installation is created.

Click on “OK” to confirm: the changes made are then incorporated in the structure displayed.




The session opening prompt will now display all registered users. It is now possible to define one of the users as the default user. Click on the user name, then on “Default session”. This user name will then be displayed by default when the application is started up.

# II) MANAGING THE SITE- Creating controllers

This section describes the operations necessary for use of the software.

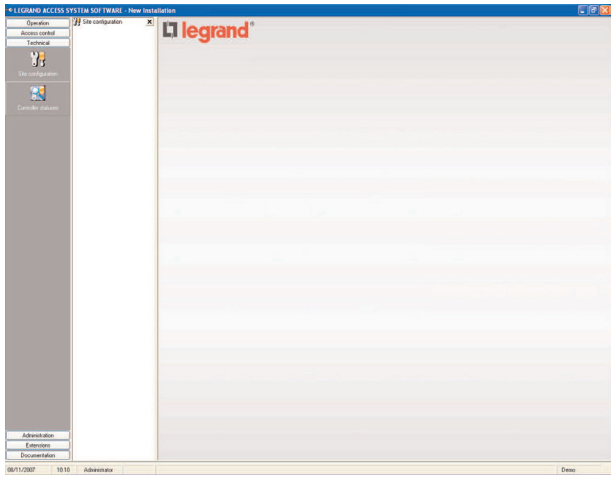
**Creating the site**

Site creation is based on a logical sequence of phases that set up the site. The setup logic is shown in the list of phases below (these phases will be described in detail later in the manual).

- Create the site controllers and the corresponding readers,
- Create the time periods and define the public holidays,
- Create the access groups,
- Create the site users.

## Creating controllers

Click on the toolbar on the left of the screen, then on the “Technical” tab.



# II - MANAGING THE SITE - Creating controllers

Click on “Configure site” and select “Create a controller”.

**Nota:**

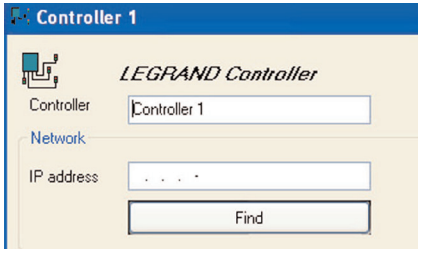
The controller is supplied with the following plant configuration:
- IP address (modifiable): 192.168.1.150
- MAC address (fixed): example: 0-20-4A-93-77-99 (marked on controller)
- Sub-network mask (modifiable): 255-255-255-00
- The controller user language is selected based on the regional parameters defined for the PC.

When creating a controller, there are two possibilities:

- Either the controller is connected to the LAN
- or it is connected directly to the PC.

## Controller connected to LAN

### Finding controllers present on the network




When the application is started up, it identifies the controllers present on the network, and the list of controllers detected is then displayed.

# II - MANAGING THE SITE - Creating controllers

There are two possible statuses for a controller connected to the LAN:

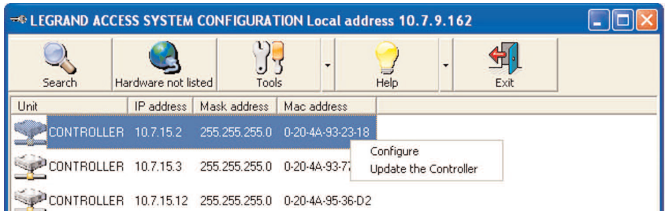
The Controller is in the correct sub-network mask. In this case, its IP address and its MAC address are shown, and its advanced properties can be configured.

The Controller is not in the correct sub-network mask and only its MAC address is shown.

New searches are initiated by clicking on

**Configuring controllers**

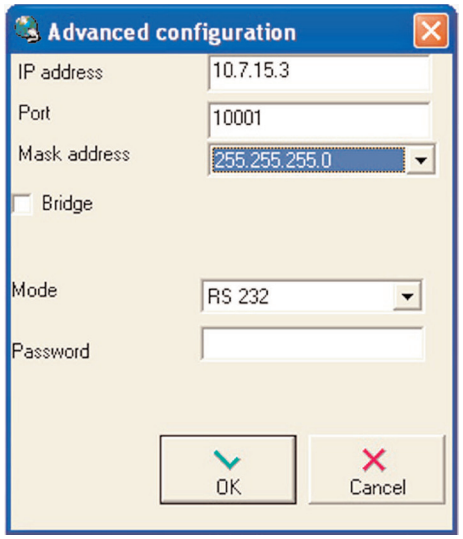
Right-click on one of the units in the list. The setup menu corresponding to the Controller's status is then displayed:




To access the setup window, click on "Configure".

# II - MANAGING THE SITE - Creating controllers

Setup window:



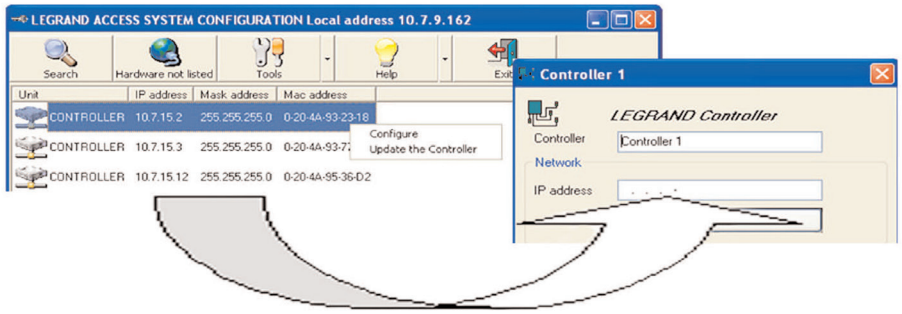

- Controller IP address
- Controller IP port (for Legrand Access System Software, the port must be 10001)
- Sub-network mask
- Select this box to configure a bridge
- Communication mode (must be RS232)
- Password: enter a password to protect access to the Controller IP configuration (this password is not related to that of the Legrand Access System JAVA or Legrand Access System Software). The pass word prevents the IP configuration from being changed by anyone else and is not mandatory.

If the controller is not in the correct sub-network mask, then a valid address will have to be configured for it (generally, the first 3 digits of the address are those of the host PC address, and the last digit must be unique on the LAN.

Example: If your PC address is 192.168.0.2, then the Controller address must be 192.168.0.X where 1<X<255 and X≠2).

# II - MANAGING THE SITE - Creating controllers

With the Controller configured in the correct sub-network mask, its setup parameters can be imported into Legrand Access System Software simply by dragging and dropping from LAS Configuration to LAS Software.




Do not enter the IP address directly into the administrator window.

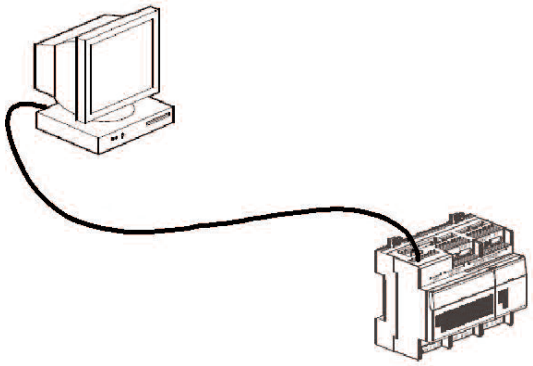
Assigning an address directly

If another PC has just taken an address that is identical to that of the controller, thus preventing any communication with the hardware, or if, for any other reason, the Controller cannot be detected and doesn't respond, even to a ping, then it is still possible to at least change the system address, as follows:
1- Note the MAC address shown on the Controller housing.
2- Click on the button "Hardware not listed"
3- Enter the MAC address in the command window.
4- Confirm and wait for the Controller to restart.
5- Run a search.

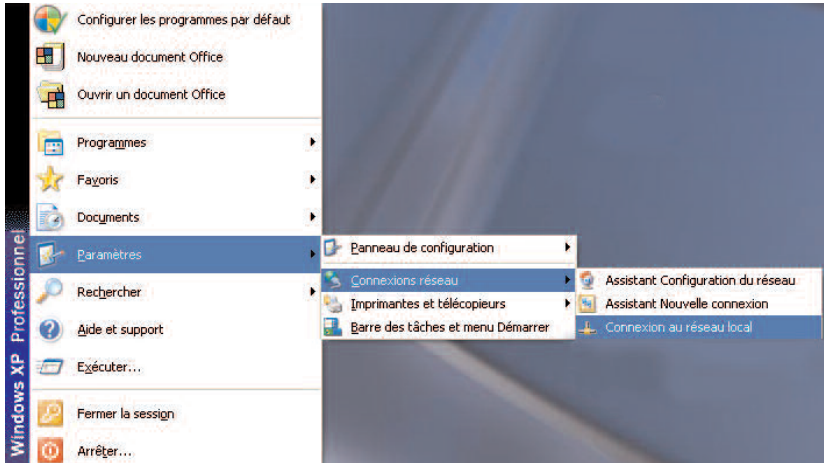
# II - MANAGING THE SITE - Creating controllers

## Controller connected to a PC

PC environment installed: Ethernet cable (crossed).



