



WatchNET Access Integrated Security Management Software
Software Manual V1.2.21.0



Revision History	7
Chapter 1 Introduction	7
1.1 WATCHNET ACCESS - Overview.....	7
1.2 Software Overview	7
1.3 Features	7
1.4 Web & FTP Sites.....	7
1.5 Getting Started	8
1.6 Computer Requirements	8
Chapter 2 Main Operating Window	9
2.1 Logon	9
2.2 Menu Bar	10
2.3 Tool Bar	10
Chapter 3 Management Menu	11
3.1 Clients Manager.....	11
3.2 User Manager	11
3.3 Change Password.....	16
3.4 Departments.....	17
3.5 Group Management	21
3.6 Site Management	21
3.7 Change Database.....	21
3.8 Glossary	23
3.9 System Management	24
3.10 Holiday Settings.....	30
3.11 Daylight Savings Time	30
3.12 Import Directory	31
3.13 Connect WatchNET Active Directory Database	31
Chapter 4 Setup Menu	33
4.1 Hardware	33
4.1.1 Controller Configuration	36
4.1.2 TCP/IP Setting.....	42
4.1.3 Search Controller	42
4.1.4 Door Configuration	42
4.1.5 T & A.....	54
4.1.6 Standalone Controller Configuration	55
4.1.7 Controller Components.....	55
4.1.8 Pre-set Components Status.....	56

4.1.9 Disable/Enable Doors.....	57
4.1.10 Prosys Intrusion.....	58
4.1.11 Prosys Plus Intrusion	58
4.1.12 DSC Intrusion	58
4.1.13 PIMA Intrusion	58
4.1.14 DVR Configuration.....	59
4.1.15 Search Configuration.....	62
4.1.16 DVR Channel	62
4.1.17 Channel to Doors/Zones Mapping	63
4.1.18 Fingerprint Reader	63
4.1.19 Face Recognition	64
4.1.20 LED Screen	64
4.2 Cards.....	65
4.2.1 Access Security Groups	65
4.2.2 Personnel List	66
4.2.3 Visitor List.....	81
4.2.4 Access Level	84
4.2.5 Pre-set Personnel Access Level	84
4.2.6 Department area limit	86
4.2.7 Emergency Card	86
4.2.8 Bank Card	87
4.3 Event Alerts.....	87
4.3.1 Access Event Alerts	87
4.3.2 Prosys Intrusion Event Alerts	92
4.3.3 Prosys Plus Intrusion Event Alerts	92
4.3.4 DSC Intrusion Event Alerts	93
4.3.5 PIMA Intrusion Event Alerts	93
4.3.6 CCTV Intrusion Event Alerts	94
4.4 Map.....	94
4.4.1 Multi-site Setup.....	94
4.4.2 Map Designer	99
4.4.3 Delete map.....	99
4.4.4 Icon Library	99
4.5 Flow Control.....	100
4.5.1 Access Flow Control	100
4.6 UDP Broadcast	104

4.7 Wiegand Format	105
4.8 Special Date	107
4.9 Communication Configuration.....	109
4.10 Area Name	120
4.11 Saved Events	121
4.12 Car Parking.....	124
Chapter 5 Monitor	125
5.1 Boot Platform	127
5.2 Access Tree	127
5.3 Intrusion Tree.....	127
5.4 CCTV Tree.....	127
5.5 Map Tree.....	127
5.6 Map Page	127
5.7 Events	128
5.8 Intrusion Virt Keypad	128
5.9 Photo Viewer	129
5.10 Camera 1.....	133
5.11 Camera 2.....	133
5.12 Camera Playback 1.....	134
5.13 Camera Playback 2.....	134
5.14 Park Counter	134
5.15 Area Viewer	136
5.16 Camera or Grid (Area Viewer)	136
5.17 Card Validity Display	136
5.18 Camera View.....	136
5.19 Clients	137
Chapter 6 Report	137
6.1 All Cards Events.....	137
6.2 Quick Query Cards Events.....	140
6.3 Cards Events Filter	141
6.4 All Hardware Events.....	142
6.5 Face Recognition Records	144
6.6 Bank Card.....	143
6.7 Area Report.....	144
6.8 Personnel Area Report.....	144
6.9 Area Changed Report.....	144

6.10 Personnel In/Out Reports	145
6.11 Access Level Report	146
6.12 Access Security Group Report.....	147
6.13 Time Attendance.....	147
6.14 Times Canteen Report	148
6.15 All Intrusion events	149
6.16 All Intrusion System Status	149
6.17 All CCTV Event.....	149
6.18 All Alert Events.....	149
6.19 All Events Filter	150
6.20 System Log.....	150
Chapter 7 Maintenance.....	151
7.1 Delete Records.....	152
7.2 Backup Database	152
7.3 Auto Backup Database.....	155
7.4 Restore Database.....	155
7.5 Compact/Repair Database.....	155
7.6 Auto Compact/Repair Database	156
Chapter 8 Tools.....	157
8.1 External Tools.....	156
8.2 Imports from Excel.....	157
8.3 Export Events Automatically	161
8.4 Capture Tool.....	166
8.5 Card Printer.....	167
8.6 Run as Task Scheduler once Windows Start	167
Chapter 9 Window	168
9.1 Save Desktop	168
9.2 Delete Desktop	168
9.3 Screen Style	168
Chapter 10 Help.....	169
10.1 Help.....	169
10.2 Home Page.....	169
10.3 On-Line Update.....	169
10.4 License Information	169
10.5 Upgrade License	169
10.6 About	170

Revision History

Revision	Date	Author	Description of Changes
1.0	12/05/2017	Peter Punzalan	Manual Created for No Card List version, changes on Access Level configuration
1.1	05/28/2018	Peter Punzalan	Updated software version and added features.
1.2	9/20/2018	Peter Punzalan	Updated Software version and fix some bugs
1.3	04/13/2020	Peter Punzalan	Updated Software and added some new feature
1.4	09/15/2020	Peter Punzalan	Updated Software and added features
1.5	04/22/2022	Peter Punzalan	Updated Software and SQL version
1.6	10/27/2022	Peter Punzalan	Added Aperio Lock Integration
2.1	12/13/2023	Peter Punzalan	Added new OSDP Controllers

Chapter 1 Introduction

1.1 WATCHNET ACCESS Overview

WATCHNET ACCESS is a Global manufacturer and supplier of Integrated Security Solutions such as Access Control, CCTV, and Intrusion with basic Building Management. WATCHNET ACCESS meets the tough end-user demands for safety, security and user friendliness. WatchNET has a strong global presence providing its systems to more than 40 countries. For more information please visit our web site at www.watchnetaccess.com

1.2 Software Overview

The WatchNET Access Security Management Software comprises of a suite that covers the complete range required by Access Control Professionals. The software is modular and ranges from the standard single user package to multi-user systems. Additional modules are available which include CCTV and Intrusion.

1.3 Features

The WatchNET Access Security Management Software is available in multiple languages and also has the option of installing *MS Access or SQL Server*. During the installation process the user can select the language as well as the database.

Note: Please Install MS SQL software supplied with the software on the CD first.

1.4 Web & FTP Sites

Although software is supplied on a CD at the time of purchase periodic enhancements and bug fixes renders the software out of date within a short period of time. To make it easier for the installer up to date software is located on

the *WATCHNET ACCESS FTP* site which is accessible through our web site.

1.5 Getting Started

- Connect the all-necessary cables and power up the controller (see Hardware Manual).
- Setup the controller and any converter addresses (see Hardware Manual).
- Install and Configure MS SQL Server Database
- Load the WATCHNET ACCESS INTEGRATED SECURITY SYSTEMS v1.1 software and then setup the following:
- Setup the communication port
- Search for the Panels
- Setup the parameters of each door including Time Table
- Setup Departments and Sub Departments
- Add a Wiegand Format if not already added
- Add Personnel and configure their cards and assign Access Level.
- Flash the Personnel card to a reader of a door which he has the Access Level to enter. The Lock relay should operate and a *Valid Card* event will appear in the *Events Monitor*. If *Invalid Card* or *Invalid Time/Door* event appears please check the Access Level.

1.6 Computer Requirements

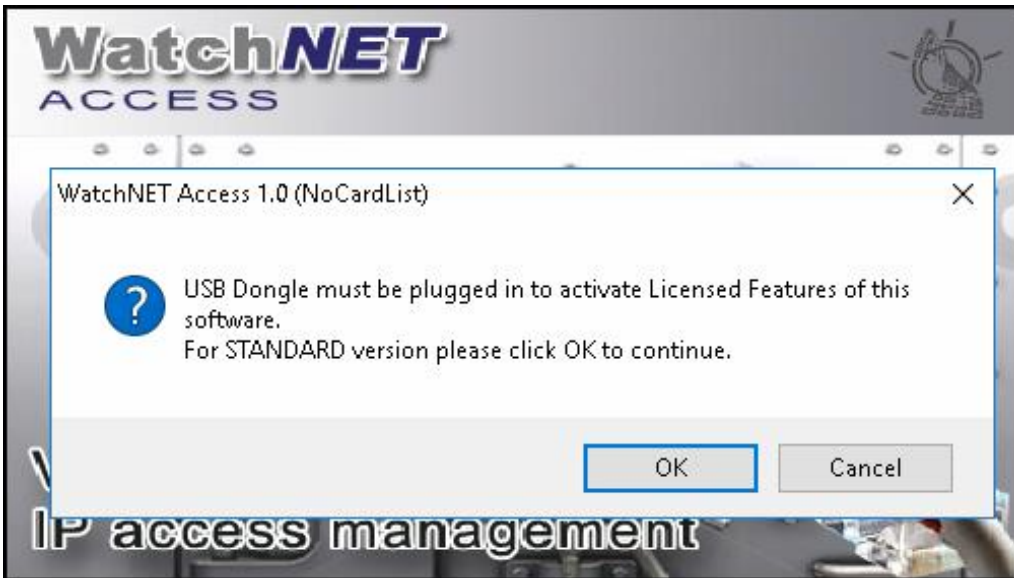
The *WatchNET Access Security Management Software* is designed to run on a Microsoft Windows platform. While the software is designed to run on Windows 7 and Windows 8 it will also run on Windows XP although the performance may be reduced. The following is the minimum computer requirement:

- Minimum 3rd Generation Intel® Core™ i5-3340s processor (6M Cache, up to 3.3 GHz) Equivalent or higher
- Free 500 GB Hard Disk space
- RAM: 8GB RAM
- VGA: 1024 x 768 pixels
- DVR ROM Drive
- Video Card - Intel® HD Integrated Graphics or Equivalent
- Free Serial and USB Port (For license dongle or RS485 connection if needed)
- Windows Server 2008, 2012, 2016, 2019 , Windows 7, Windows 10 or Windows 11

Chapter 2 Main Operating Window

2.1 Logon

The message box explains that if using more than 8 doors you require access license to run the software, for standard version just click *OK*

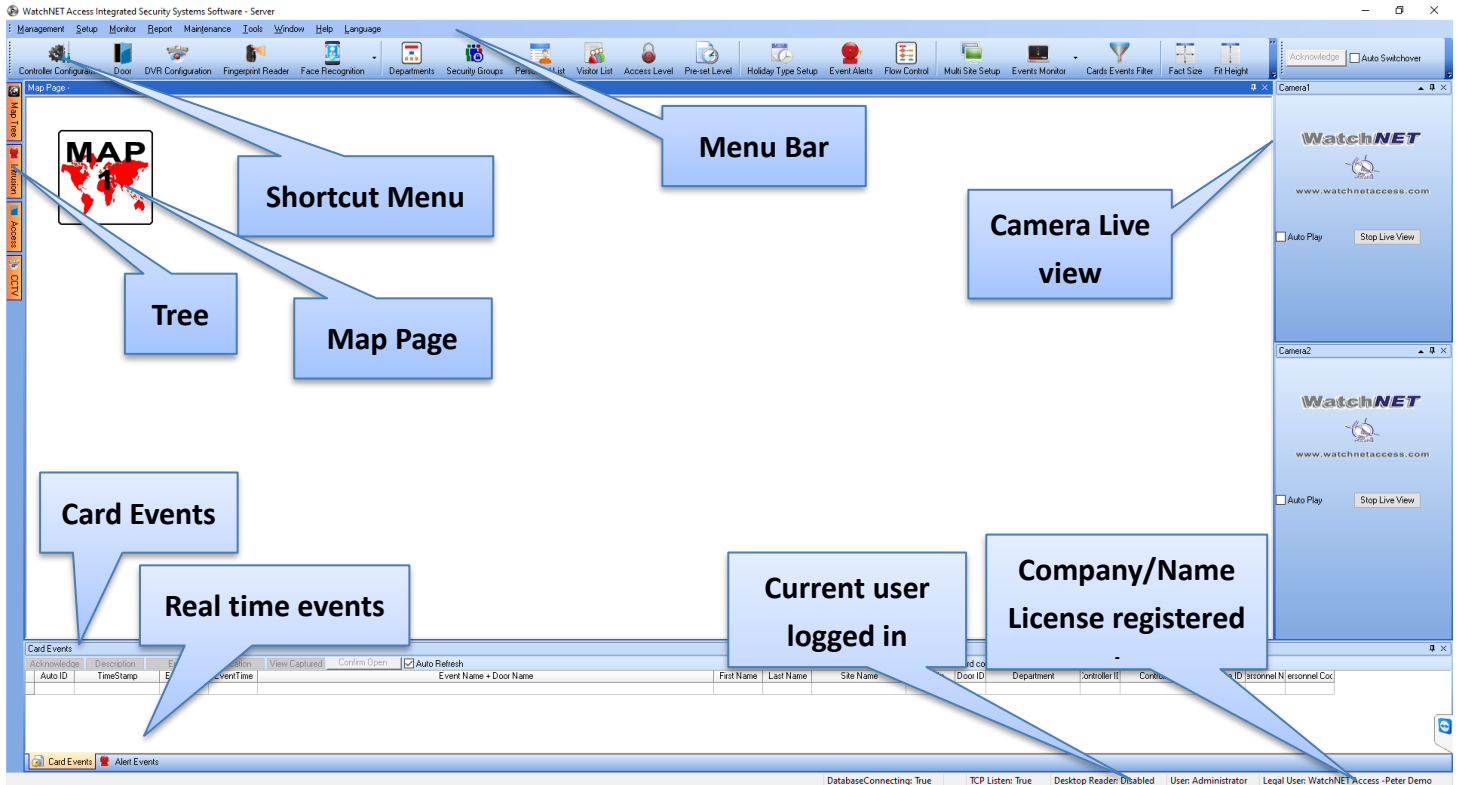


Logon with the default **Administrator** user or click the arrow to the right of the User name to logon with a different user. The default the password is **watchnet**.



Note that any additional users must be configured first, see in *Chapter 6*.

Once logged in, the main window will display. This window has a *Menu Bar*, *Shortcut Menu*; it shows the Authorized User, i.e. the company that the software is licensed to and the Current User.

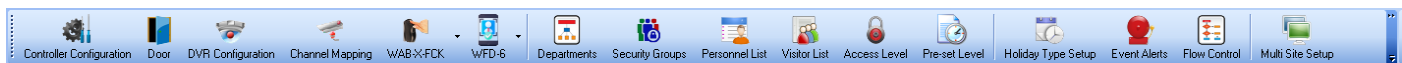


2.2 Menu Bar

The Menu Bar allows access to the entire program via a series of Sub-Menus. The Main Menu consists of the following:

Management Setup Monitor Report Maintenance Tools Window Help Language

2.3 Tool Bar

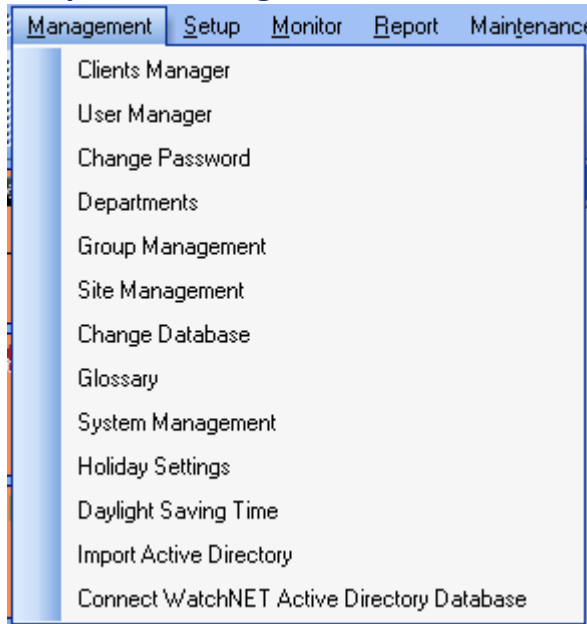


The Tool Bar or Icon Bar contains the most common icons they are as follows:

- ✓ Controller Configuration
- ✓ Door Configuration
- ✓ DVR Configuration
- ✓ Channel Mapping

- ✓ WAB-X-FCK (Fingerprint Reader)
- ✓ WFD (Face Recognition)
- ✓ Departments
- ✓ Security Groups
- ✓ Personnel List
- ✓ Visitor List
- ✓ Access Level
- ✓ Pre-set Level
- ✓ Holiday Type Setup
- ✓ Event Alerts
- ✓ Flow Control
- ✓ Multi-Site Setup

Chapter 3 Management Menu



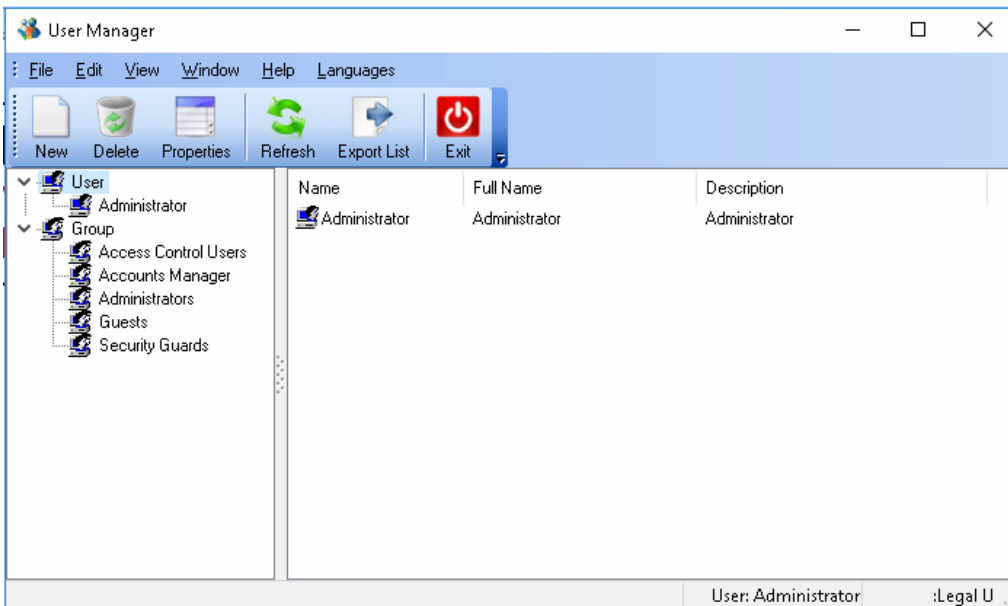
3.1 Clients Manager

Clients manager menu allows the admin user to add or delete a client access (Client Software).

3.2 User Manager

The WatchNET Access Security Management Software allows multiple users (software operators) simultaneously and can give each user a different level of access. Only the System Manager (*Administrator*) can add or delete the users and modify/add/delete user's permissions. It is important that the installer set up individual users according to their rights and privileges. The password length can be up to 20 digits and includes any keyboard characters.

Note: that initially there is only a single user called Administrator with an Administrator Permission Settings.



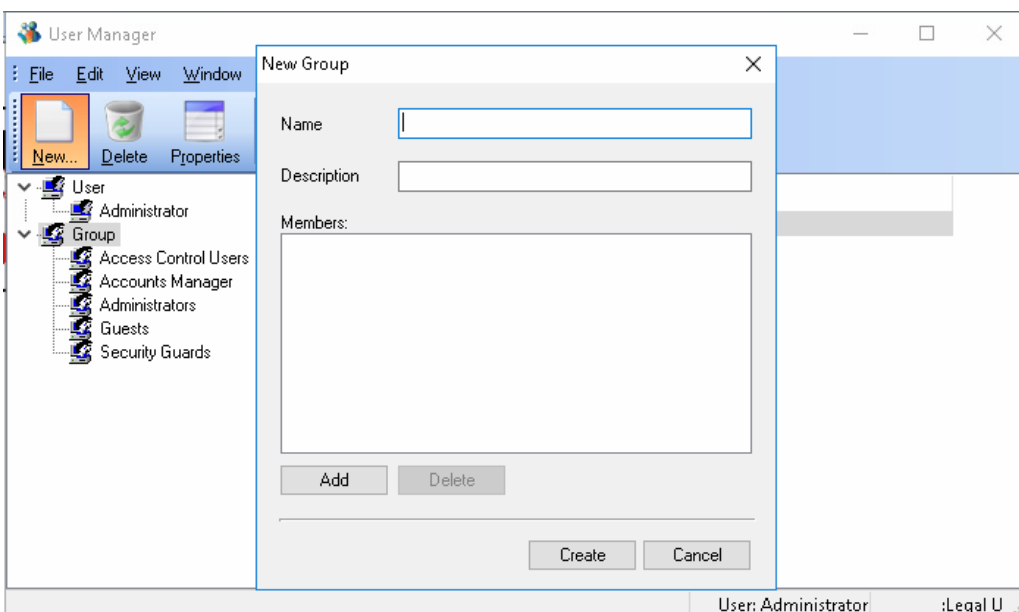
Before creating a User we will need to create a Group that the user belongs to or use one of the 5 default groups: *Administrators, Access Control Users, Accounts Managers, Guardians, and Guests.*

Note: Every User needs to belong to a Group.

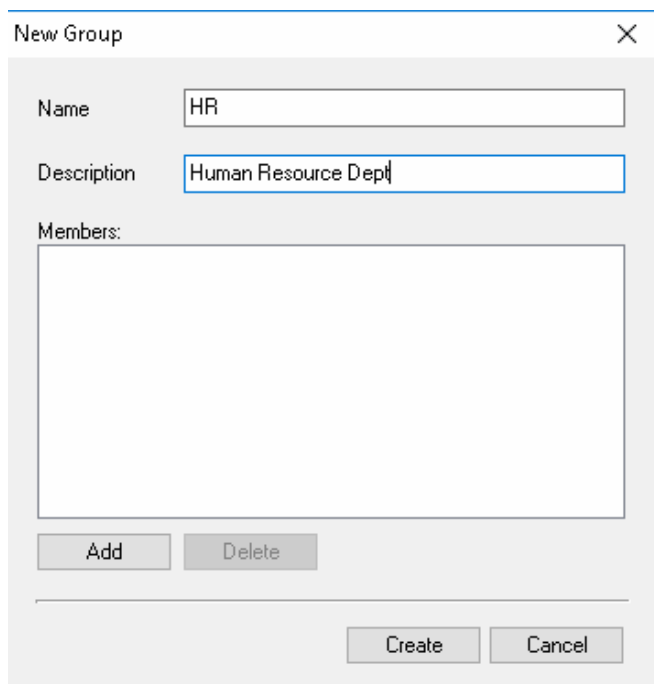
The Group grants the privileges to the kind of operations, functions, and the configurations the User will be able to perform in the system. When defining the User the system will specify to which panels/doors and departments/sub departments the privileges inherited from the Group will apply.

Adding a Group

Click or select *Group* and click *New* icon on top to create new group.



Enter details for the new Group and click on the *Create* button.



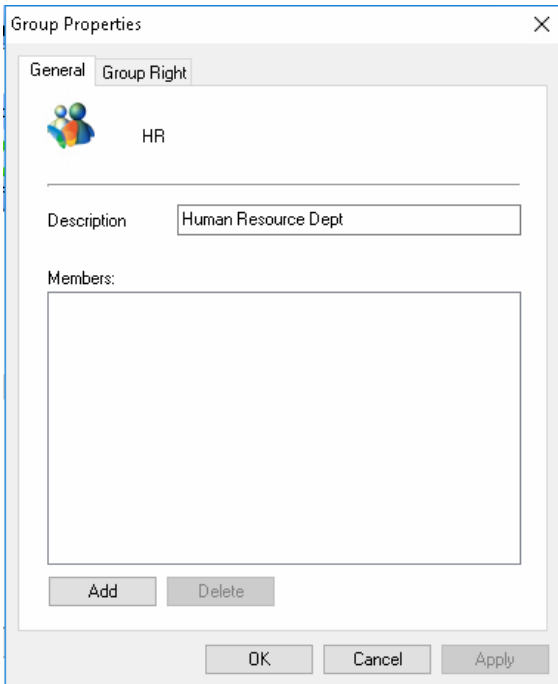
The screenshot shows a 'New Group' dialog box with the following fields and buttons:

- Name:** HR
- Description:** Human Resource Dept
- Members:** An empty list box with 'Add' and 'Delete' buttons below it.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom right.

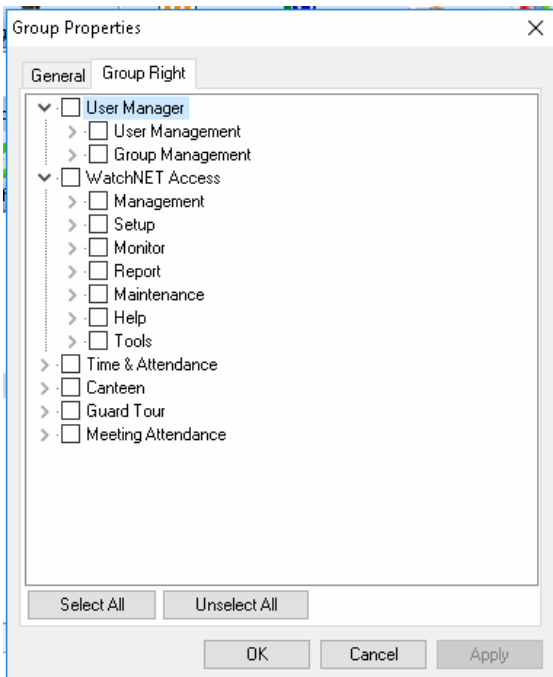
Editing a Group

When group is created, select or highlight the group name and click *Properties* icon on top.

- **General** – you can add user to this group

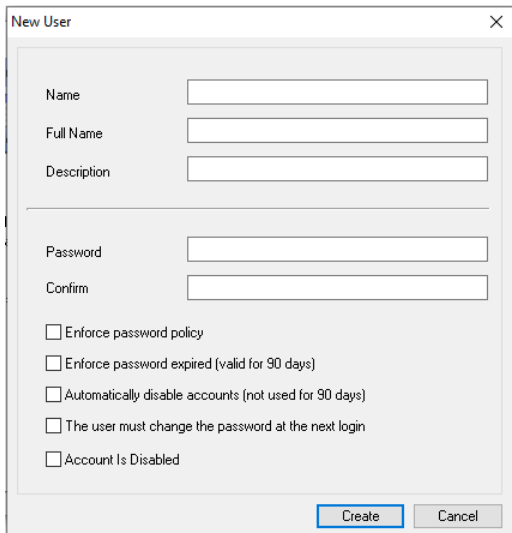


- **Group Right** – this tab allows you to modify the access rights of the group on the software, check and select which is suitable for the group



Adding a User

To create a user, select or highlight *User* on the tree and click *New* icon, input all the information needed and click create



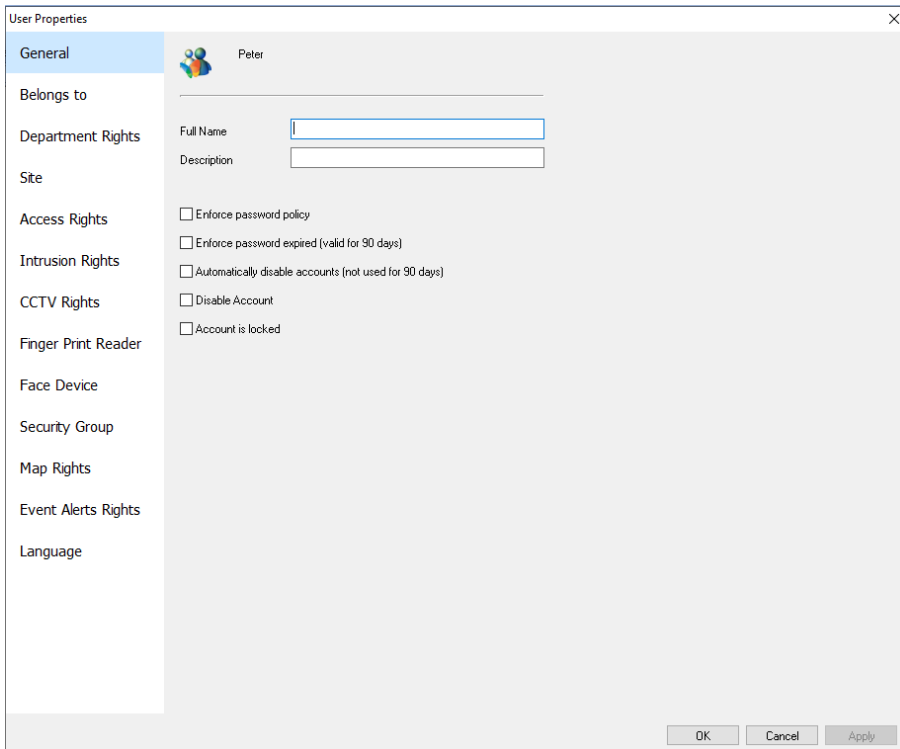
The 'New User' dialog box contains the following fields and options:

- Name:
- Full Name:
- Description:
- Separator line
- Password:
- Confirm:
- Enforce password policy
- Enforce password expired (valid for 90 days)
- Automatically disable accounts (not used for 90 days)
- The user must change the password at the next login
- Account Is Disabled

Buttons:

Editing a User

To modify a user, select or highlight and click Properties icon on top



The 'User Properties' dialog box shows the following details for user 'Peter':

- General: Peter
- Belongs to:
- Department Rights: Full Name: Description:
- Site:
- Access Rights: Enforce password policy
- Intrusion Rights: Enforce password expired (valid for 90 days)
- CCTV Rights: Automatically disable accounts (not used for 90 days)
- Finger Print Reader: Disable Account
- Face Device: Account is locked
- Security Group:
- Map Rights:
- Event Alerts Rights:
- Language:

Buttons:

General – this tab allows you to modify the full name and description

Belongs to – on this tab you can assign the user to a group

Department Rights – you can select the department rights on this tab

Site – select the site for this user to access

Access Rights – allows you to select the components or doors that the user have access to

Intrusion Rights – allows you to select the intrusion zones for alarm system

CCTV Rights – allows you to select the cameras, DVR that user should have access to

Fingerprint Reader – also allows the user to select the fingerprint reader user has access to

Face Device – select face device that the user has access to

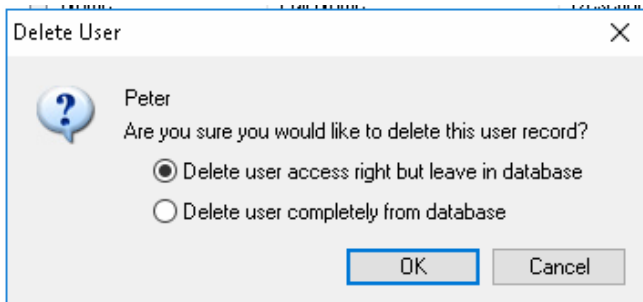
Security Group – select the security group the user has access to

Map Rights – Select the map you want the user to have access to

Event Alert Rights – Select the type of event the user to have access to

Language – select which language the user has access to change

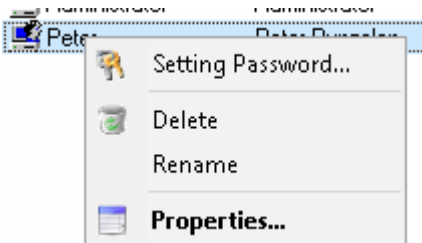
Deleting a Group or a User - To delete a user or group, select the user or group you want to delete and click **Delete** icon on top.



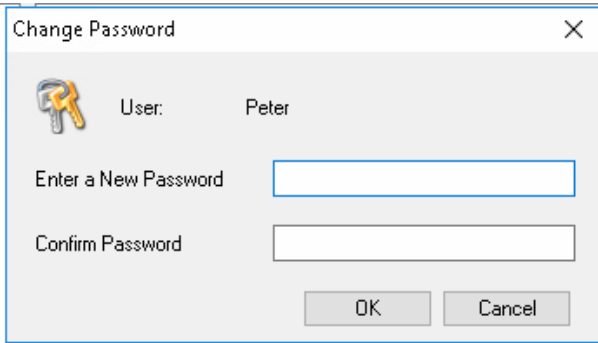
Select the option and click **OK**

3.3 Change Password

Right click the user and select *Setting Password* to change the password



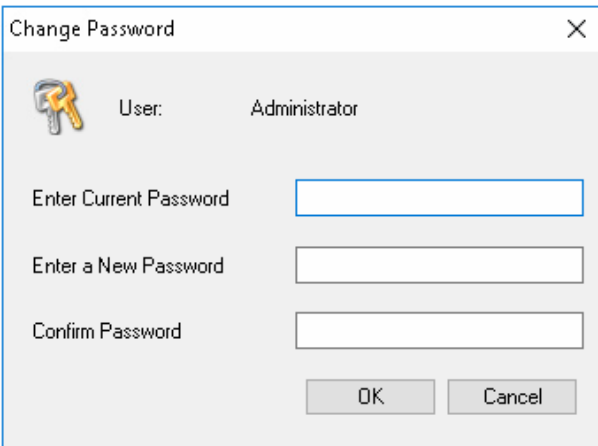
Input the new password and click **OK**



A screenshot of a 'Change Password' dialog box. The title bar reads 'Change Password' with a close button (X) on the right. On the left, there is a key icon. The text 'User: Peter' is displayed. Below this, there are two input fields: 'Enter a New Password' and 'Confirm Password'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

Change Password

The Administrator account's password can be change on the change password settings.



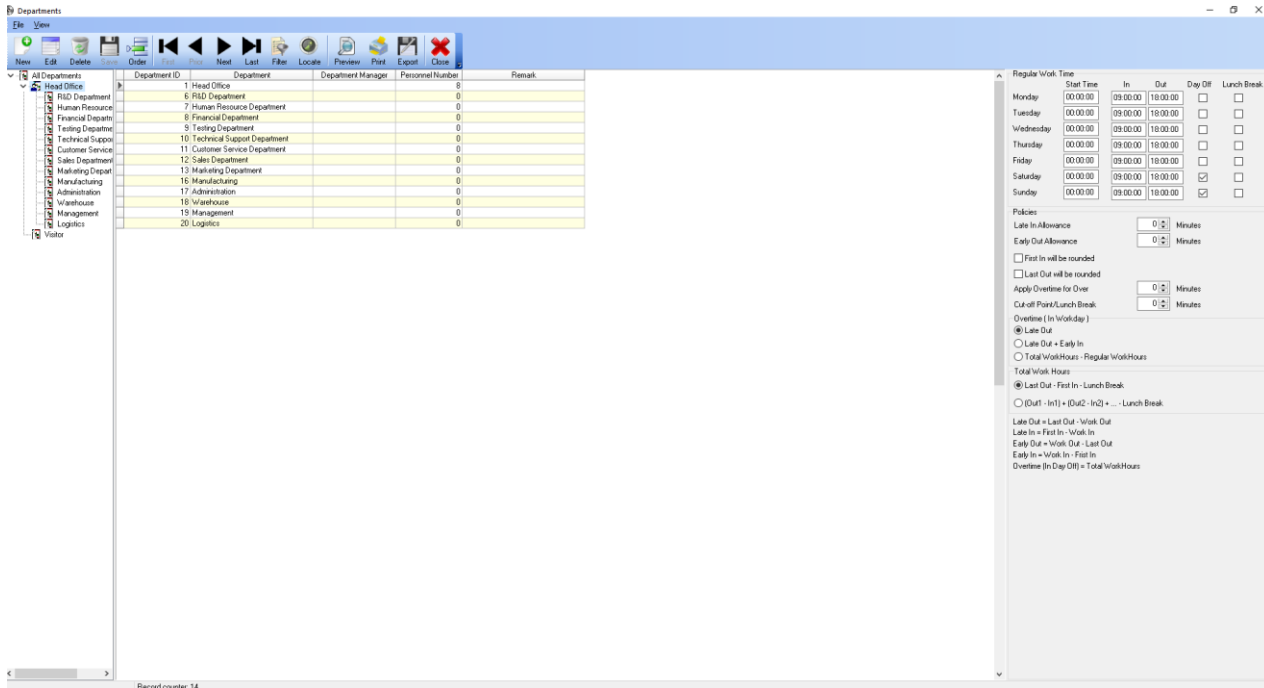
A screenshot of a 'Change Password' dialog box. The title bar reads 'Change Password' with a close button (X) on the right. On the left, there is a key icon. The text 'User: Administrator' is displayed. Below this, there are three input fields: 'Enter Current Password', 'Enter a New Password', and 'Confirm Password'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

3.4 Departments

Select *Management* on the main menu bar and then select *Departments* from the sub-menu or you can click on the



Department button. This will allow for additional departments or sub departments to be set up and an existing department to be deleted or to be edited.