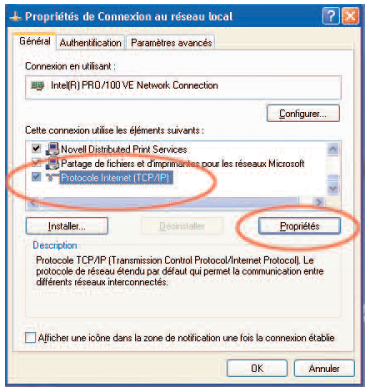
The screenshots presented below were taken on a PC running Windows XP.
They are just examples, and can vary depending on the operating system used.
Open the network configuration:



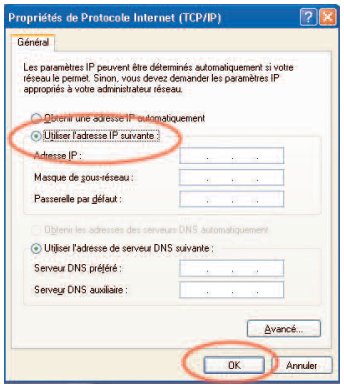
# II - MANAGING THE SITE - Creating controllers

Find the TCP/IP line corresponding to your Ethernet board in the “General” tab.

Click on


In the “Internet Protocol Properties (TCP/IP)“ window, select “Use the following IP address”, and then enter the address, for example 192.168.1.151 (different from 192.168.1.150), and sub-network mask 255.255.255.0.

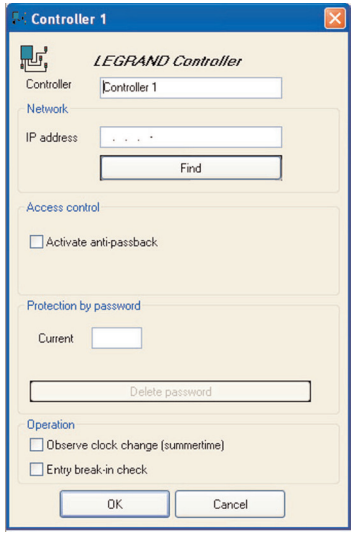



Click on


To finish configuring the controllers, repeat the procedure from operation A1 in this section.

# II - MANAGING THE SITE - Creating controllers

## Controller parameters



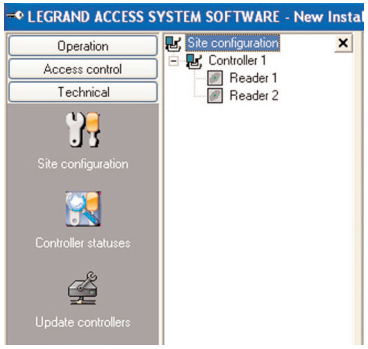

- Controller: Renames the controller.
- Network, IP address: Enter the controller IP address or click on find for automatic detection (see “Configuring controllers”).
- Access control: Anti-passback, anti-timeback (see note below).
- Protection by password: A password can be defined to protect access to the controller.
- Application of clock changes: Automatic application of summer time and winter time. If this option is not selected, the controller time is synchronised with that of the master PC when the LAS Software is started up.
- Break-in detection input: Describes the type of the controller housing self-protection contact.

### Nota :

Anti-passback: One reader can be configured in entry and another in exit. The anti-passback function means that an entry-exit cycle must always be respected (a badge cannot enter if it hasn’t gone out through an exit).

The anti pass-back function is only active if the “entry” reader and “exit” reader are connected to the same controller.

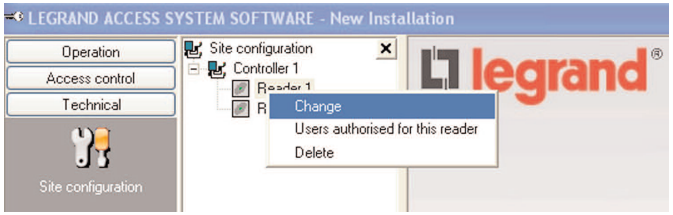
Anti-timeback: Is the time during which a user cannot enter again, after having entered a first time.



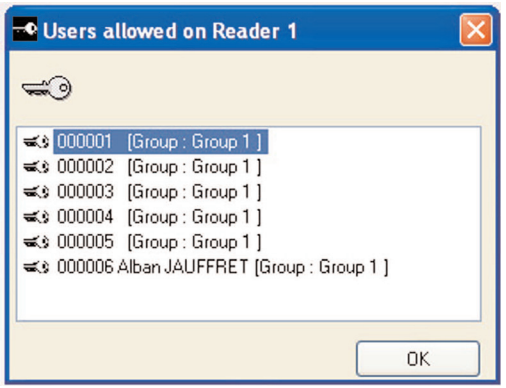

- You can then configure the readers.
  If only one reader is connected, you can delete the unused reader (select it and click on “Delete”).

## Configuring readers

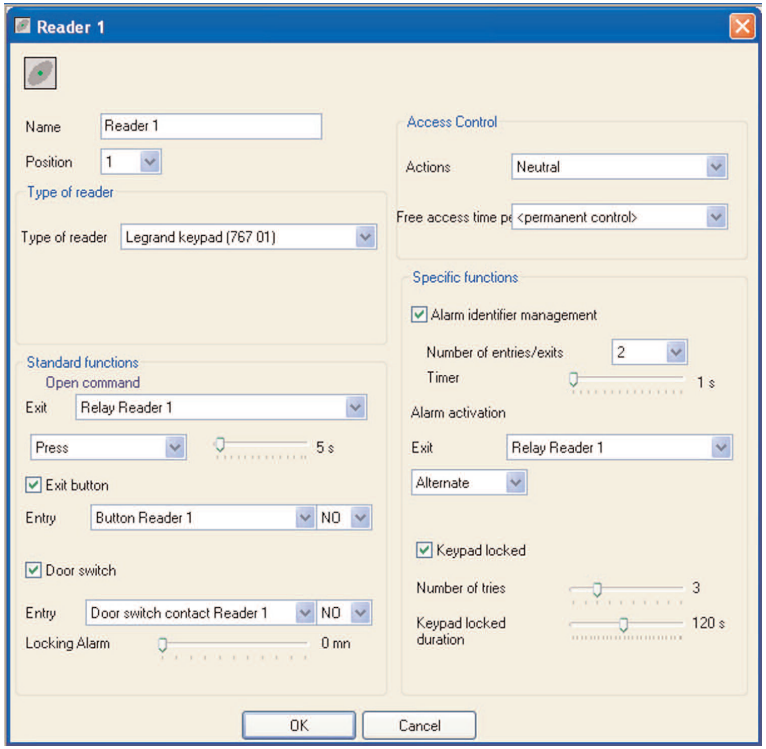
Select the reader to be configured and click on “Modify”.




- Modify: See configuring a reader.
- Badges accepted by this reader: List of badges assigned to the reader (see below).
- Delete: Deletes the selected reader.



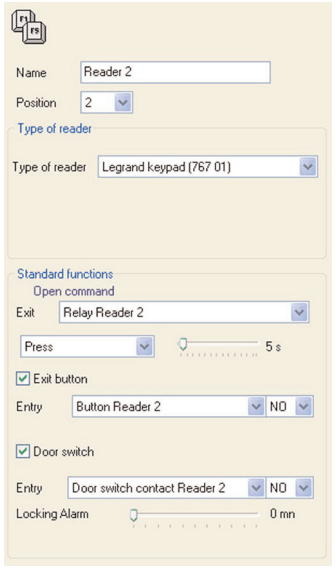
The window below is then displayed.



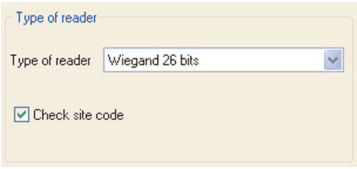
# II - MANAGING THE SITE - Configuring readers

## Configuration detail.

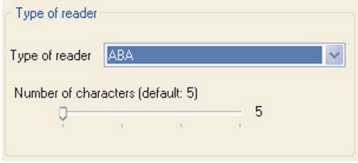
Left side of screen.