Departments may also be further divided into Sub Departments if required.

Departments and Sub Departments assist us to set structure and group personnel together.



When clicking **New Department** a sister Department will be created. When clicking **New Sub Department** a Sub (*child*) Department will be created. It can also be used in case the system should be used for a multi company installation site.

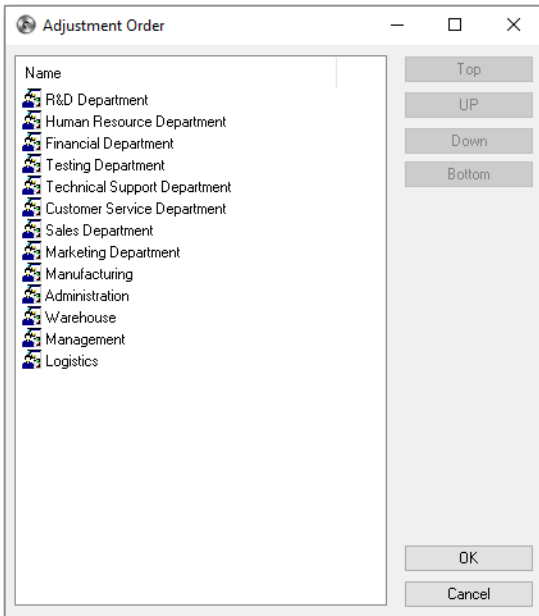
In such case each company will be a department and each company department will be a Sub Department.

The software enables the user to begin the configuration from the general setup menu. This way the setup is performed structurally and easily. Before adding new Personnel to the system we can design the company structure first and then assign the Personnel to Departments.

By Gender - The configuration performed in the 4 tabs will apply to personnel by gender.



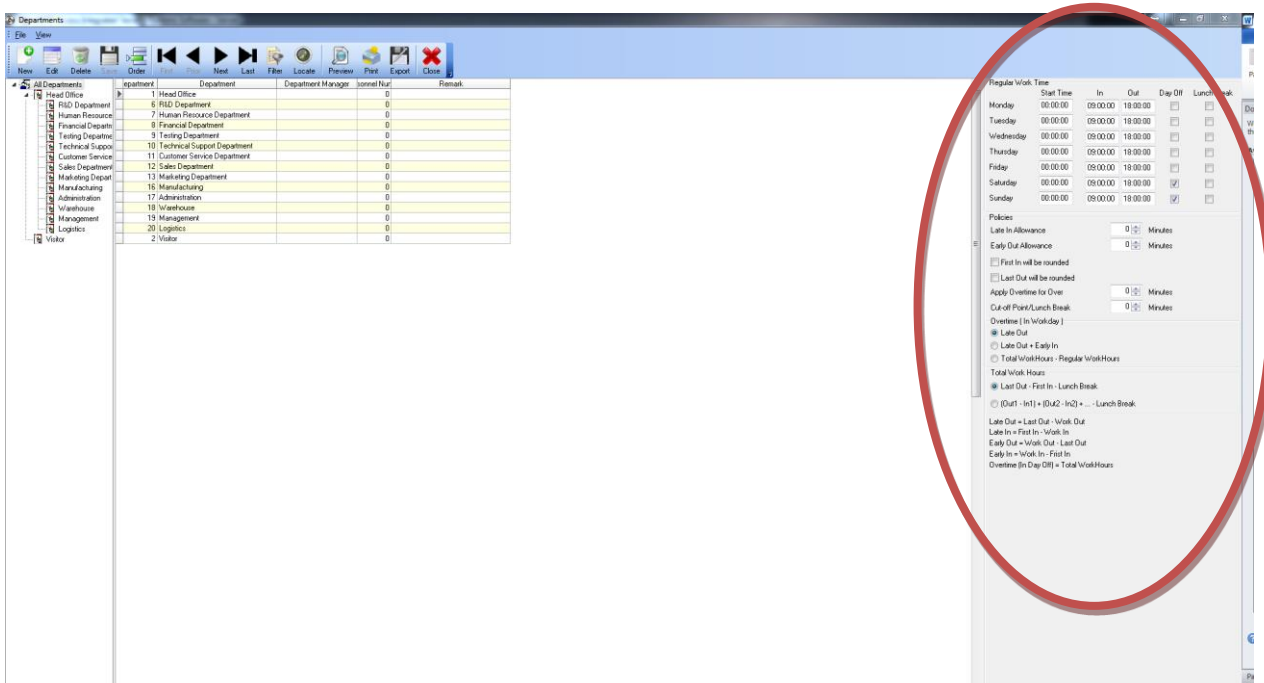
If **Set Sub Department Order** is clicked, the Window of Figure 6-17 will be opened.



You can adjust the order of the department which you selected by clicking the button *up* and *down*, *Top* and *Bottom*.

Time and Attendance Policy

Defining the Time and Attendance policy for the Department/Sub Department is done on the right hand side of form. Each Department/Sub Department can have its own policy.



Regular work time - including *IN* (or Work IN), *OUT* (or Work OUT) and *Day Off*.

IN Time is based on the time Personnel are coming to the office (the time the card event was created). The system will also calculate *Late In* (if he/she comes late) or *Early In* (if he/she comes to the office early).

Out Time is the time that the Personnel have left the office. This will be used to calculate *Early Out* or *Late Out* similar to *Early In* and *Late IN Time* based on the policy.

Day Off will be used to determine when the employee is entitled to a day off.

Late In/Early Out Allowance - The number of minutes allowed for coming *IN* late or going *OUT* early. The system will not report that the Personnel came late to the office if he arrives at 08:05 while the *Work IN* time is 08:00 and *Late IN* allowed is 15 minutes.

The Personnel will also be considered late only if he/she came after 08:15. The same rule applies for *Early Out Allowance* as well.

First In/Last Out will be rounded - Check this option if you would like to round the *IN* time if the minutes between in time and *Work In* are less than *Late In Allowance*. For example if Personnel arrive at the office between 07:45 to 08:15 there *In Time* of that day will be reported as 08:00 if the Allowance is 15 minutes. The rounding will be done similarly for *Last Out*.

Apply Over time for Over – The system will report that a Personnel has worked over time on a day if his/her *Over Time* of that day is bigger than X minutes then the *Over Time* will not be reported. The method to calculate over time is configured in the *Overtime section*. If 30 minutes is set and the Personnel over time is only 20 minutes on that day then the over time will not be counted.

Cut-off point/Lunch break – This period will be deducted from the time the Personnel have worked during the day.

Overtime Policy

In the *Overtime Policy* we can define if over time will be considered as *Late Out* only by the extra time the Personnel spent in the office or by adding the extra time (*Late Out* + *Early In*) of arriving at the office before the Regular *In time*. The third option is the total working hours minus the Regular Working hours.

Total Work Hours

This can be defined as *last Out – First In – Lunch Break*. In This way we ignore all *In/Out* during the working day. Alternatively, it can be defined as the intervals between the *In/Out* minus the *Lunch Break*. We can use this option if we would like to deduct the time the Personnel stayed Out of the office during the working day.

Variable Definition:

- *Last Out*: the last time the Personnel flashes his card at any of the system readers during a certain day. This time will be considered as the time the Personnel leaves the office.

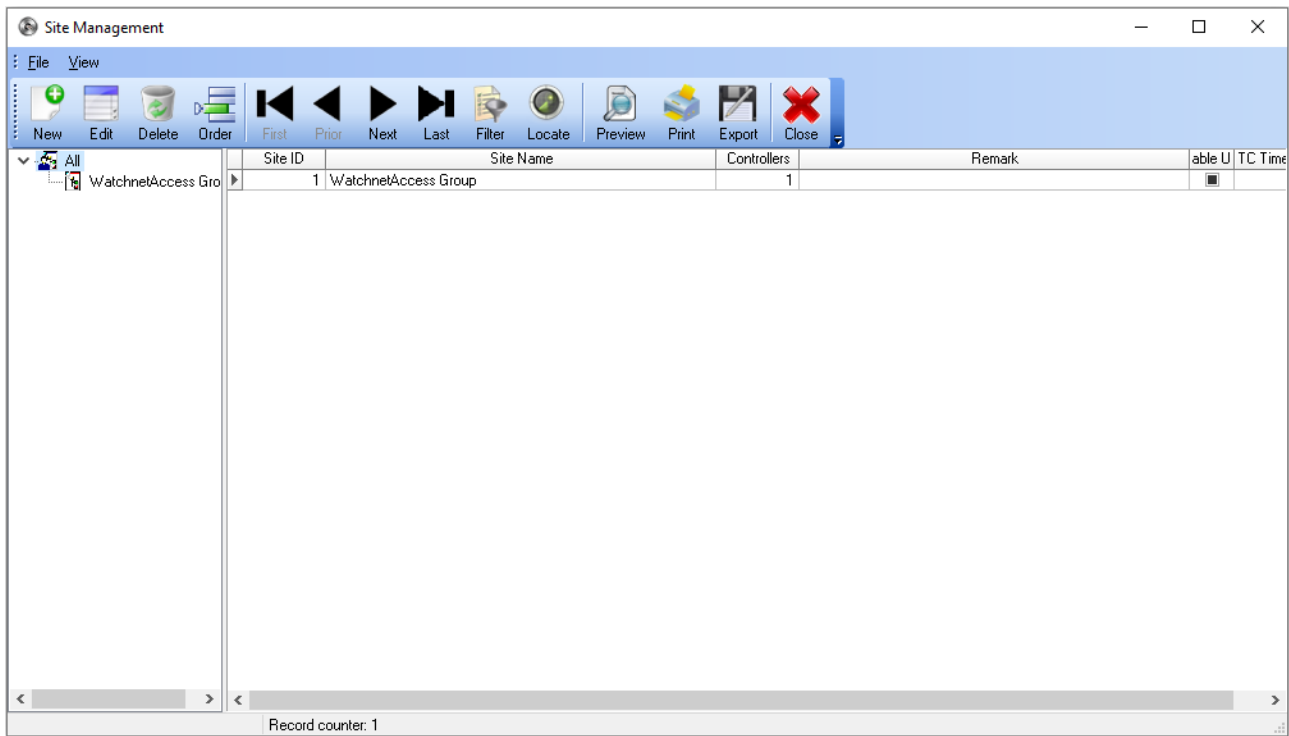
- *First IN:* the first time the Personnel flashes his card at any of the system readers during a certain day. This time will be considered as the time the Personnel arrives in the office.
- *Work IN:* the IN time which is defined in Regular Working Time.
- *Work OUT:* The Out time which is defined in Regular Working Time.

3.5 Group Management

Group Management allows you to create new group for personnel.

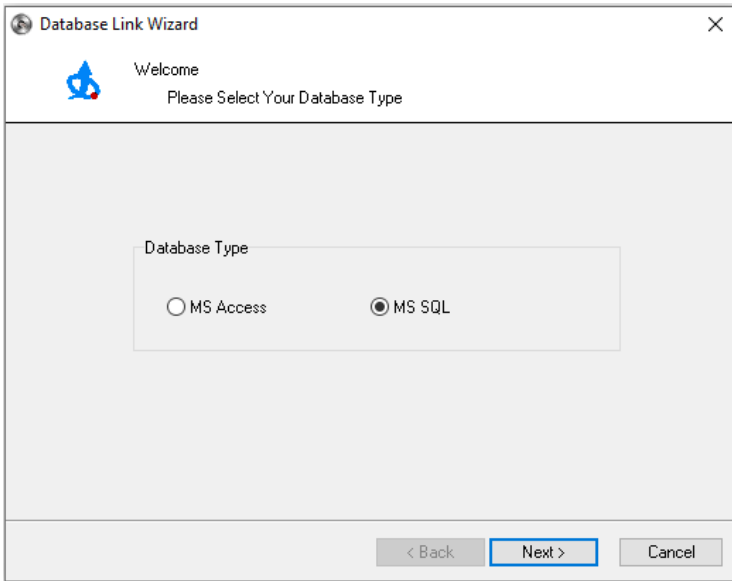
3.6 Site Management

Site Management allows you to add manage or delete different sites.



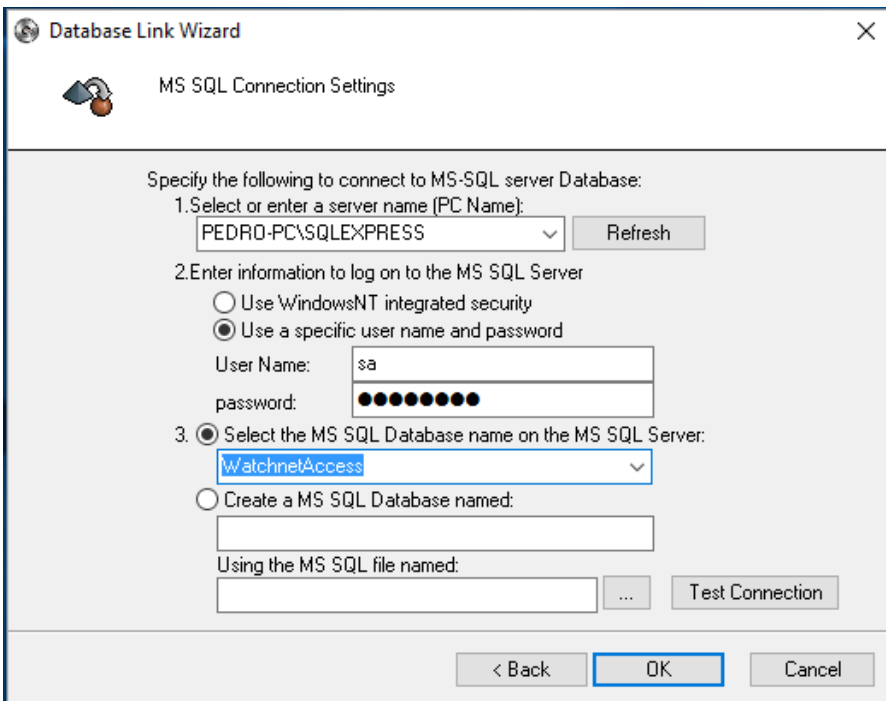
3.7 Change Database

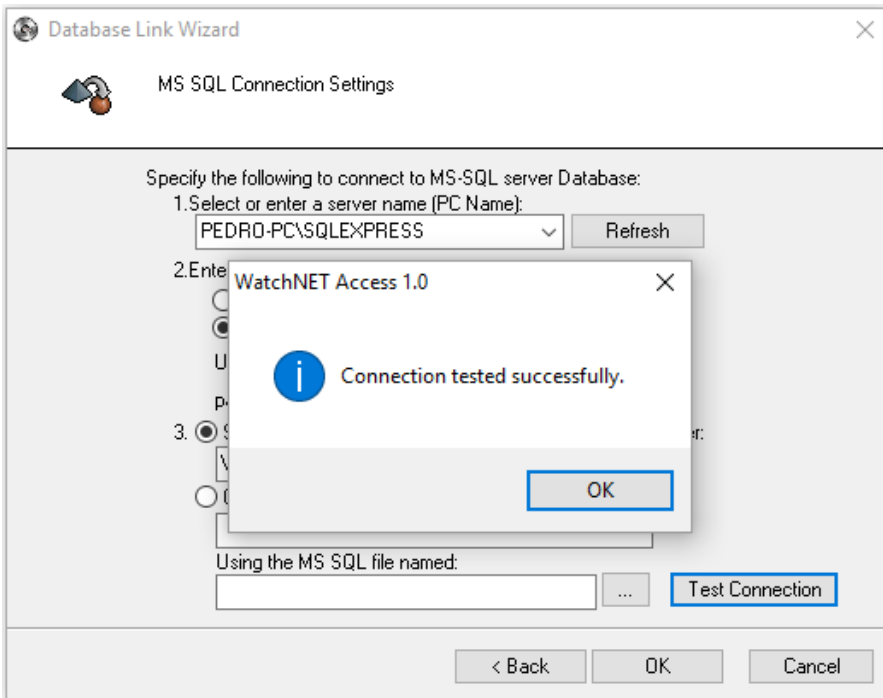
This setting allows you to change the database or connect the server to a different server as client



Select MS SQL data base

If you do not see the name of the SQL Server (*PEDRO-PC\SQLEXPRESS*) then copy and paste the name of the server from the *Microsoft SQL Server Management Studio Express*. Use *sa* and *watchnet* as the *User Name* and *Password* and select *WatchnetAccess* as the database from the pull down menu. Once this done click on the *Test Connection* button to test connection.