- Name: Name assigned to reader.
- Position: Reader 1 or 2 (the application automatically assigns the reader number as a function of its physical position on the controller).
- Type of reader: Assigns a type to the selected reader. A Wiegand 26-bit reader is suitable for Wiegand output readers such as HID® readers and equivalent. This type of reader enables the site code to be checked. To do this, select the “Check site code” option (see screenshot below).
- Latch control: Configures the relay that will be used by the reader, and the opening time (alternate or pulsing mode from 1 to 99 seconds).
- Button: Configures the input that will be used to control the button on the reader, and its type (NO: normally open or NC: normally closed). This function is mainly used on the exit from a “security” zone.
- Door contact: Configures the input that will be used to test the status of the door contact (used to detect any break-ins) and the locking time, from 1 to 99 minutes (after this period, a door remaining open following a programmed opening will generate a “door locked” event or Automatic system process).
  Deselect this option if there is no door contact.



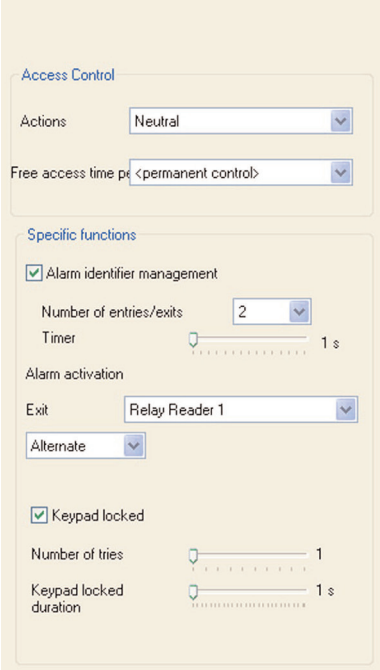

- For Wiegand 26-bit readers:
  To configure the site code, go into the “Extensions” tab, click on the “Site code” icon and then define your site code.




- ABA reader: Is suitable for readers with “clock & data” output. With this type of reader, you can select the number of last characters used to identify users (between 5 and 8 characters). For further information, contact your Legrand after-sales department.

# II - MANAGING THE SITE - Configuring readers

Right side of screen.



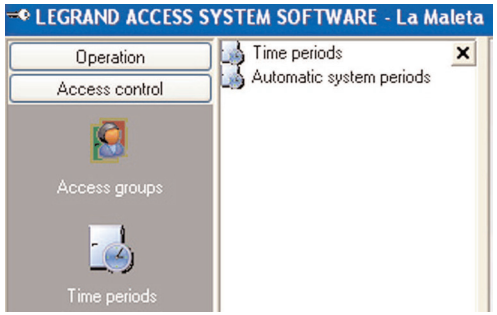

- Mode: Neutral by default. Entry or exit may be selected for “Anti Pass-back” operation.
- A free access period (if necessary): during this period, the reader is permanently in open status.
- Alarm identifier detection: This function is used for an “Alarm” identifier (identifier for which the “Alarm identifier” box is selected) to be able to activate one of the Controller outputs. To set this function, configure the number of entries/exits of this identifier, the time required by the identifier to complete this number of entries/exits (1-15 secs), the output to be used to control the alarm, and the alarm delay timer (from 1 to 99 seconds, or in alternating mode). The timer value can be finely adjusted using the keypad arrows.
- Integrated keypad management: Allows a keypad to be linked to the other reader on the administrator, to obtain badge + keypad management.

# II - MANAGING THE SITE - Time periods

## Time periods (accesses and automatic systems) and public holidays

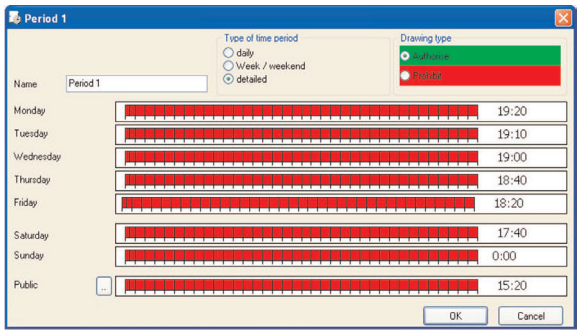
### Time periods

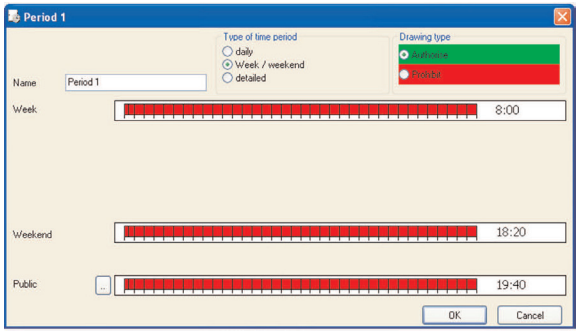
Go into the “Access control” tab and click on the “Time periods” icon (time periods are configured in the same way for both entries/exits and automatic systems).

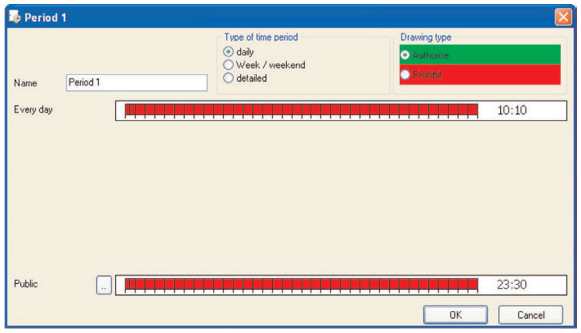



Next create your time period. There are three types of setup:

- Daily,
- Week/WE,
- Detailed.

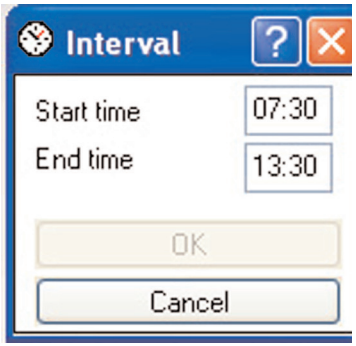


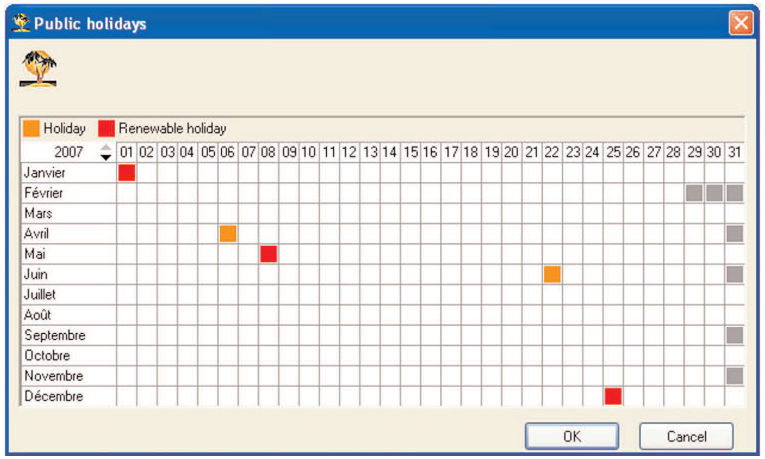
# II - MANAGING THE SITE - Time periods

Changes are applied by right-clicking and selecting the periods (authorised in green, prohibited in red).
To fine-tune a green period, right-click on it. This opens a window in which the exact times required can be entered.




Time periods are used to define the control periods for users and/or groups.
Authorised zones (in green) represent the reader free access times (permanently open).
Automatic system time periods are used to define and configure automatic systems, and to define the control periods for readers, keypads and finger-print readers.

## Public holidays

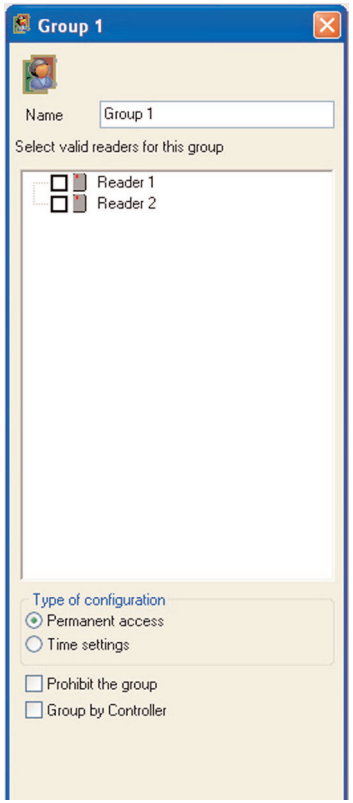



• Click on the “Public holidays” tab, and then on the appropriate dates to define them as public holidays. These dates will be displayed in orange. If you click a second time on the same date, it will be defined as renewable (displayed in red), i.e. it will automatically be applied every year.

Public holidays take precedence.

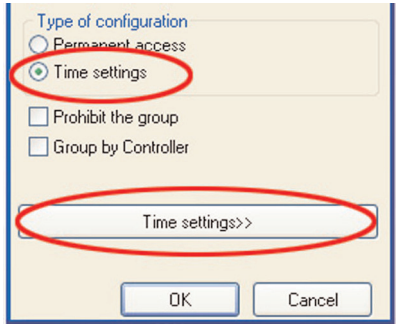
# Creating a group

Go into the “Access control” tab, click on the “Access groups” icon and create a group.



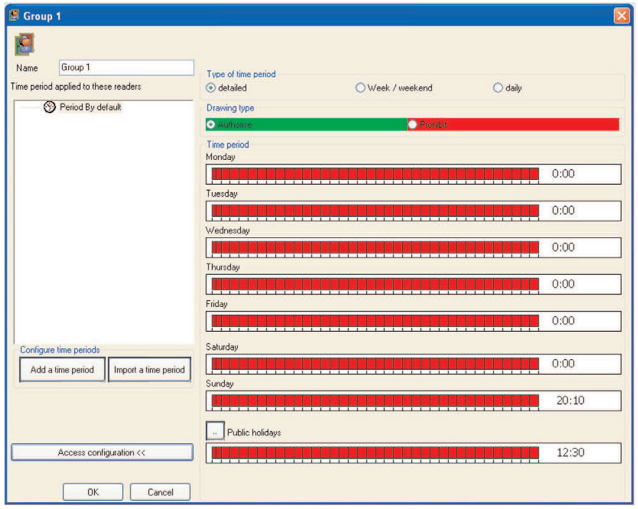

- Name: Assign a name to the group.
- Select the readers for this group: Assign the appropriate readers to the group.
- Type of configuration: Permanent access or time periods configured. If “Time configuration” is selected, a button is displayed that enables a time period to be assigned or created for this group (see below).
- Prohibit the group: Prohibits access for the entire group on the selected readers.
- Group by controller: If this option is selected, the controllers are displayed in the window. If this option is not selected, only the readers are displayed.

When “Time configuration” is selected, a new button is displayed.



# II - MANAGING THE SITE - Creating a group

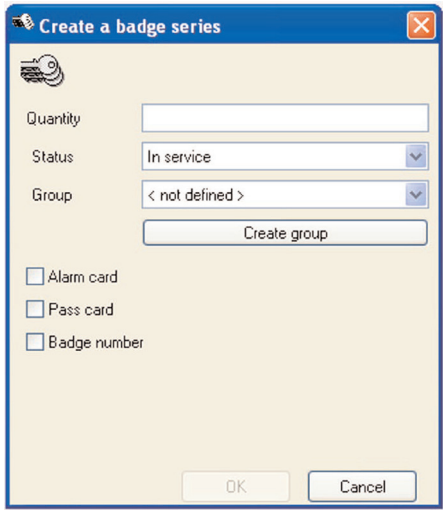
Clicking on this button opens a new window.




• To define the time period assigned to a group, the period must be created and the times defined, or a previously defined period may be imported (“Access control” tab / “Time periods”).
Then the corresponding readers must be assigned to the time period by dragging/dropping them under the period.
A time period with no reader assigned to it is not saved by the application.
The default time period doesn’t have to be retained. If it isn’t assigned to any reader, it will be deleted.

## Creating an installation user

Go into the “Access control” tab, click on the “Users” icon and create a series.

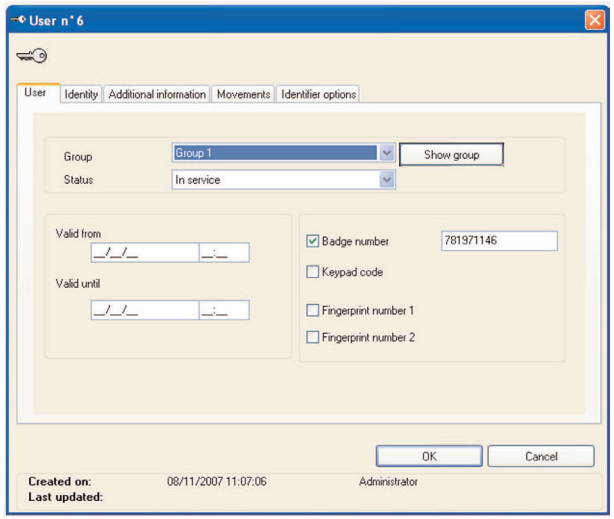



- Quantity: Number of users in the series being created.
- Status: Active or suspended.
- Group: Assign a group to this user series.
- Alarm badge: Badge that activates or deactivates an alarm.
- Pass badge: Badge that will not be blocked by the anti pass-back function.
- Badge number: Assign a badge number to the user.

# II - MANAGING THE SITE - Creating an installation user

When the series is created, click on the users to complete the corresponding information:

**- User tab:**

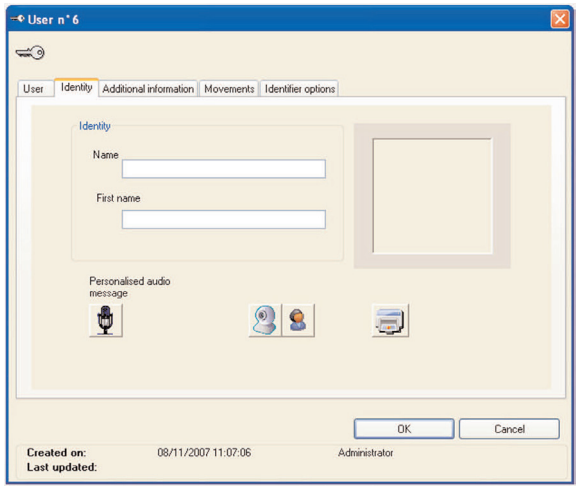



- Group: Assign a group.
- Status: Valid, Suspended, Stolen.
- Valid from / to: Assign “valid from / to” dates - times to the badge (for example for an external visitor).
- Badge number: Enter the badge number shown on the Legrand badge.
- Keypad code: Enter the valid code on the keypads to be used by the users.
- Fingerprint number 1: Enter the number of the recorded fingerprint in the biometric reader(s).
- Fingerprint number 2: Enter the number of the recorded fingerprint in the biometric reader(s).

**Note:**

- A time must be entered.
- The validity start date/time must be later than the current time.

**- Identity tab:**



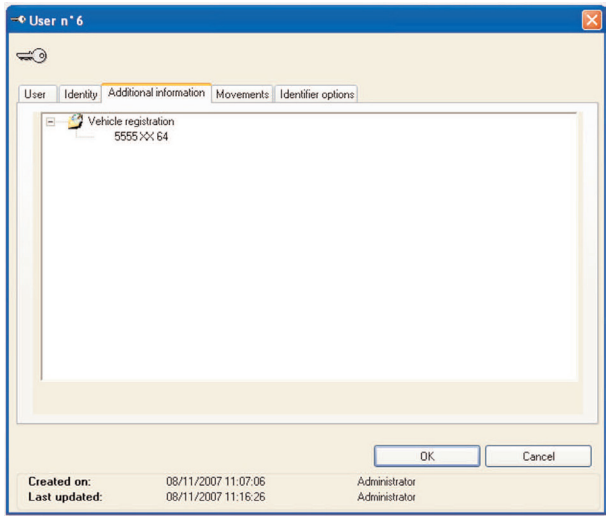

- Identification: User’s name and first name.
- Microphone icon: Record a personalised audio message for this user.
  Example: When a badge is accepted, you’ll hear “Badge accepted”, followed by a personalised audio message.
- Webcam icon: Enables a photo of the user to be taken, which is then automatically positioned in the grey frame on the right.
- Colours icon: Attaches an existing image to the badge.
- Printer icon: Prints out a sheet showing all the badge information.

**Note:**

If the installation has several biometric readers, the fingerprint numbers of a user must be the same on all the readers.

# II - MANAGING THE SITE - Creating an installation user

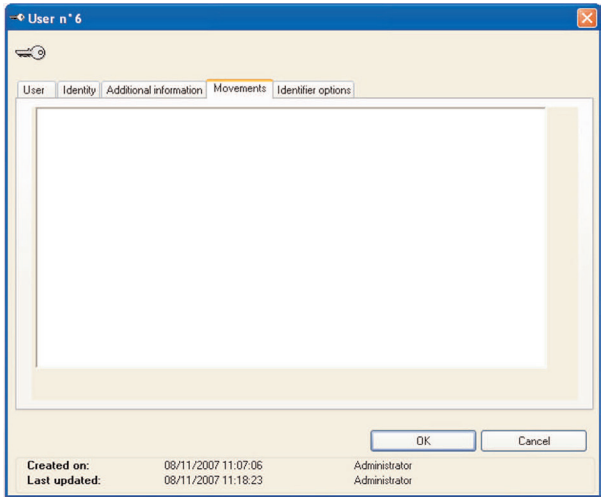
**- Additional information tab:**




- This tab is used to enter additional information relating to the user (e.g. vehicle registration number).