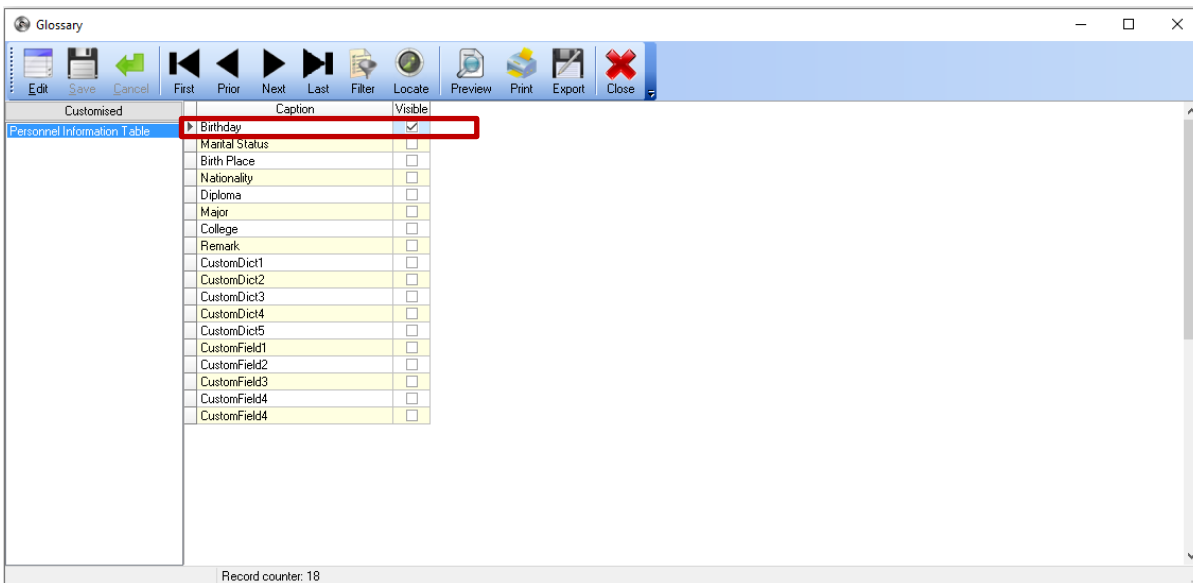




If the installation was configured correctly then you will see the above screen.

3.8 Glossary

Glossary allows you to modify the fields you want to display on the Basic Information tab of the Personal Information, you can hide, show or edit the field name that shows up on the tab.



Enabling the check box for the Birthday field will enable that field on the Basic Information tab

Personal Information

Basic Information

Card

Access Level

Fingerprint

Fingerprint Reader

Face Info

Personal Information

No. Code

First Name* Last Name

ID Number Gender

Department

Group Position

Joining Date

Last Day

Address Floor No.

TEL E-Mail

Birthday

3X4

Card Events QR Code Card Print OK Cancel Apply

3.9 System Management

System Management

Uniqueness Inspect

Events View/Alert Range

Screen Saver

Photo Viewer

Area Viewer

Card Validity

Other Options

Required and Repeatability Check

Personnel Code: Can not be empty Should be unique

First Name: Can not be empty Should be unique

Last Name: Can not be empty Should be unique

ID Number: Can not be empty Should be unique

Card Number for Wiegand should be unique (can not be duplicated)

Remove personnel information, directly to delete records; otherwise, to remove the tag

Delete expired visitor card automatically

Visitor will be in blacklist when it is expired

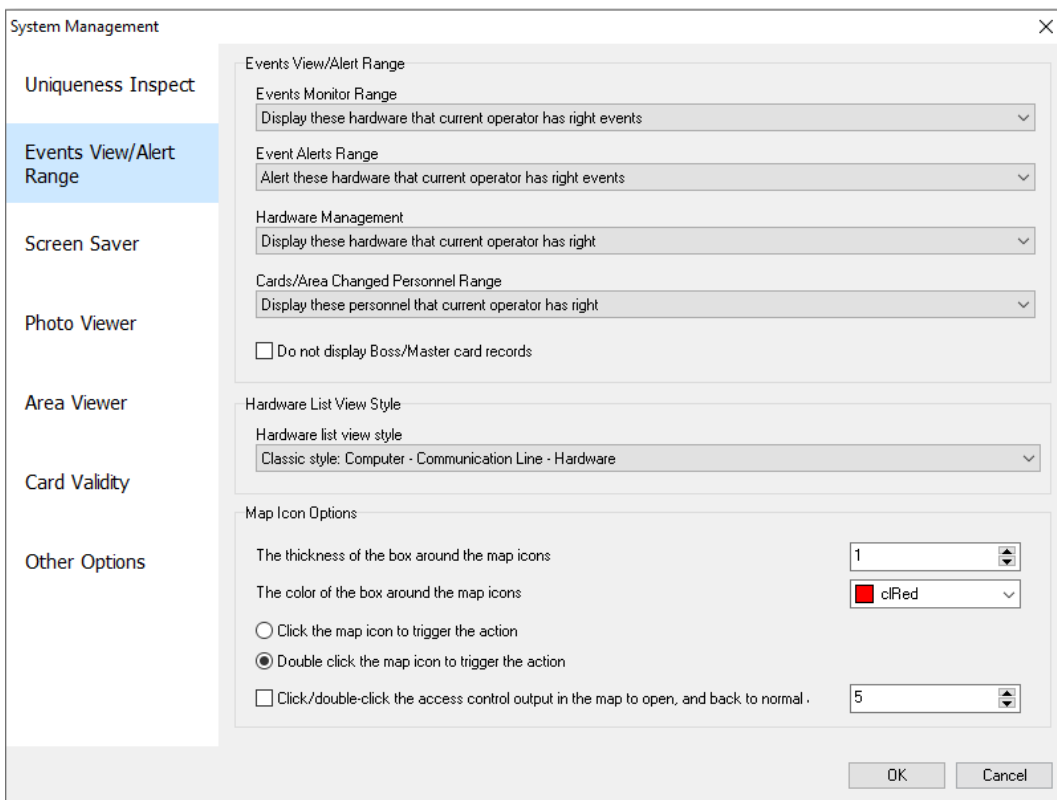
When a new person is registered, the Personnel ID should get vacant ID; Otherwise the ID will increased 1

OK Cancel

- **Uniqueness Inspect** – Below option to disable duplicate or field cannot be empty
 - **Personnel Code**
 - **First Name**
 - **Last Name**
 - **ID Number**

Events View/Alert Range

A user can define the range of events and alerts presented on the WatchNET Access software which is Events Monitor, Multi-Site View monitor and the Controller Manager

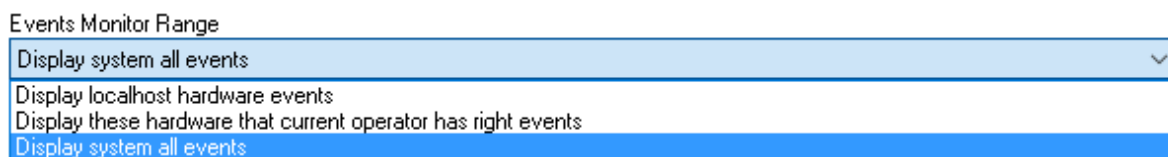


Events Monitor Range:

Display Localhost hardware events – Display events only on local server

Display these hardware that current operator has right events – Display events only for operator that has access rights to the software

Display system all events – Display all events for local server and client software



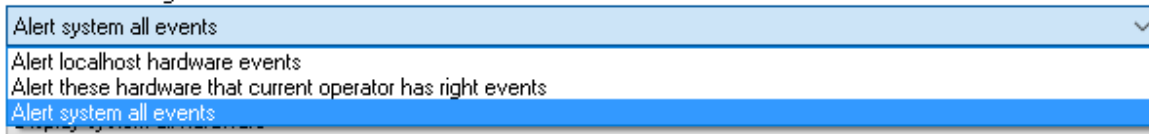
Events Alerts Range:

Alert local host hardware events - Only Alerts from panels which are connected to the PC which is running WatchNET Access Software will be displayed.

Alert this hardware that current operator has right event - Displays Alerts only from panels which are connected to the PC and that the user (see *User Accounts*, e.g. *Administrator*) has the privileges to monitor.

Alert system all events - Alert information from all panels will be displayed in the WatchNET Access Software including Server panels and the Client panels.

Event Alerts Range



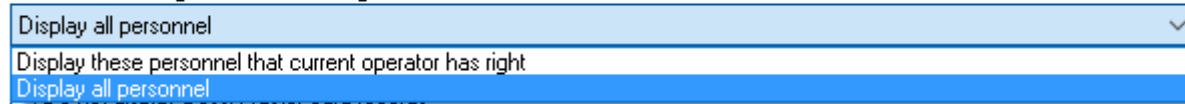
A screenshot of a dropdown menu titled "Event Alerts Range". The menu is open, showing three options: "Alert system all events", "Alert localhost hardware events", and "Alert these hardware that current operator has right events". The first option, "Alert system all events", is highlighted in blue.

Cards/Area Changed Personnel Range:

Display these personnel that current operator has right - Displays the personnel's cards and area's events.

Display all personnel - Displays all the cards and area changed events.

Cards/Area Changed Personnel Range



A screenshot of a dropdown menu titled "Cards/Area Changed Personnel Range". The menu is open, showing three options: "Display all personnel", "Display these personnel that current operator has right", and "Display all personnel". The first option, "Display all personnel", is highlighted in blue.

Screen Saver

To start up *Screen Saver* click the *Screen Saver* tab and check the *Enable* checkbox and then set up the time.

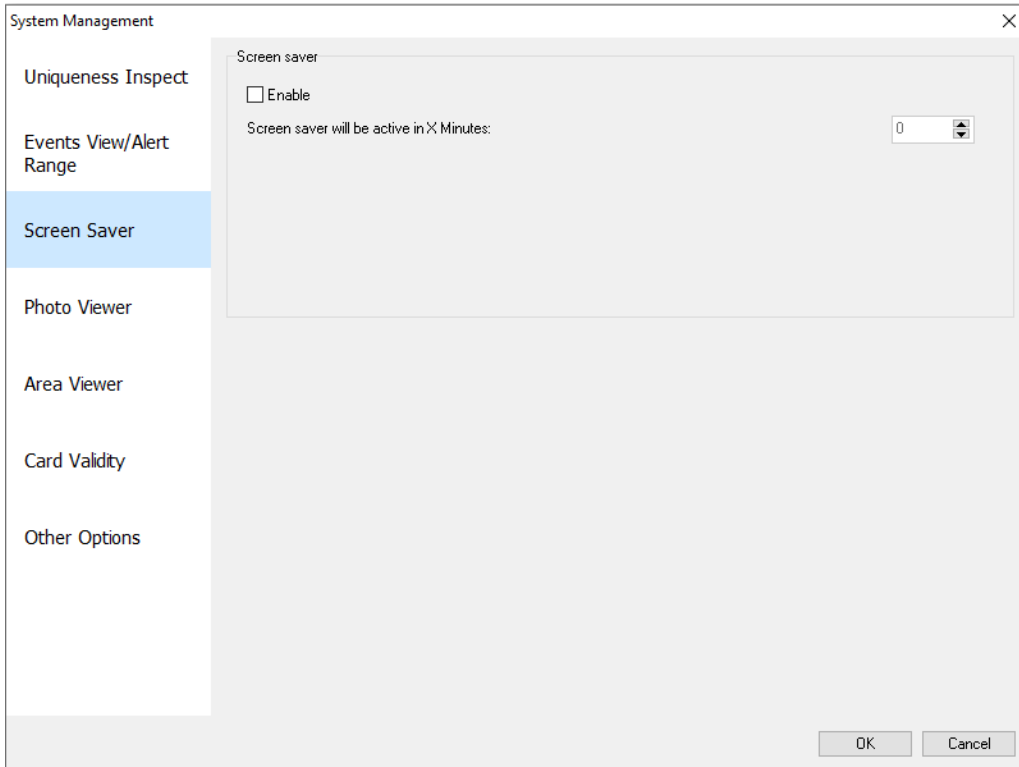
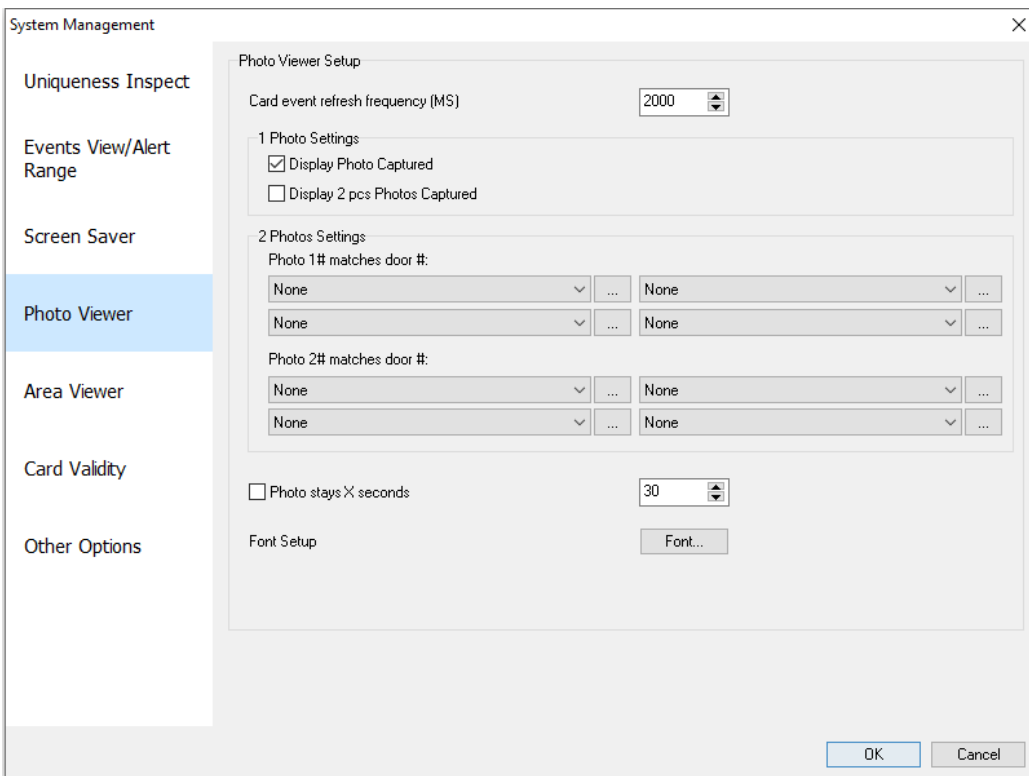


Photo Viewer

To set up the photo display times click on the *Photo Viewer* tab and then check the Photo Display Time(s) checkbox and then adjust the time. You can adjust the *Font* by clicking the *Font...* button.



Area Viewer

The area viewer is for Anti-passback feature and setup the area such as inside area and outside area, can also select a camera where the anti-passback door is configured.

The screenshot shows the 'System Management' window with the 'Area Viewer' tab selected in the left sidebar. The main content area is titled 'Area Setup' and contains the following fields and options:

- Inside Area:** A dropdown menu set to 'Inside'.
- Outside Area:** A dropdown menu set to 'Outside' and a checkbox for 'Show personnel list of outside'.
- Reset Counter:** A checkbox for 'Multi transactions of the same card, will be marked as one time only' (checked), a dropdown for '1:00:00 AM' (checked), and a checkbox for 'Reset personnel counter'.
- Scroll Text:** A section with a 'Message' text box, a 'Speed(1-100)' dropdown set to '60', and a 'Font' button.
- Channel:** Two dropdown menus for 'DVR' and 'Channel', with an ellipsis button next to the 'Channel' dropdown.
- Number of Display Style:** A dropdown menu set to 'Simple Count' and a 'Display Content Definition' button.

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

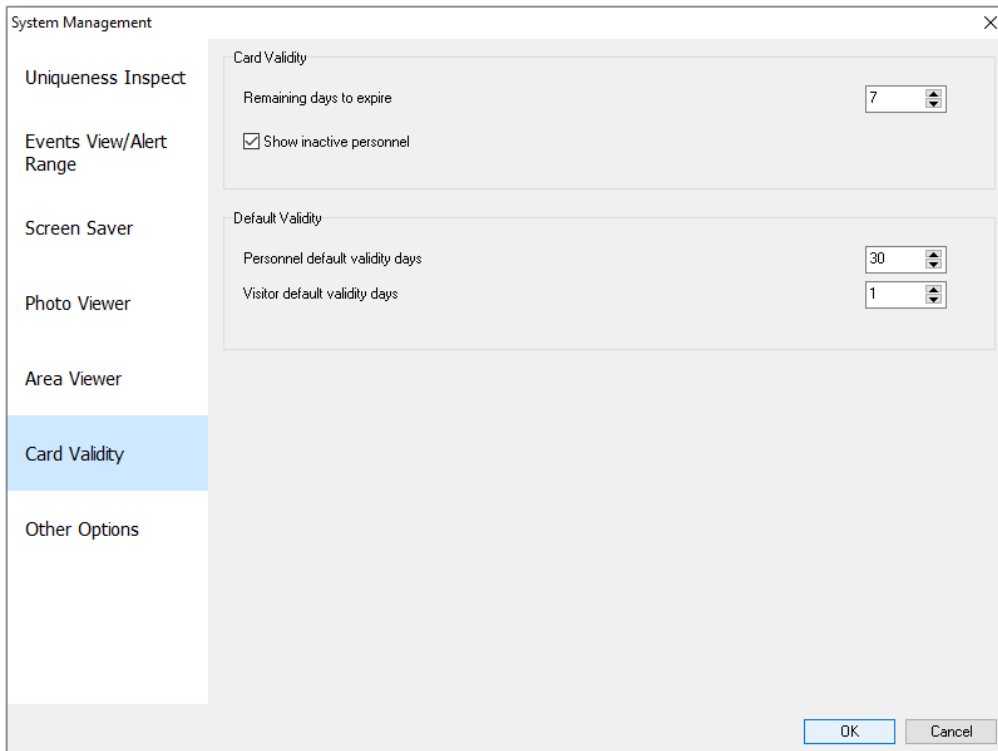
Area Setup: enables you to count who is in an area and to display these details on a large screen monitor.

- **Scroll text:** sends a scrolling message to a large screen monitor.
- **Channel:** displays the designated camera on the Window.

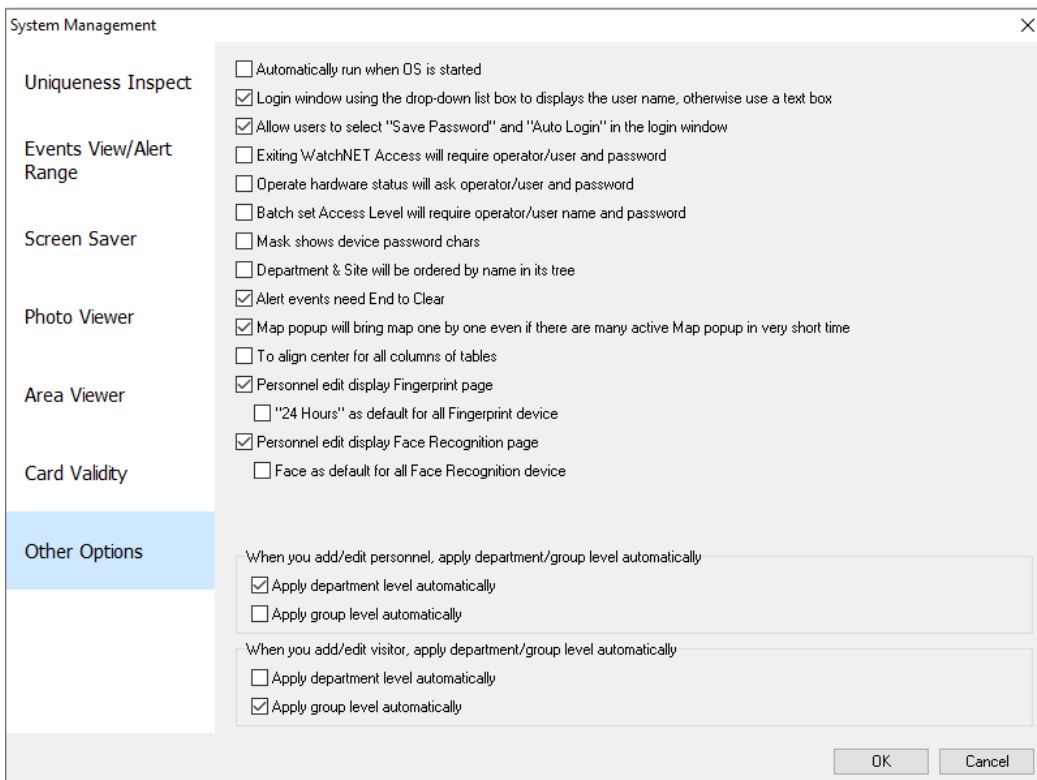
Note: this has been designed for large screen monitor and so on a standard monitor the resolution may not be appropriate

Card Validity - To set up card validity of personnel when card is inactive and shows inactive personnel from the

software

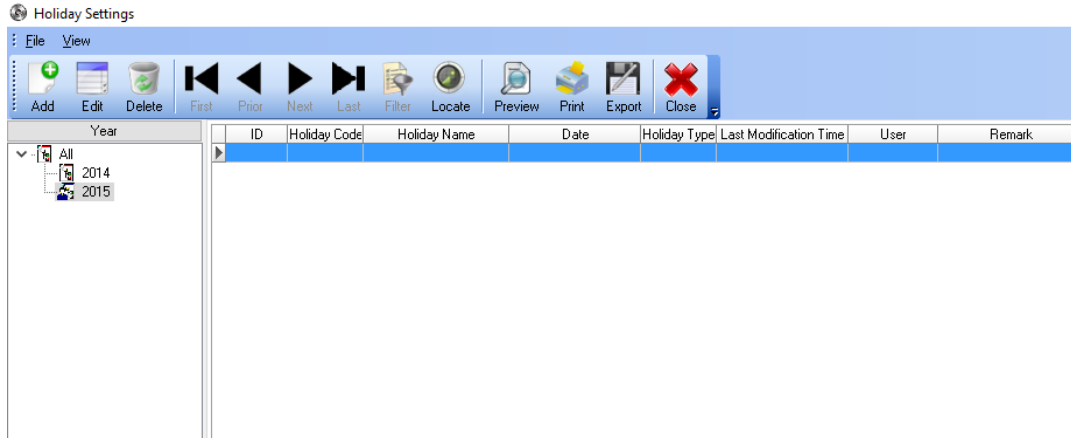


Other Options – Other options you can disable/enable such as Automatically run when OS is started, ask username/password when opening hardware status and others.



3.10 Holiday Settings

Configure and rename holidays for the year

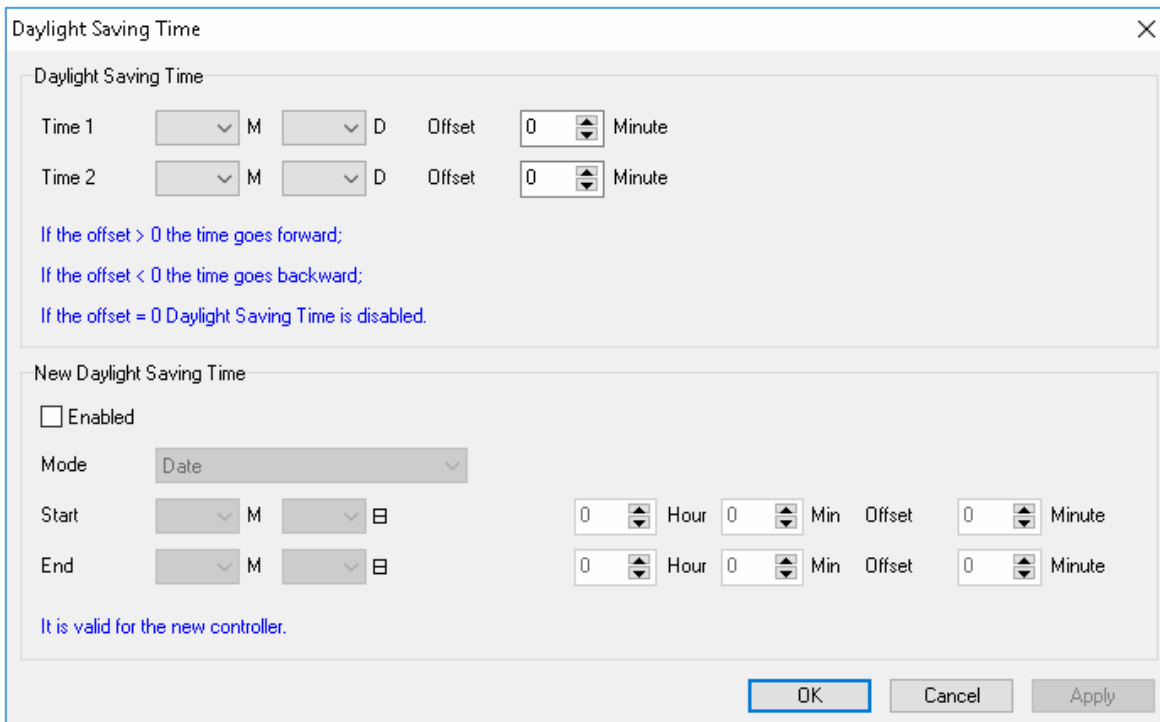


3.11 Daylight Savings Time

To set up Daylight Savings Time select *Management* and then *Daylight-Saving Time*.

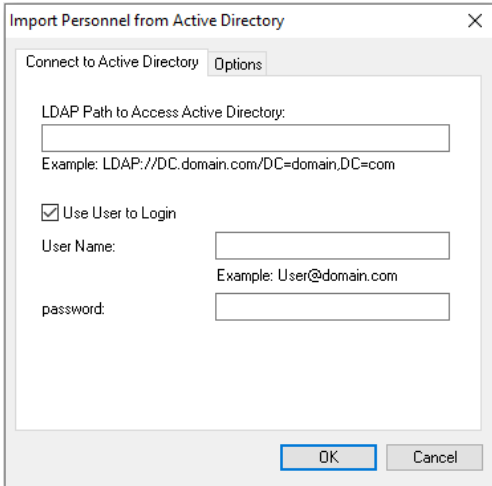
Use the drop-down menus of Time 1 to set the month then the day that the daylight savings time begins and the number of minutes that the time will be advanced.

Note: *Upper setting only works on Ver.45 controllers, "New Daylight-Saving Time" setting works only on Ver.03 controller*



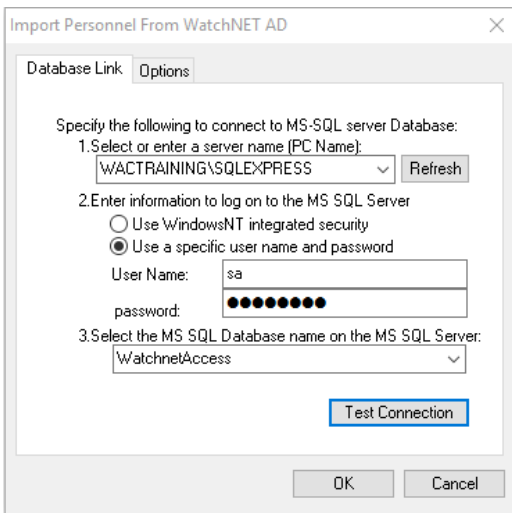
3.12 Import Active Directory

You can import personnel names from an active directory using this feature



3.13 Connect WatchNET Active Directory Database

To connect to the Active Directory select *Management* and then *Connect WatchNET Active Directory*.



In the *Import Personnel From WatchNET AD* select the *Database Link* tab. Select the server name from the *Select or enter a server name (PC Name)* from the drop down menu.

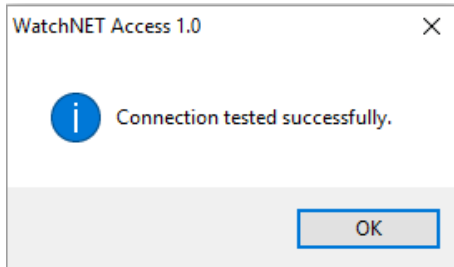
Note: if the drop-down menu is empty then click on the Refresh button.

Next select *Use a specific user name and password* from the *Enter information to log on to the MS SQL Server* option. Type *sa* for *User Name:* and *watchnet* for *password:*

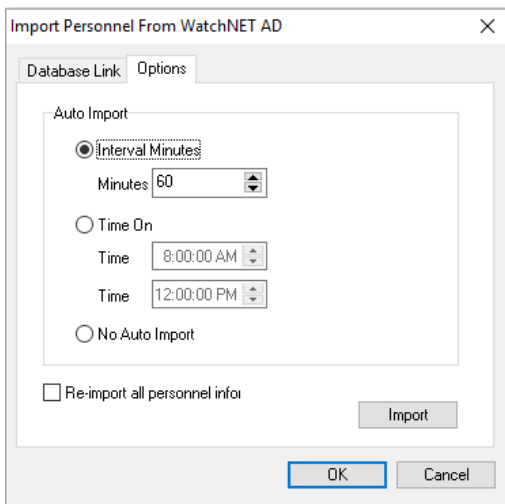
Next select the *WatchnetAccess* database from the drop down menu of the *Select the MS SQL Database name on*

the MS SQL Server: option.

To finish configuring the Active Directory setup click on the *Test Connection* button.

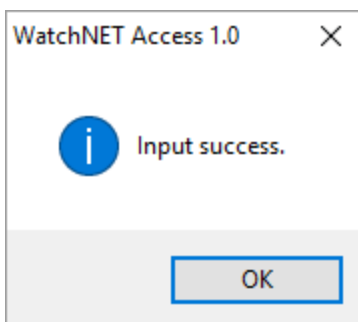


The *Connection tested successfully* message appears. Click *OK* to close the message box.



To select AD importing options click on the *Options* tab.

Click the "*Import*" button for the first import.



Note: If the database "WatchNETAD" table does not exist when you click the import button then the software will auto create the table in the database.

WatchNETAD table structure:

```
CREATE TABLE [WatchNetAD] (  
    [AutoID] [int] IDENTITY (1, 1) NOT NULL ,  
    [ID] [nvarchar] (50) NULL ,  
    [State] [smallint] NULL ,  
    [FirstName] [nvarchar] (20) NULL ,  
    [LastName] [nvarchar] (20) NULL ,  
    [DisplayName] [nvarchar] (50) NULL ,  
    [Office] [nvarchar] (50) NULL ,  
    [TelephoneNumber] [nvarchar] (20) NULL ,  
    [CardNumber] [varchar] (20) NULL  
) ON [PRIMARY]  
ALTER TABLE [WatchNetAD] WITH NOCHECK ADD  
    CONSTRAINT [PK_WatchNetAD] PRIMARY KEY CLUSTERED  
    (  
        [AutoID]  
    ) ON [PRIMARY]
```

Chapter 4 Setup Menu

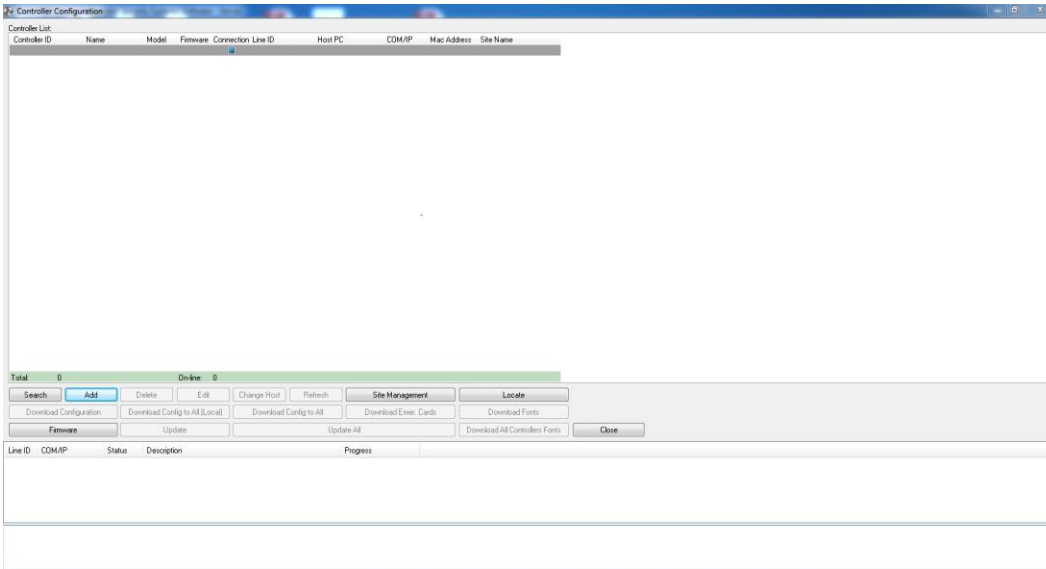
4.1 Hardware

4.1.1 Controller Configuration

To start to search for the controllers click on *Setup -> Controller Configuration*.



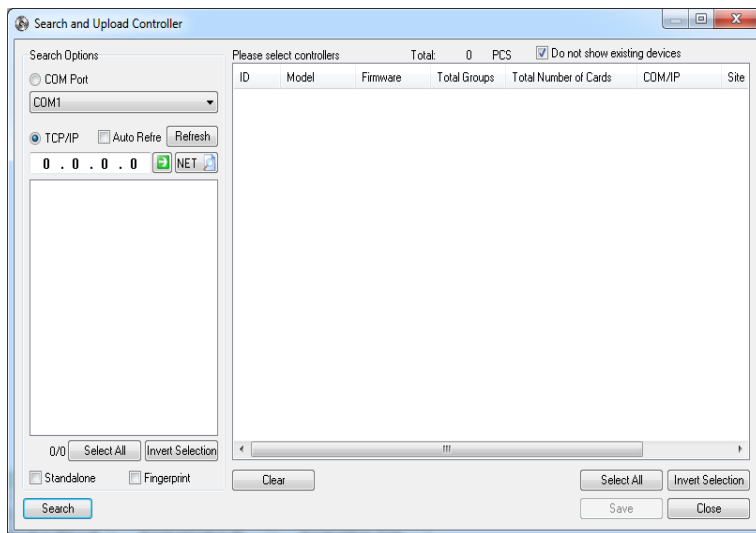
Or you can click *Controller Configuration icon* -



Searching for Controllers

The WatchNET Access controller’s architecture allows for one quick step searching without the need for manually configuring panels.

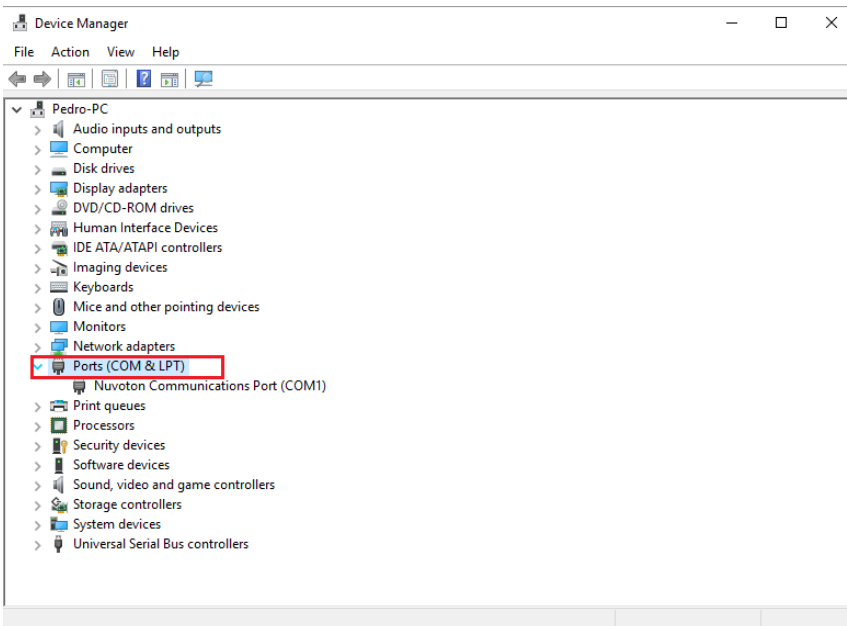
To begin searching for the panels click on the *Search* button and then the *Search and Upload Controller* window will display.