  The procedure is described in detail in the “Options” section, “Badge personalisation”.

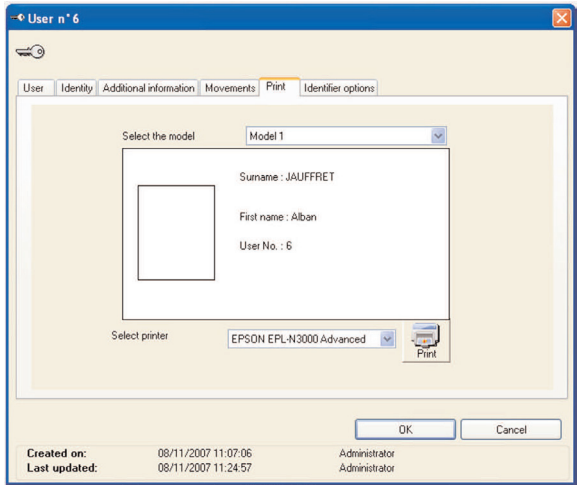
**- Movements tab:**




- This window displays the entries and exits for this badge over the last 30 days.

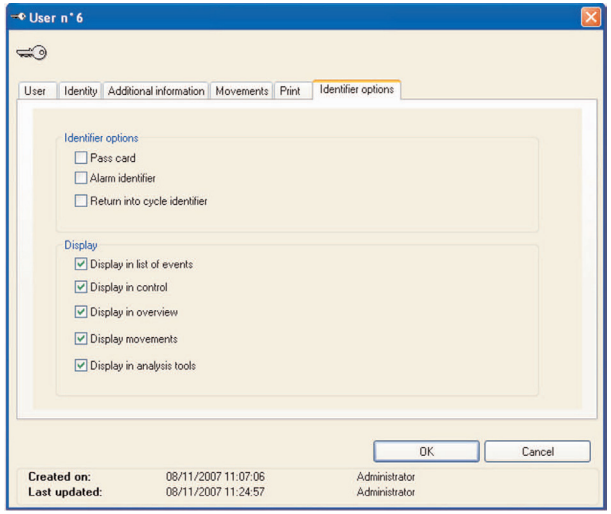
# II - MANAGING THE SITE - Creating an installation user

- **Print tab:**




- Select the badge model (see “Extensions” tab / Creating a printable badge format).
- Print the badge for this user.

- **Badge options tab:**




- This window is used to change the badge options and the various displays of events related to this badge, in the appropriate sections.

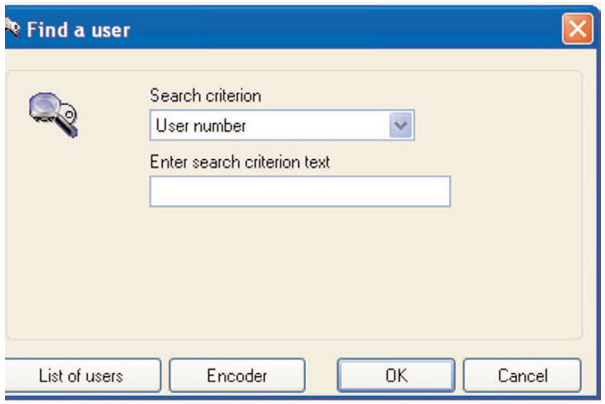
- Return into cycle badge: Useful when the anti pass-back function is active.

When this badge is presented to a reader, all badges relating to the controller will be in neutral status for the next presentation to a reader (the badges will be accepted on both entry and exit).
Subsequently, they will again be subject to the anti- passback mechanism.

## Searches and analysis tools

The “Operation” tab contains two search tools:

- The first is accessed by clicking on the “Find a user” icon.

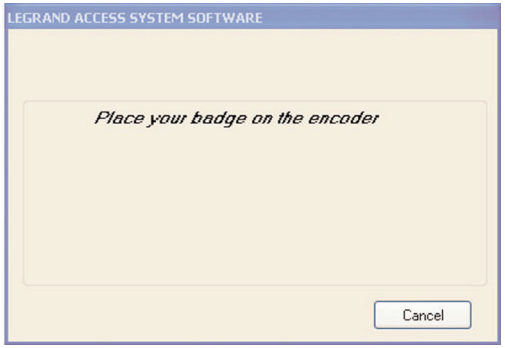



• The “Find a user” function accesses the records of one or more users, according to a search criterion.
To find a user using another criterion (e.g. name or the contents of a personalised field), enter the search text as fully as possible so as to minimise the possible number of responses.
The search finds those users for which the search criterion contains the text entered.
If the criterion corresponds to several users, a list is displayed.
Select one or more lines by keeping the “Ctrl” key pressed down while clicking on “Open”.
For more complex searches, use the analysis tool.

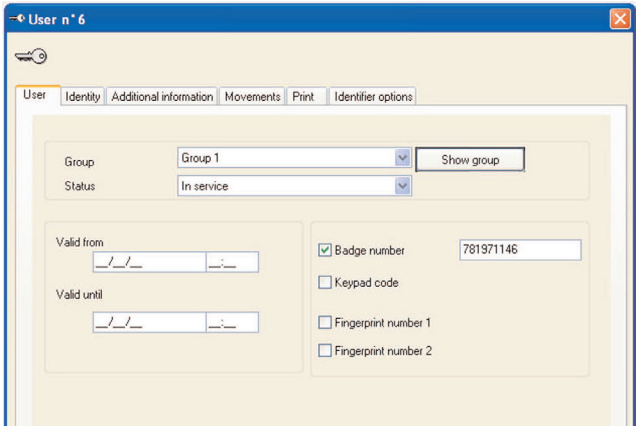
• **Using the encoder 767 05:**

To validate the use of encoder 767 05: In the “Technical – Site setup” tab, right click on “site configuration” and select “add an encoder” (the encoder must be connected to the PC).

To obtain information relating to a badge, click on “Encoder” (the encoder must be connected to the PC).




Place the badge on the encoder and the corresponding user record will be displayed.

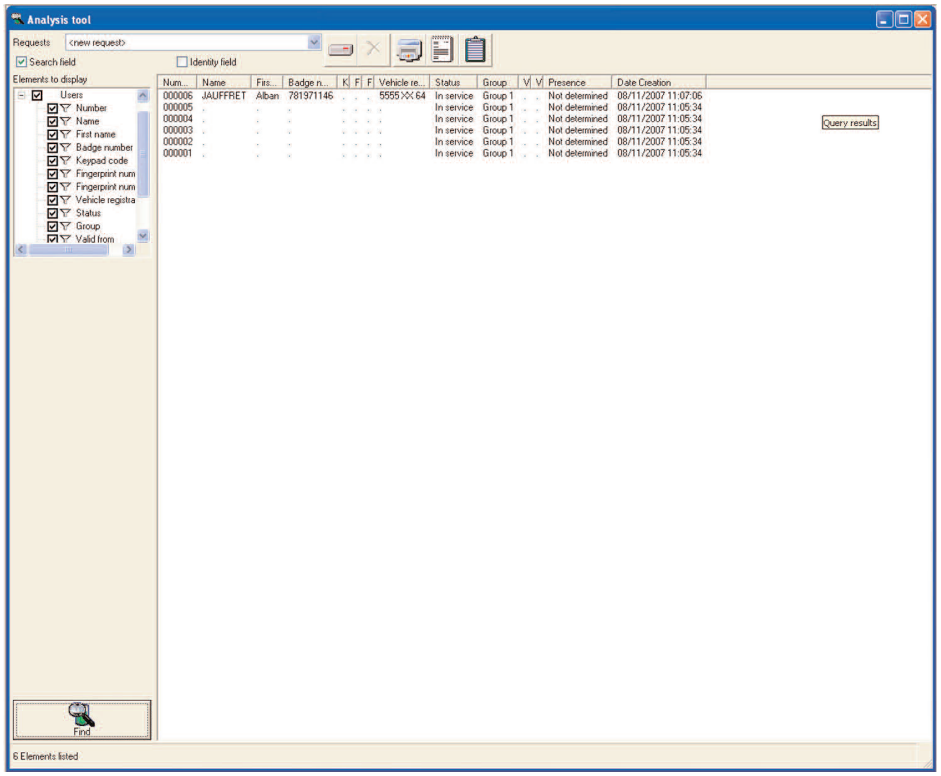



The badge can be placed on the encoder at any time, and the corresponding user record will be displayed.

# III - USING THE APPLICATION - Searches and analysis tools

• **The second tool is accessed by clicking on the “Analysis tool” icon.**

The analysis tool is used to extract information relating to users and/or events collected, and to sort, store, print and export this information.



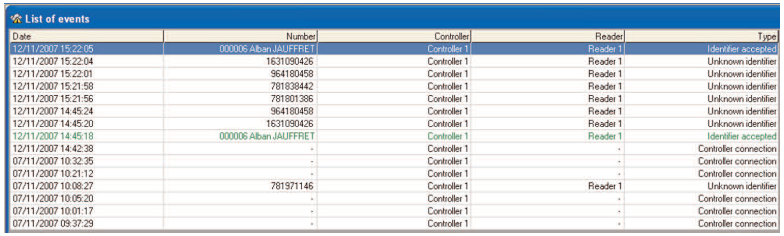

The icons on the right of the tool bar are used to:

- Save search criteria in the form of a query, so that the same search can be run in the future.
- Print the results of the query.
- Export the result of the query to a text file.
- Export the result of the query to the clipboard (a right click in the table performs the same operation).

Selecting “Identity zone” accesses the user record when you click on a line.

The “Badges” option, within the “elements to be displayed” section, contains the “presence” option.
This function lists all the persons who have entered through a reader configured in “Entry” and who are therefore on the site.

# List of events



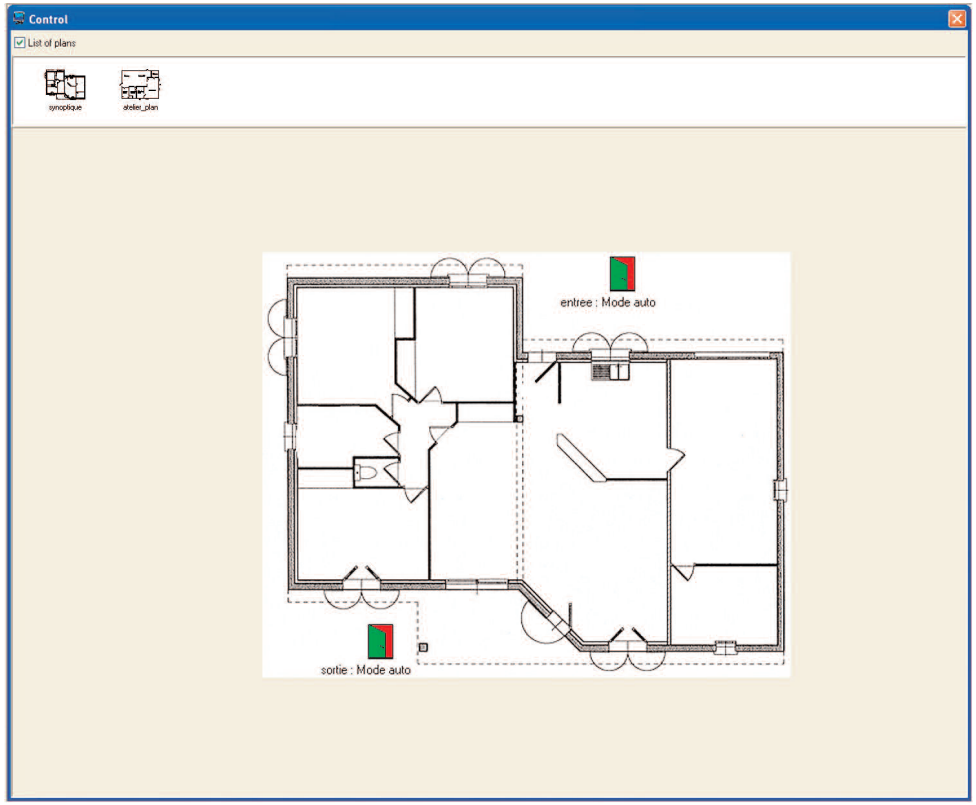

The list of events enables “real-time” monitoring of the events being processed. Depending on the type of event, the line is displayed in a specific colour, and a configurable audio message can be generated.
The “User record” button accesses the user record corresponding to the selected line.

Events to be displayed can be selected in the “Access control” tab.

## Control and overview

• **Control:**

This window is used to import black and white or colour plans (.bmp or .jpeg) of the site and incorporate the readers, automatic systems and counters, thus enabling events to be displayed in real time on the plan, and opening actions to be remotely controlled directly from the plan.



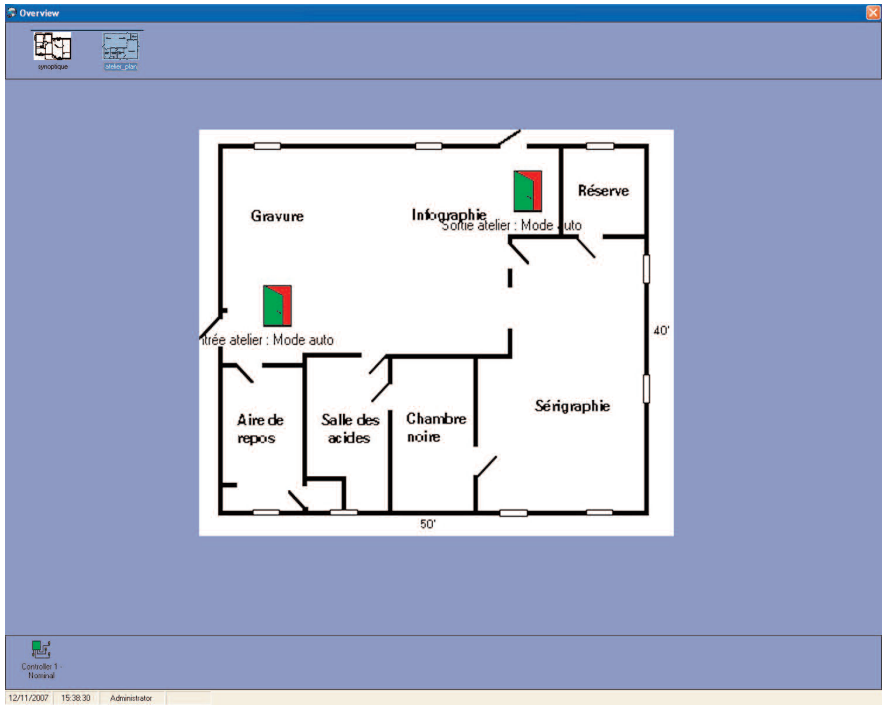

- To import a plan, right-click in the blank window and select the file containing the desired plan.
- To add a reader, an automatic system, a camera or a reader on the plan, right-click on the plan at the appropriate position and select “add a reader”.
- To move the position of the reader on the plan, press “Ctrl” and drag and drop the reader. When the reader is properly positioned, clicking on the reader enables the corresponding door to be opened or kept closed.

Clicking on the camera icon displays a camera display window. The value of a counter can also be changed by clicking on the counter.

# III - USING THE APPLICATION - Control and overview

- **Overview:**

Displays the real-time status of doors and controllers on the various installation plans.




- Clicking on a reader controls the corresponding door, which can be opened or maintained closed.
- Controller statuses are shown at the bottom of the screen.

Various display, scale or depth of view options are available by right- or left-clicking in the main window.

## Opening an installation:

Enables another installation to be opened.

## Closing the session :

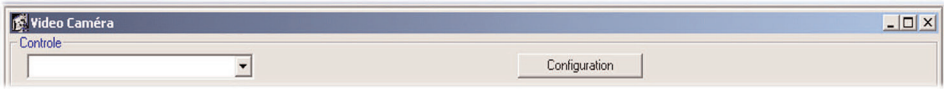
Closes the current session. A session can then be opened using a different user profile.

## IP camera :

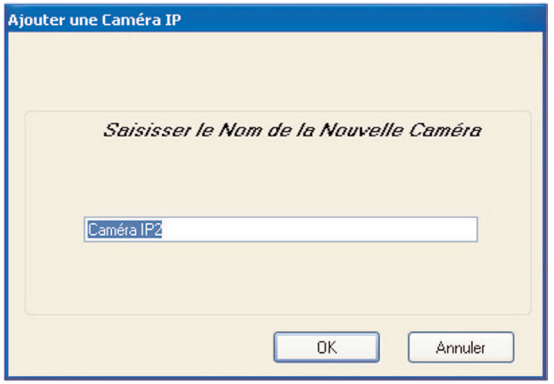
Several network IP cameras can be used and incorporated in the control function (for example, to clear any doubt in cases of break-in). The cameras first have to be identified on the network, and then positioned on the plans.

**Creating a camera:**

- Click on “Configuration”, then add a camera.