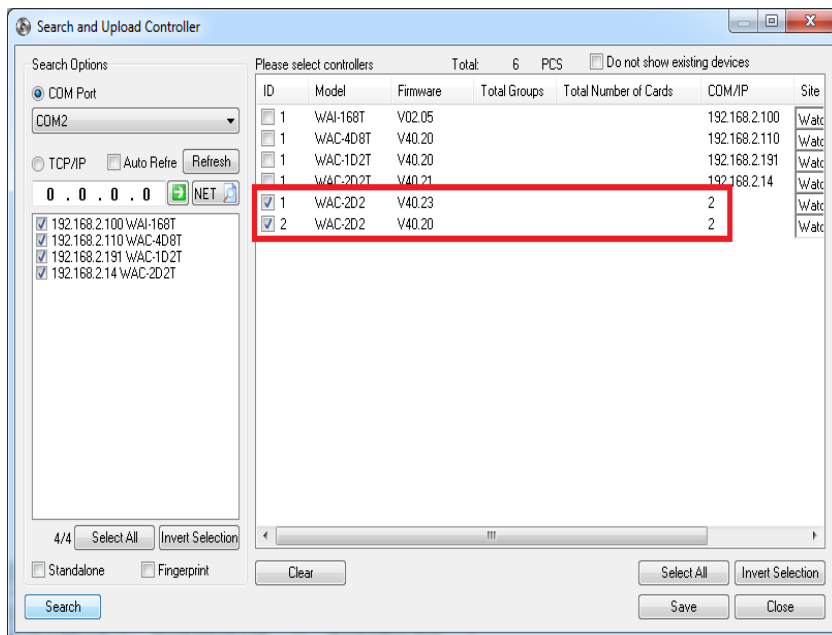
You can search the WatchNET Access panels either through a COM port or through TCP/IP.

Searching panels over a COM port – Is used when the controller is connected directly to the Server through the RS232 connectors or USB port if a RS232-USB converter is used. This also applies when a group of panels are connected together through RS485 communication or when a RS485 to RS232 converter is used to connect to the serial port of the Server. If you are not sure to which COM Port your panels are connected please go to the *Windows*

Control Panel -> System -> Hardware -> Device Manager -> Ports (COM & LPT).

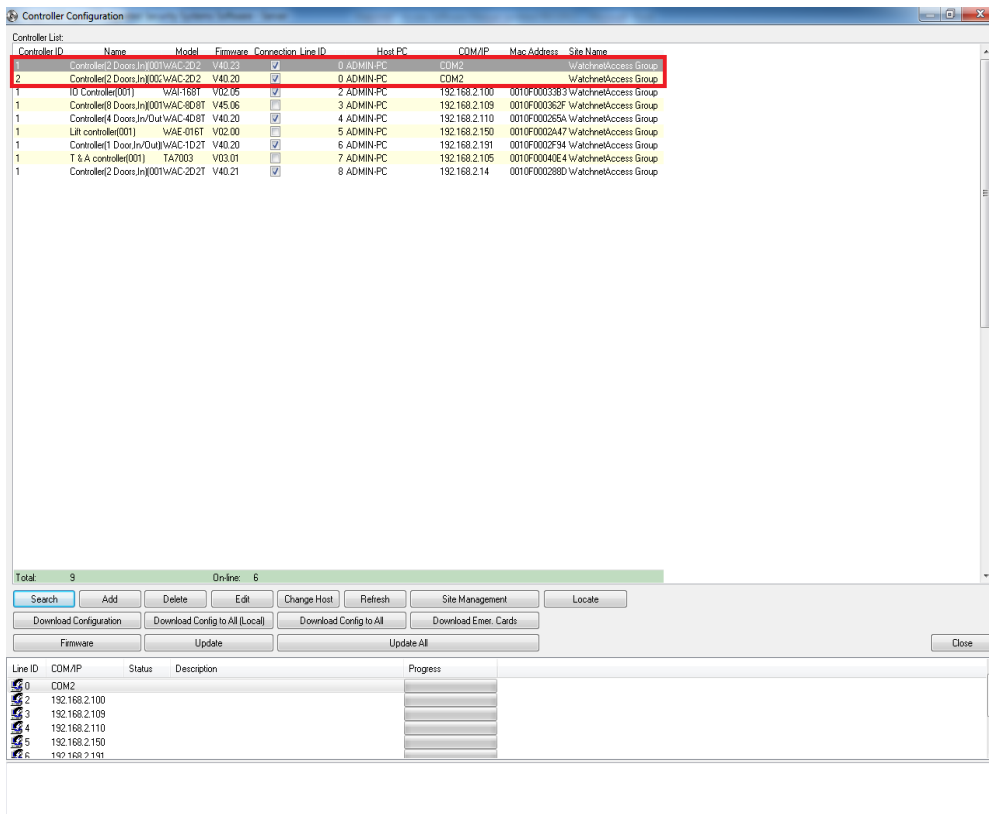


Click on *Search* and the connected panels will be listed.



Check the boxes of the ID column of the panels you would like to connect to.

Click *Save* and then *Close*. The panels will be listed in the *Controller Configuration* dialog box.

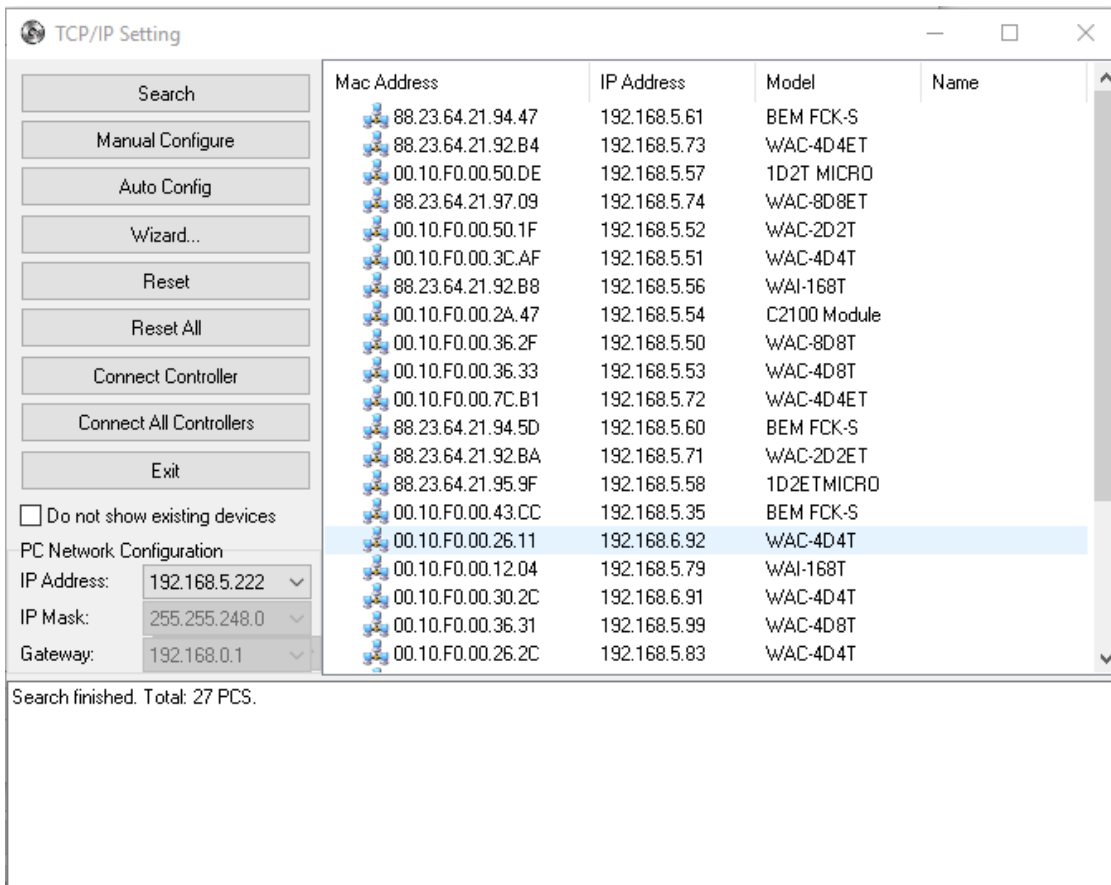


Searching Panels over an IP address - WatchNET Access provide panels with built in fully integrated TCP/IP module. Unlike other Access Control Software's in the market which are using external converter and Virtual IP address. WatchNET Access panels use real TCP/IP communication and real IP address.

The setup of the IP address can be done automatically.

- **Search** – Searches for controller in the network
- **Manual Configure** – Manually configures the IP address by setting each of the parameters.
- **Auto Configure** – Software will configure the IP address automatically.
- **Wizard...** - The wizard will collect the information necessary to configure the controller module
- **Reset** - Restarts the controller module.
- **Connect Controller** – Connects the selected controller(s) which works under the *TCP Server* mode.
- **Connect All Panels** – Connects the entire controllers which work under the *TCP Server* mode.
- **Exit** – Exits the dialog box.

On the controller PCB board near the blinking communication LEDs, there is a DIP Switch (S2) with DIP1 and DIP2. DIP1 is Write Protect for the IP address; please make sure DIP1 is ON before configuring the IP address. DIP2 sets a fixed IP (factory Default IP) of 10.1.1.10 regardless of the status of DIP1. Please make sure DIP2 is OFF.



To start searching for panels click on the *Search* button. All Mac addresses will be listed. Double click on the one you would like to configure and the *TCP/IP Setting* window display.

- **Mac Address:** A unique identifier attached to the network adapter (the TCP/IP module).
- **Name:** Controller name which can be a maximum of 30 alpha-numeric characters.
- **IP Address:** The IP address of the controller.
- **Mask:** The Subnet Mask of the Network
- **Gateway:** The Default Gateway
- **Port:** TCP/IP port which can be between 1024 to 65535. The default value is 8000.
- **Work Mode:** If you select *TCP Client* then the controller will connect the host which is specified by the Host IP otherwise the controller will wait for the client's connection.
- **Host IP:** The IP address of the PC which is connected to the panels through the TCP/IP network. The Host PC will receive all panels' card events.
- **Server Port:** Can be between 1024 to 65535. The default value of 8000.

TCP/IP Setting

Model: WAC-4D4T

Mac Address: 00.10.F0.00.26.11

Name:

IP Address:

Mask:

Gateway:

Port:

Work Mode:

Host IP:

Host Port:

Auto Config

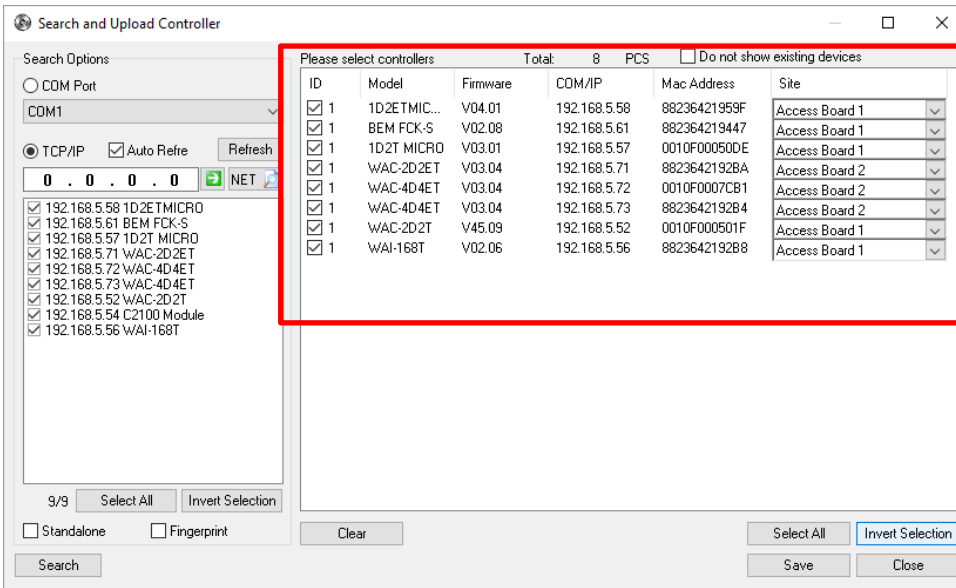
Click *OK* to finish and log message should come up saying *'parameter successfully'*

TCP/IP Setting

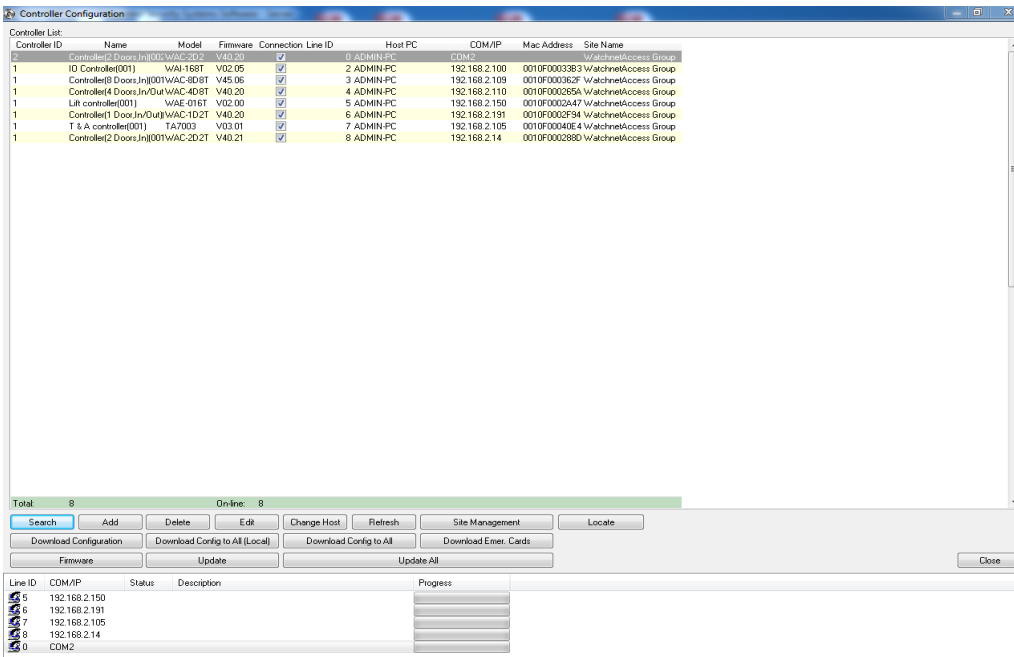
Mac Address	IP Address	Model	Name
88.23.64.21.94.47	192.168.5.61	BEM FCK-S	Access
88.23.64.21.92.B4	192.168.5.73	WAC-4D4ET	
00.10.F0.00.50.DE	192.168.5.57	1D2T MICRO	
88.23.64.21.97.09	192.168.5.74	WAC-8D8ET	
00.10.F0.00.50.1F	192.168.5.52	WAC-2D2T	
00.10.F0.00.3C.AF	192.168.5.51	WAC-4D4T	
88.23.64.21.92.B8	192.168.5.56	WAI-168T	
00.10.F0.00.2A.47	192.168.5.54	C2100 Module	
00.10.F0.00.36.2F	192.168.5.50	WAC-8D8T	
00.10.F0.00.36.33	192.168.5.53	WAC-4D8T	
00.10.F0.00.7C.B1	192.168.5.72	WAC-4D4ET	
88.23.64.21.94.5D	192.168.5.60	BEM FCK-S	
88.23.64.21.92.BA	192.168.5.71	WAC-2D2ET	
88.23.64.21.95.9F	192.168.5.58	1D2ETMICRO	
00.10.F0.00.43.CC	192.168.5.35	BEM FCK-S	
00.10.F0.00.26.11	192.168.6.92	WAC-4D4T	
00.10.F0.00.12.04	192.168.5.79	WAI-168T	
00.10.F0.00.30.2C	192.168.6.91	WAC-4D4T	
00.10.F0.00.36.31	192.168.5.99	WAC-4D8T	
00.10.F0.00.26.2C	192.168.5.83	WAC-4D4T	

Search finished. Total: 27 PCS.
Set 88.23.64.21.92.B4 parameter successfully!

Close *TCP/IP Setting*



Check the panels you would like to add and click *Save* and then *Close*. The panels have been searched and recognized by WatchNET Access Software.



Adding a Controller

Alternatively to searching for the panels automatically the user can add a controller by clicking on the *Add* button on the *Controller Configuration* form. The *Add Controller*. Click on the drop down menu to select the *Controller Type Model* then enter a *Name* for the controller. The controller name can be a maximum of 30 alpha-numeric characters. Next enter the *COM Port* or the *IP Address* and *Port* of the controller that is being added.

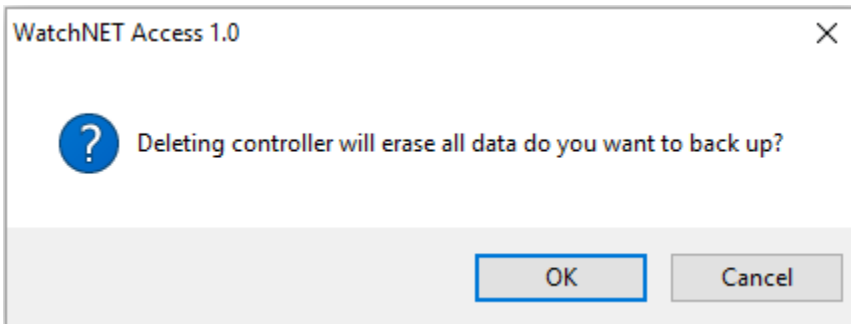
Note: the controller hardware DIP switches (1-8) must be configured before panels are added.

Deleting a Controller

To delete a controller highlight the controller to be deleted and then click on the *Delete* button.

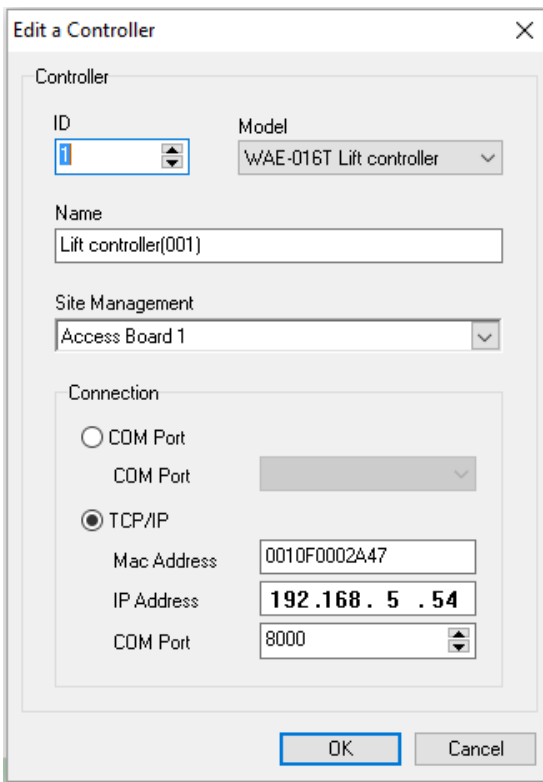
Controller ID	Name	Model	Firmware	Connection	Line ID	Host PC	COM/IP	Mac Address	Site Name
2	Controller(2 Doors,In)001WAC-2D2	V40.20	✓	COM2	0	ADMIN-PC	192.168.2.100	0010F0003B3	WatchnetAccess Group
1	ID Controller(001)	WAI-168T V02.05	✓	COM2	2	ADMIN-PC	192.168.2.109	0010F000362F	WatchnetAccess Group
1	Controller(8 Doors,In)001WAC-8D8T	V45.06	✓	COM2	3	ADMIN-PC	192.168.2.110	0010F000355A	WatchnetAccess Group
1	Controller(4 Doors,In/Out)WAC-4D8T	V40.20	✓	COM2	4	ADMIN-PC	192.168.2.150	0010F0002A47	WatchnetAccess Group
1	LIR controller(001)	WAE-016T V02.00	✓	COM2	5	ADMIN-PC	192.168.2.191	0010F0002F94	WatchnetAccess Group
1	Controller(1 Door,In/Out)WAC-1D2T	V40.20	✓	COM2	6	ADMIN-PC	192.168.2.105	0010F00040E4	WatchnetAccess Group
1	T & A controller(001)	TA7003 V03.01	✓	COM2	7	ADMIN-PC	192.168.2.14	0010F000288D	WatchnetAccess Group
1	Controller(2 Doors,In)001WAC-2D2T	V40.21	✓	COM2	8	ADMIN-PC			

Click *OK* to confirm deletion.



Editing a Controller

Editing the selected controller parameters (Figure 7-17)



Refresh a Controller

To refresh the displayed status of all the panels click on the *Refresh* button.

Download a Configuration

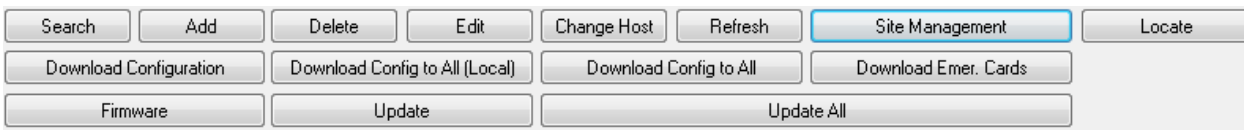
To download a current WatchNET Access Software database setting and configuration from the Server to a specific controller, highlight the controller then click on the *Download* button.

Download Configuration to All (Local)

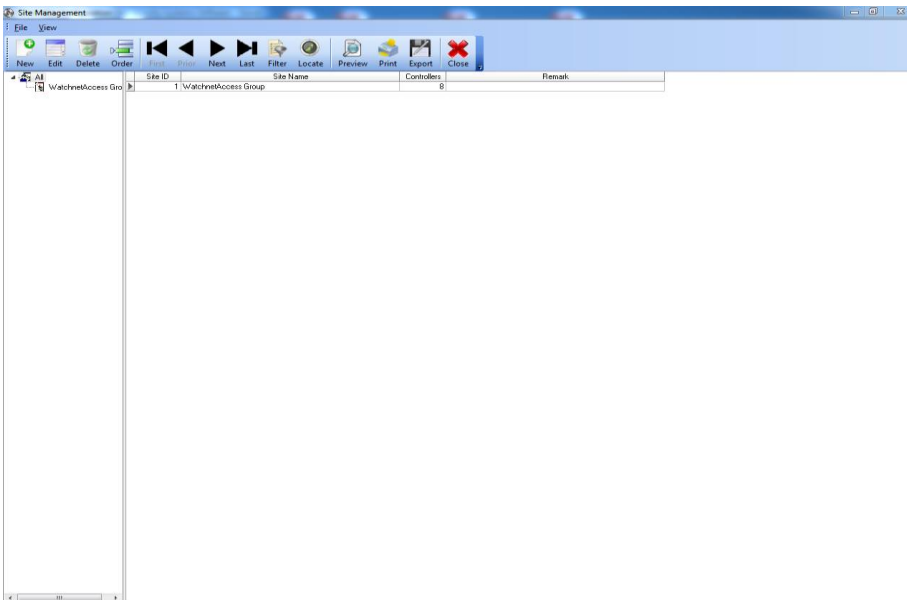
To download the current database from the Server to all the panels, click on the *Download Configuration to All (Local)* button.

Site Management

To open the Site Management window click on the *Site Management* Button from the *Controller Configuration* window.



The *Site Management* window appears.



In the *Site Management* window, you can add the name of projects or installations.

4.1.2 TCP/IP Setting - This menu is same on controller configuration.

4.1.3 Search Controller - This menu is same on controller configuration.

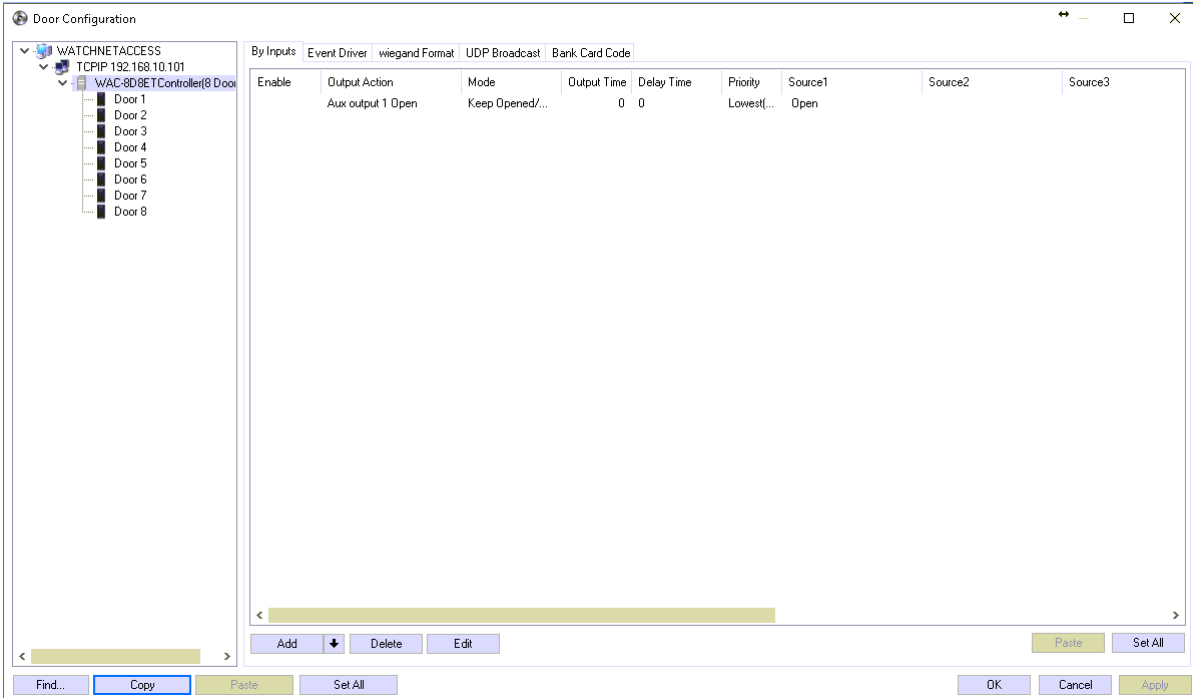
4.1.4 Door Configuration - To start configuring the doors, select Setup -> Hardware and then *Doors Configuration*



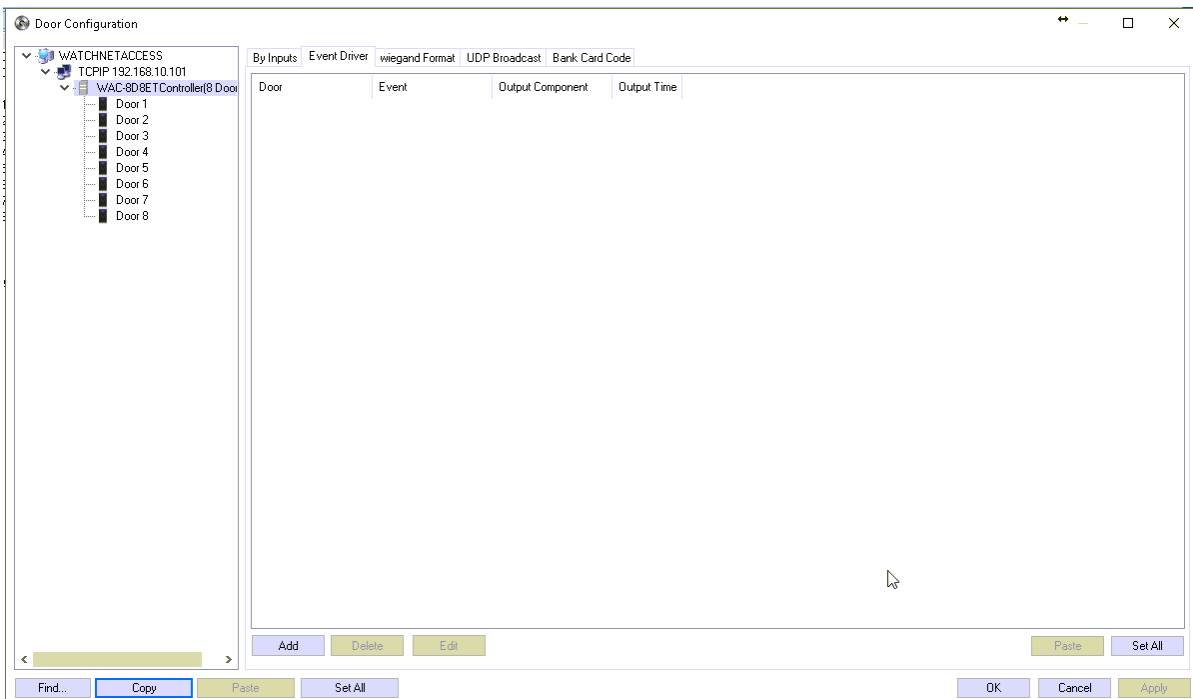
from the main menu or you can click on the *Doors* icon.

The *Door Configuration* window consists of 5 tabs: *Parameters*, *Door Status Schedule*, *Door Access Schedule*, *Personnel Access Level* and *Channel Mapping*, also on door configuration you can setup a flow control, event driver, wiegand format, UDP Broadcast and bank card code.

By Inputs - By Inputs configuration allows you to modify the flow control on the specific control such as open and closing condition



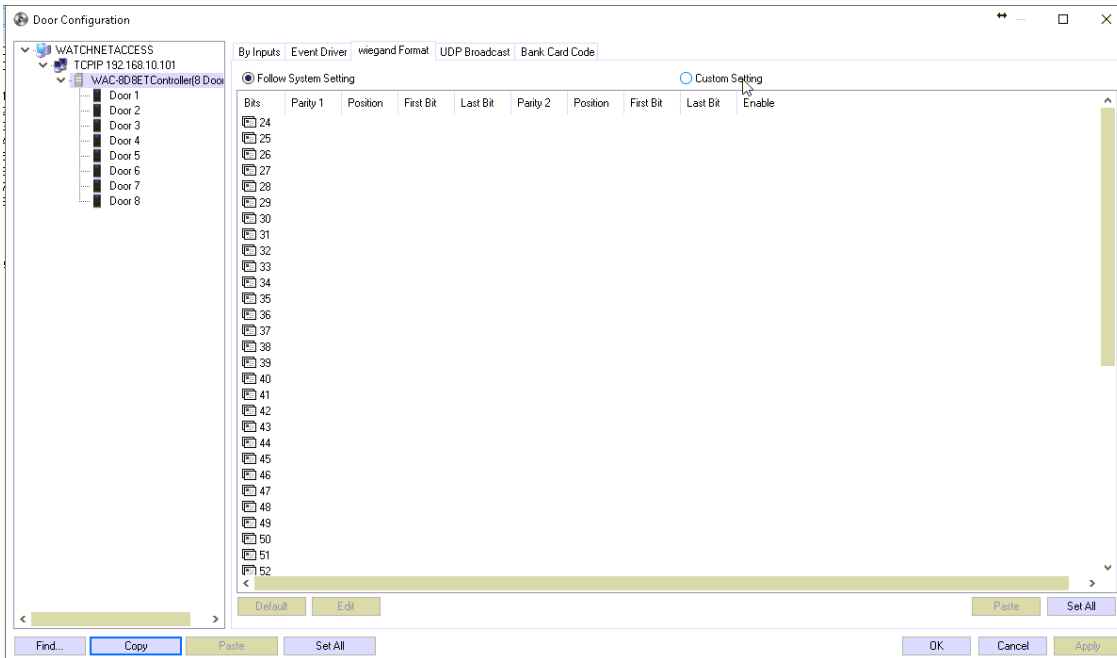
Event Driver - Event driver is where you can configure a flow control using events.



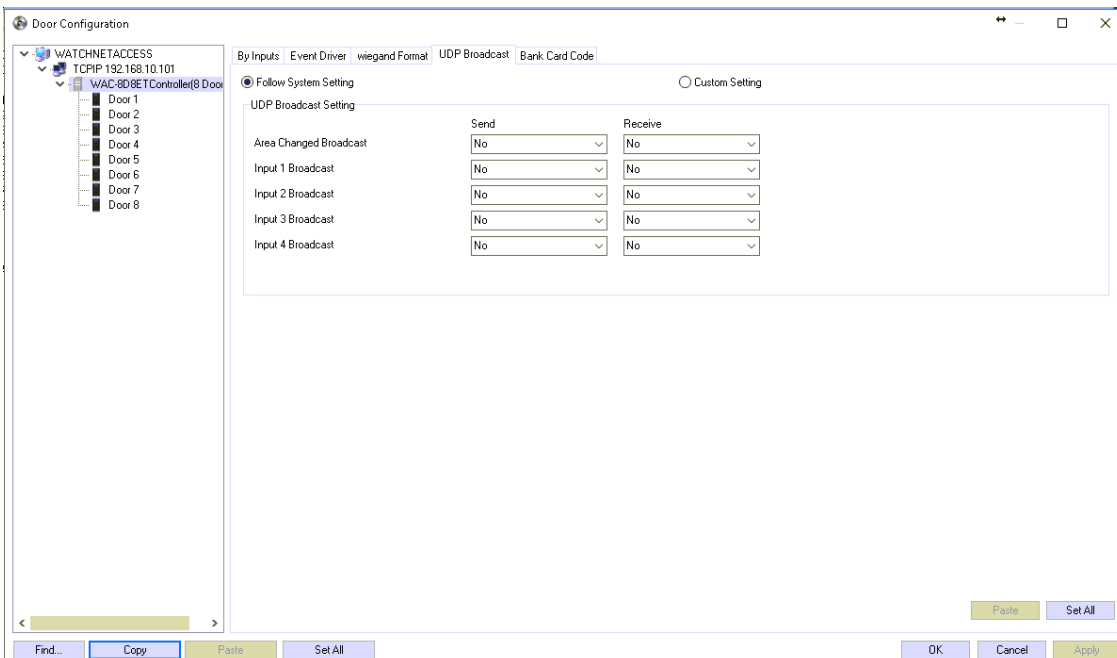
Wiegand Format - Wiegand format allows you to modify the bit format of reading from a single control or let it

follow the system settings.

Note: Do not change settings unless needed.



UDP Broadcast - Broadcast settings are configuration for global flow control that does not require the server to be running to execute.



Bank Card Code – Settings for bank code feature.

Click any door to show this menu

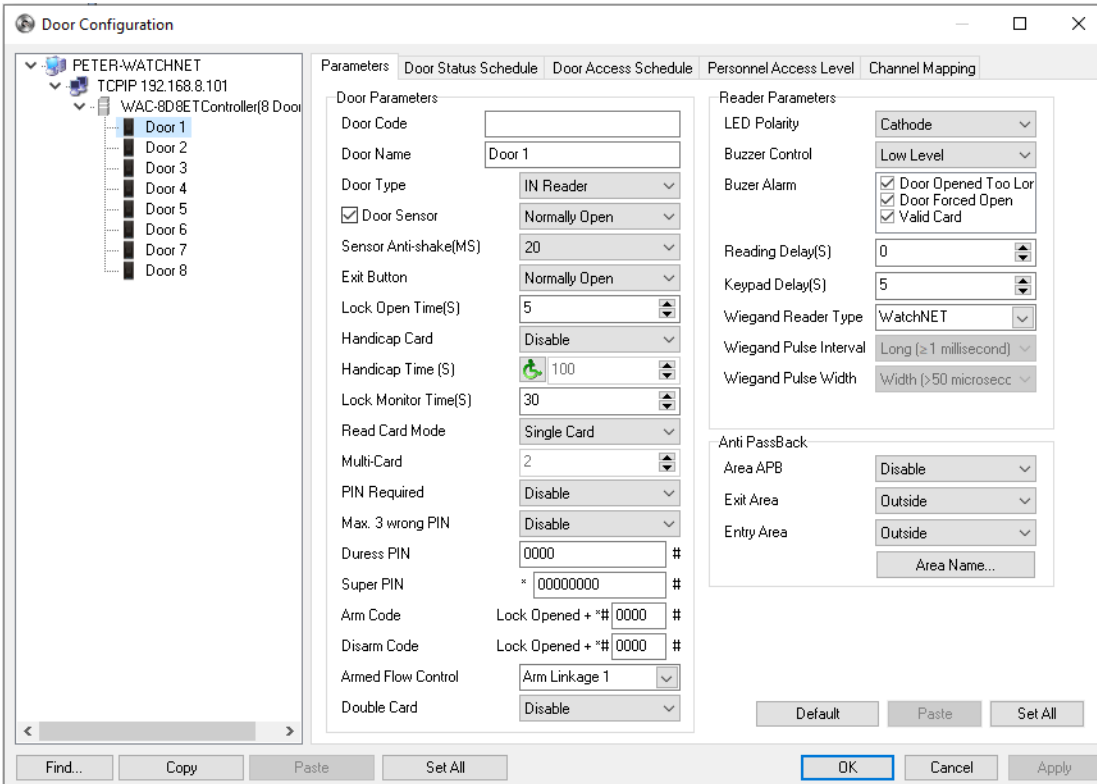
Parameters - This is where any general function related to a specific door is configured. To start configuring a

door, first highlight the door from the list of panels and doors on the left-hand side. Once the specific door has been highlighted then the items for that door can be configured.