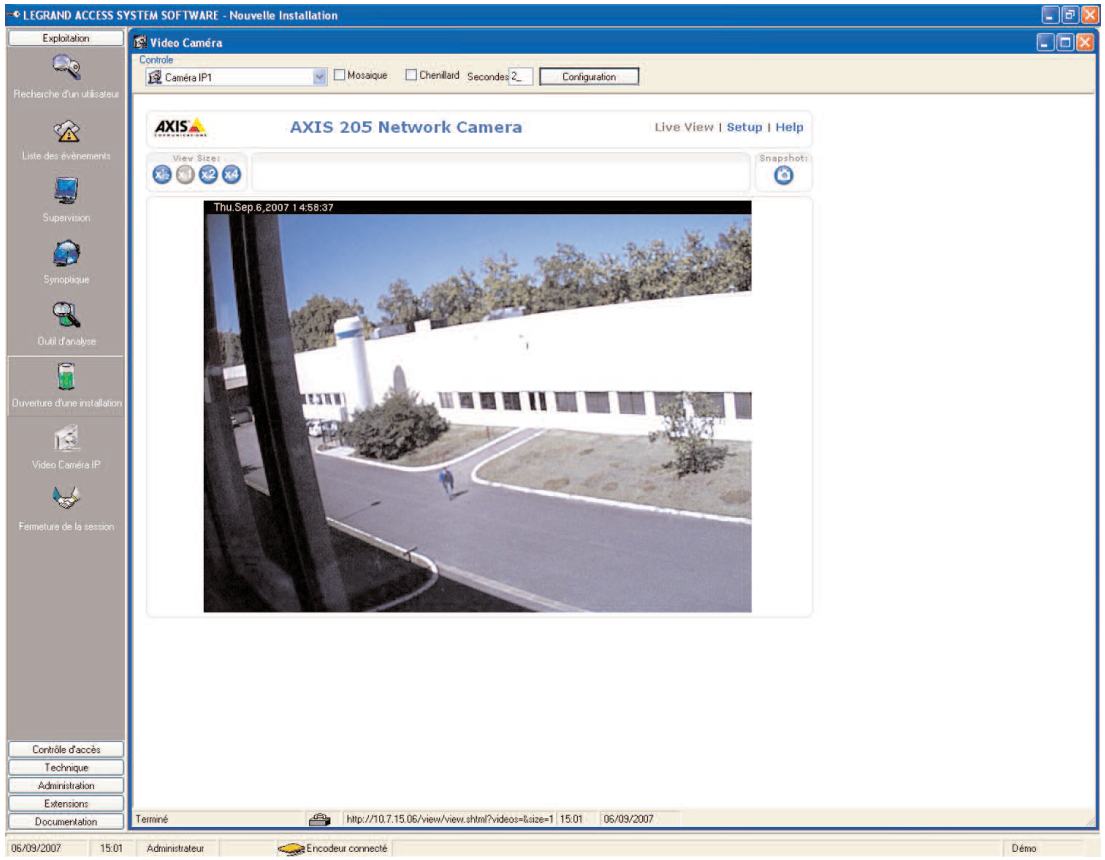

- Enter the camera IP address and the desired name.



# III - USING THE APPLICATION - IP camera

- Repeat the above operation if you wish to add more cameras.

The display can be in mosaic format (select mosaic), image scrolling (select scrolling and interval between images), or in the form of a fixed image.



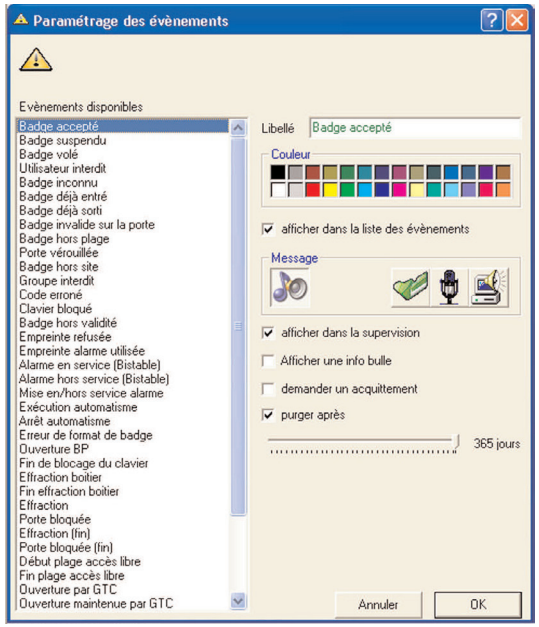

To add a camera in the control function: from the “Control” tab, right-click on the plan at the position where you wish to place the camera icon. This icon will enable you to open a control window at any time.

# IV - OPTIONS - “Access control” tab

## “Access control” tab

### Configuring the events

Click on “Configure events”.
A colour can be assigned to each type of event, to facilitate identification in the event display and on the control screen.
A specific audio message can also be assigned to each type of event, and will thus be generated when the event occurs.
The system can automatically clear events earlier than a predefined conservation time (365 days by default).
The event names can also be changed for their display in the events list.




- Active ou désactive le message sonore.
- The icons in the “Message” zone are, from left to right:

- Audio message active or deactivated.
- Assign a specific audio file to an event.
- Record a personalised message with a microphone connected to the PC.
- Play back the message assigned to the selected event.

Selection squares:

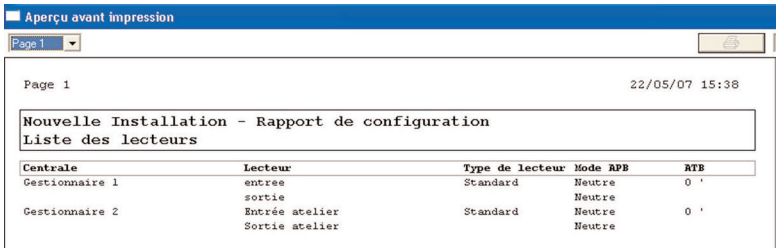
“Display technical tip”: displays information on the screen when the event occurs.
“Must be cleared”: when an event occurs, instructions are displayed on the screen and have to be cleared by the user before they are deleted.

# IV - OPTIONS - “Access control” tab

## “Technical” tab

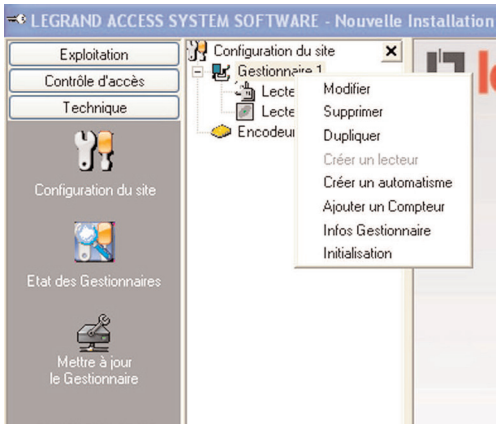
This function lists:
- The installation controllers and readers (page 1).
- List of groups (page 2).
- Group entry/exit time periods on the various readers (subsequent pages).

To print, you must select a printer (the application uses the printers installed on the PC).



# “Technical” tab

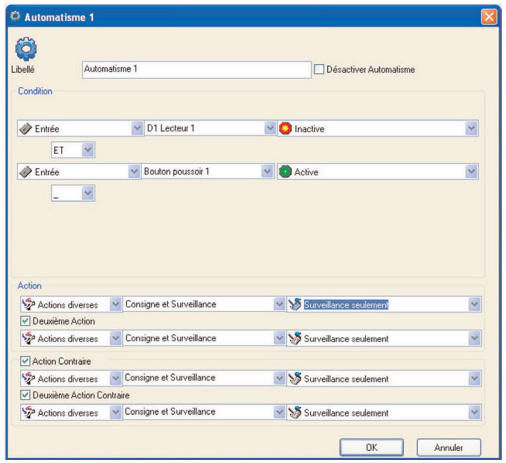
## Configuring the site




- The “Duplicate” function is used to create another controller with the same characteristics as an existing one.
- The “Controller info.” function gives the software release used by the controller.
- The “Add a counter” function: The controller has internal counters that can be used to create an automatic system. There are 32 counters which enable counting up to a maximum value of 65535. The counters can be displayed and modified on the control screen, and can be used and/or modified in automatic systems. In this case, they are incremented each time a defined event occurs.

- Initialise: Restores the factory configuration for the controller.

Creating an automatic system

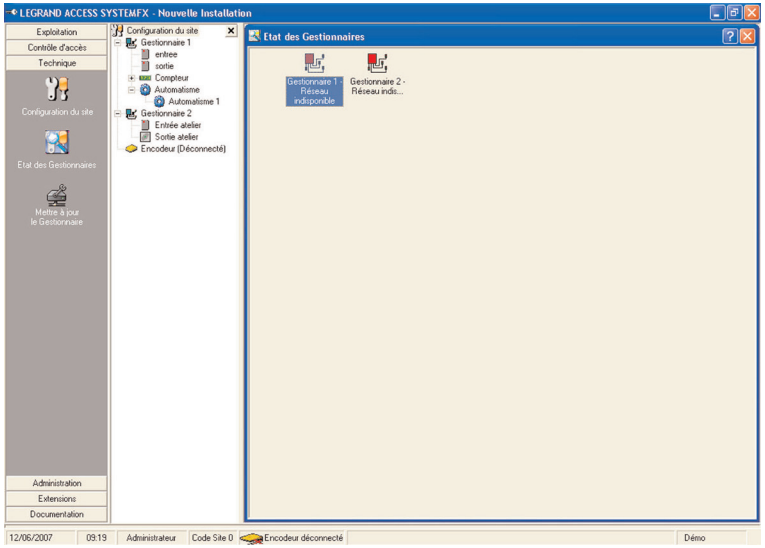



The controller can run automatic control systems as a function of physical inputs, access control events and time periods.

- The “Condition” parameter: Up to 4 conditions can be activated.
- The “Action” parameter: 2 actions are possible (a counter can be incremented or decremented).
- The “Undo action” parameter: 2 “undo actions” are possible.

# IV - OPTIONS - “Technical” tab

Controller statuses




The main control station has a controller status display function, which lists the controllers installed along with their statuses.
Possible statuses are:

- Nominal: the controller is operating normally.
- Initialisation in progress: the application has requested a reset of the controller contents. This phase is run when a controller is connected but not referenced in the database, when a controller is installed, when a controller is replaced or a controller address is changed.
- Configuration: the system collects the new events available in the controller or when the time is adjusted (clock change).
- Collect events: the system collects new events available in the controller.
- Update: the system updates the controller program (see below).

Updating controllers

The “Update controller” function is used by the Legrand Technical department to update the controller. In this case, you will be given the new password.

Specific messages

Certain messages are displayed to indicate a configuration or installation error:
- Incompatible type: the controller connected is not a Legrand controller.
- Network unavailable: the PC cannot communicate with the controller.
- Disconnected: the controller is not communicating with the PC.

# IV - OPTIONS - “Administration” tab

## “Administration” tab

### Log

The log lists all the creation, change or delete operations performed on the various elements of the installation.
The log is updated in real time. Thus any change entered by another user through a subscriber terminal is immediately displayed on all the other terminals connected to the installation.

### Personalising users

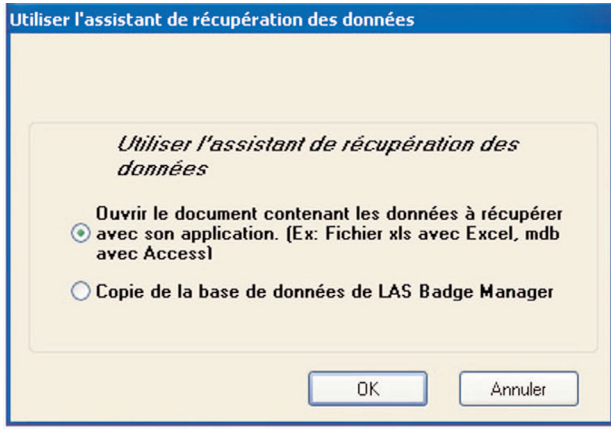
This function is used to add, change or delete sections that will be completed in the “Supplementary information” tab, when users are created:

- This information can be entered for each user in the installation. This will enable simple searches to be run using these criteria. This data can also be used in the analysis tool and can be displayed in the list of users.
- Personalised data can also be entered directly in the quick data recovery sheet but the personalisation fields must already have been created in order to assign them.

# IV - OPTIONS - “Administration” tab

## Quick data recovery

If the information relating to badge holders already exists in Word,, Excel,, Access, or text format, it can be imported simply by copying (CTRL C or Copy) the files, and then pasting them onto the LAS Software quick data recovery sheet.



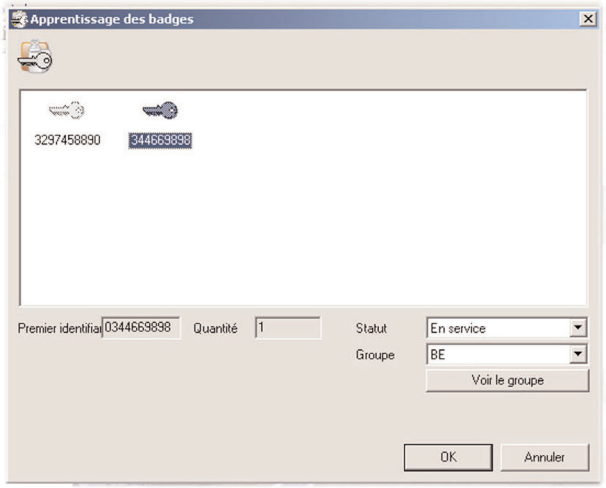

- Enables data to be recovered from another document: name, first name, additional information.
- Enables the recovery of data created using LAS Badge Manager.
  Specify the file Base.mdb contained in the LAS Badge Manager installation directory (by default: C:\Program Files\LAS\LAS Badge Manager\.

To recover data from another document, open the document containing the data (e.g. an EXCEL file), and then copy the data.
Next assign the corresponding LAS Software field to each column.

# IV - OPTIONS - “Extension” tab

## “Extension” tab

### Learning




- When this window is open, any unlearned badge presented in front of a badge reader in the installation, or in front of the encoder, will be displayed in the window.
  You must then click on the badge to define its status and group.
  When you click on “OK”, a new user is created. You must then go into the “Access control” tab, and then select “Users” to obtain details of the identity and the attached readers.

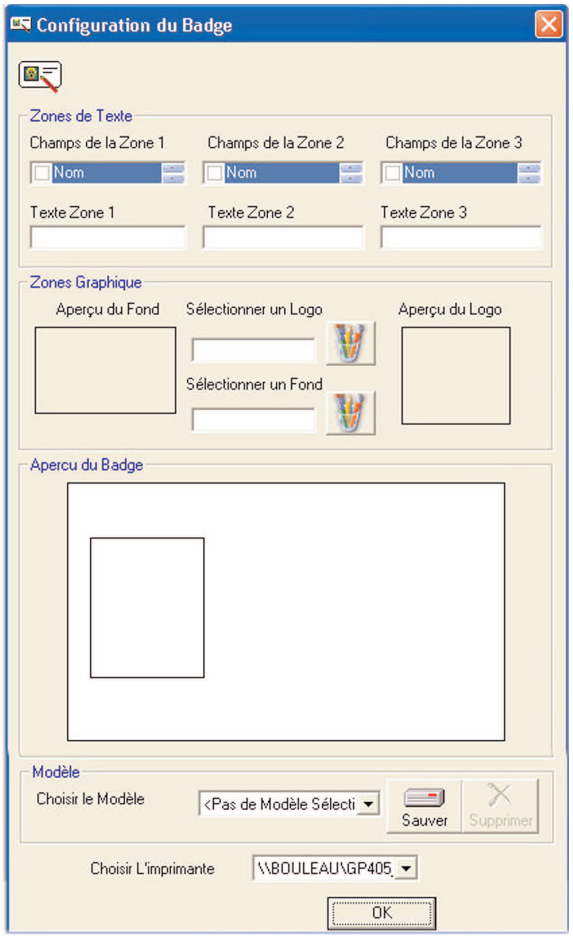
  Badges already declared are displayed dimmed in the list.

**Note**

To use the encoder, it must have been added previously (see “III OPERATION – Searches and analysis tools”

# IV - OPTIONS - “Extension” tab

## Creating a printable badge format




Text zone:

- Fields in zone: Select a field, which will be automatically completed using the data related to each user.
- Text in zone: Complete the squares if you want to print the same text on all the badges to be printed.

Graphic zone: You can select an “image” file for the background and a logo.

Badge preview: You can change the background colour, text colour and character font by clicking on the text. You can also move it by keeping “Ctrl” pressed down and dragging and dropping the text.
You can resize the photo or logo by right-clicking on it and moving the outline.

When the badge model is as required, save it by clicking on “Save”.
You can delete a badge model by clicking on “Delete”.
The selected printer will be prompted by default in the badge printing tab.

# IV - OPTIONS - “Extension” tab

## Site code

You can define a site code for each controller. The site code is used for badges of brand names other than Legrand.

## Configuring automatic backup

You can configure an automatic backup. In this case, the user is reminded that an installation backup must be performed at scheduled intervals: daily, weekly or monthly.

Thus all data contained in the controller is backed up.
In the event of an incident, this data can be restored whenever an installation is opened. Right-click on the installation and select “Restore”

**LEGRAND FRANCE**
SNC with registered capital of 6,200,000 euros
Limoges company register B 389 290 586 (92 B 412)
A.P.E. code 516 J, VAT number FR 15 389 290 586

**Head office**
128 Av. du Maréchal-de-Lattre-de-Tassigny
87045 Limoges Cedex - France
tel: 00 33 5 55 06 87 87
telex: 580048 F
fax: 00 33 5 55 06 88 88

LE00477AB_GB