This includes:

- **Door Parameters**

Door Code	Door code names
Door Name:	E.g. Front Door
Door Type:	An IN reader only or an IN/OUT reader. (This field will be available depending on the panel type)
Door Sensor:	Normally Open or Normally Closed (Can also be disabled if not in used)
Sensor Anti-Shake (MS):	Allows you to modify the sensor's time when to beep when event happen
Exit button:	Normally Open or Normally Closed
Lock Open Time(S):	The relay unlocks time which is normally 5 seconds.
Handicap Card:	Enable or Disable, when enabled door will be open for a long period of time when handicap card is swiped
Handicap Time(S):	door will stay open when handicap card is scanned depending on time setup
Lock Monitor Time(S):	The time before an alarm which is normally 30 seconds. The <i>Lock Monitor Time</i> is used to make sure that the door was not left propped opened for a long period of time.
Read Card Mode:	can choose from two options: Single card or multiple cards which is needed for opening the door.
Multi Card:	the number of valid cards that need to be flashed before the door can be opened.
PIN Required:	If enabled, card and pin have to be presented on the keypad reader to open door
Max. 3 wrong PIN:	If enabled and an incorrect PIN is entered 3 times then the software will delete the access level of the card.
Duress PIN:	A fixed 4-digit PIN to be used when under duress.
Super PIN:	When enabled the door can be opened with a PIN only by entering *12345678# where 12345678 is the Super PIN.
Armed Code:	A code that arms or activates a link on a keypad reader.
Disarmed Code:	A code for disarming/deactivating a link on the keypad reader.
Armed Flow Control:	Activates the programmed links.
Double Card:	Enable/Disable Double Swiped for Boss/Master Card



Reader Parameters - are also setup from within the Parameters window as follows:

- LED Polarity:** Changes standby mode color from blue or green.
- Buzzer Control:** To test the buzzer of a reader
- Buzzer Alarm:** To enable or disable event alarms
- Reading Delay:** The shortest time interval between reading 2 different cards.
- Keypad Delay:** The shortest time interval between 2 digits being entered at a keypad.
- Wiegand Reader Type:** can change from WatchNET reader, HID IClass or short interval readers
- Wiegand Pulse Interval:** manage the pulse interval of sending data from reader to controller
- Wiegand Pulse Width:** manage the pulse width on how long the reader sent the data to the controller
- As a card issuer** : To set the reader as a card enroller from the personnel list

Anti-Pass Back

- Area APB:** Select *Enable* for Area Anti Pass back.
- Exit Area:** Exit Area for Anti Pass back.
- Entry Area:** Entry Area for Anti Pass back.
- Area Name:** Select this button to give an area an alpha numeric name.

The door parameters can be copied from one door to another providing the doors are of the same type (IN door to an IN door). Highlight the door that you want to copy and click on the *Copy* button and highlight the door that you want to paste the parameters to and then click *Paste*. YOU will notice that there are two *Set All* buttons on the

window. The one on the right-hand side of the window is used to set all the doors (Door 1) of the same type of controllers on the network to the same settings. The *Set All* button on the left side will copy the settings of all the tabs to all the doors (Door 1) of the same type of controllers. If you have copied the settings of door 1 then all door 1s will be set. The same has to be repeated for door 2 and so on from the first controller.

Door Status Schedule

This is where the schedules for a specific door are configured. There are 15 available time tables per door. Double click on a *Time Table* or click on the *Edit Status* button to launch the *Door Status Time Set* window. On this window the actual status for the doors can be configured. Enter the *Start Time* and then click on the arrow next to the *Entry Status* label to select a status.

Options are:

- Open from 1st Card:** Door opens as per the schedule depending on first valid card. If the first valid card is before the scheduled door open time then door closes after access granted. If no valid card is presented on the door when it is set to open from 1st card then the door stays closed. When a first valid card is presented then the door opens and stays open as per schedule.
- Normal:** Door is always close and only opens when valid card is presented
- Sleep:** The system is effectively asleep and will not read a valid card.
- Always Open:** The door is always open (unlocked).
- Always Closed:** The door is always closed (locked) and can only be unlocked with a *Master Card*.
- Card + PIN:** Card and PIN required.
- APB:** Anti Pass back.
- Open/Closed:** Door status changes on valid card. First valid card will open door and it stays open until next valid card is presented to close
- Twin Card Mode:** Twin Cards have to be swiped both to open door
- Group Card Mode (GCM):** group card has to be presented to open door

Door Status Time Set
✕

Status Time

Start Time H M

Entry Status Confirmed by Centre

Card Count Group 1# Group 2# Group 3# Group 4# Backup PIN During Offline

+ + + * #

Valid Date Set

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

H1 H2 H3 H4 H5 H6 H7

T1 T2

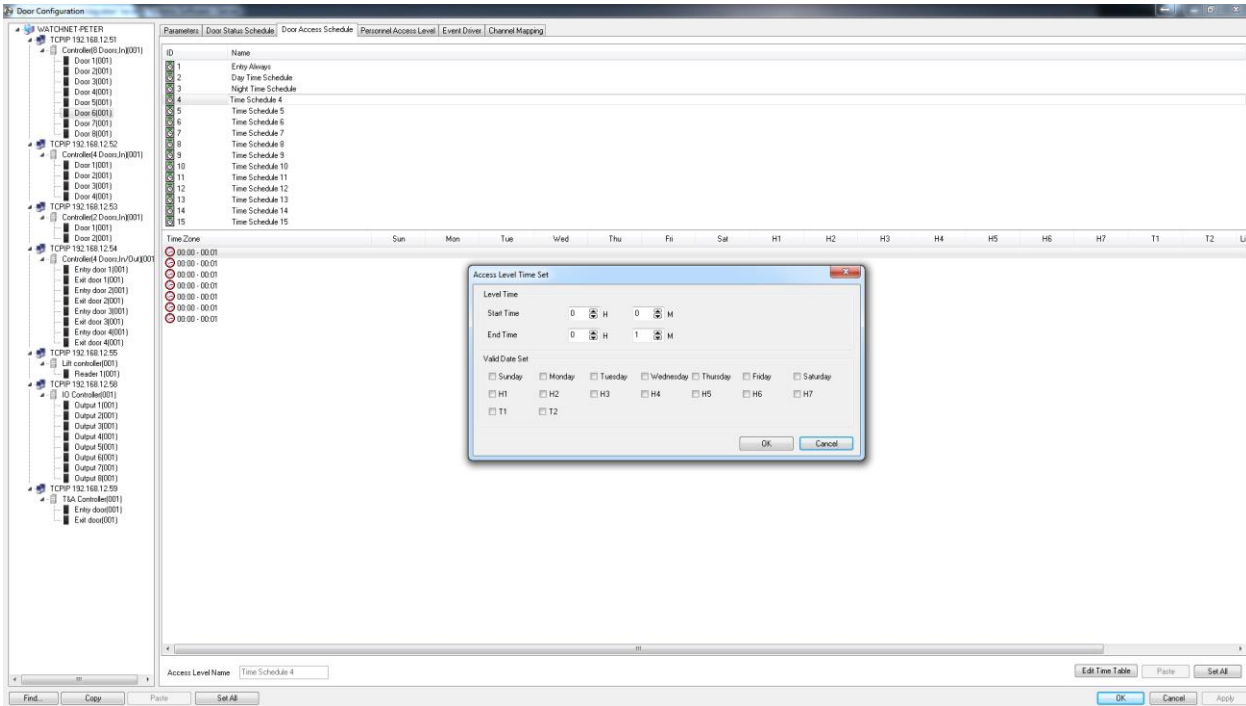
To configure the *Door Status Schedule*, check the days of the week to apply the chosen status for. The *H1-H7* boxes refer to the seven types of holidays that can be configured and the *T1-T2* boxes refer to the two types of temporary dates that can be configured.

Note: GCM Mode is only available in Ver. 03 controllers

Door Access Schedule

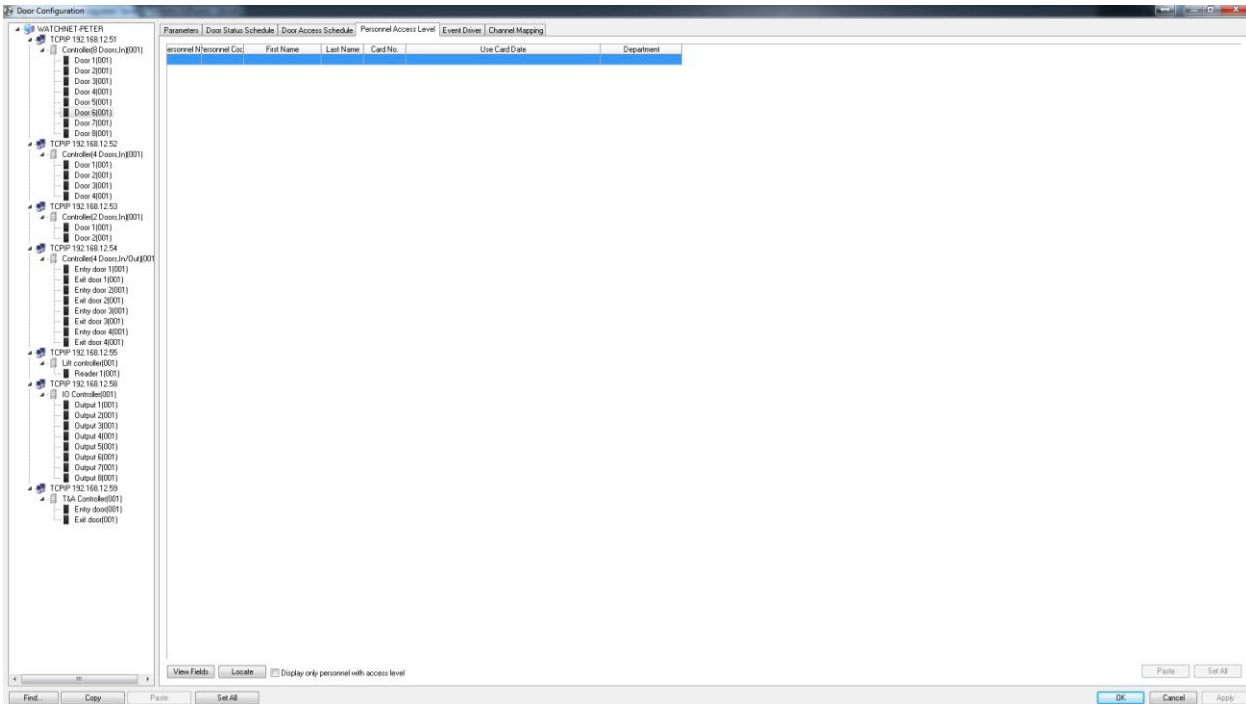
The *Door Access Time Table* sets the Time Tables for Door Access and is configured similarly to the *Door Status Time Table*. At the *Door Access Time Table* we also specify the *End Time*.

Each door can have up to 15 different Time Schedules while each Time Schedule can have up to 7 different Time Zones. In the Time Zone section is where the days and time period for the door access are configured. Different Time Zones can have different days and hours.



Personnel Access Level

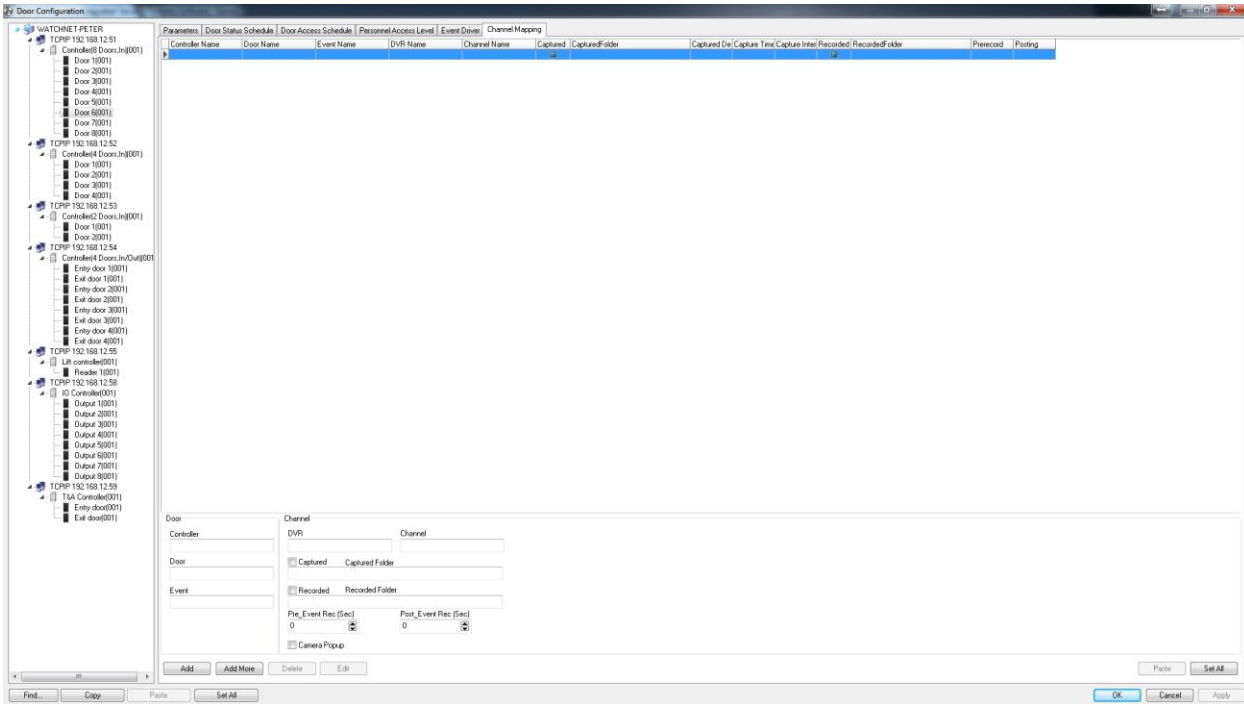
Display the Personnel who have access to certain door.



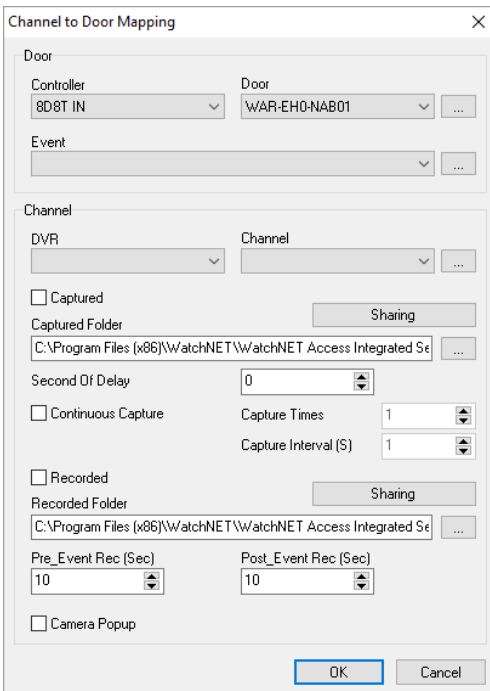
For Example, when Access is granted on Door 1 the controller can turn on Auxiliary Output 1 for a specified amount of time.

Channel Mapping

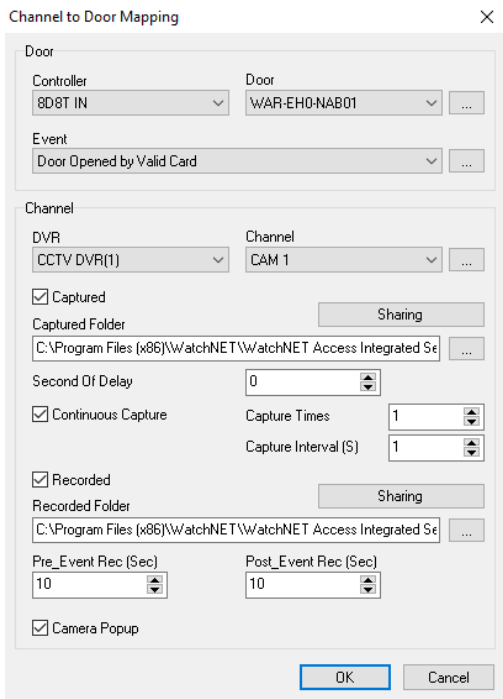
Allows for the integration with DVR's which allows for the taking of snapshots and the recording of live video when an event occurs.



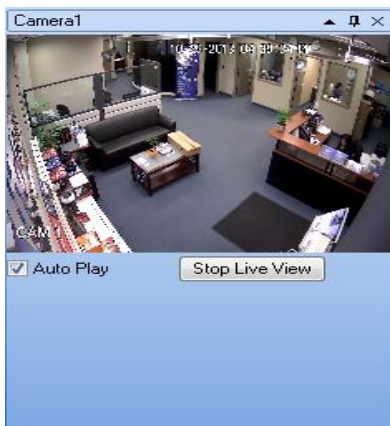
To start configuring *Channel Mapping* click on the *Channel Mapping* tab and click the *Add* button.



Select the *Controller, Door and Event* from the *Door* section. Then select the *DVR and Channel* from the *Channel* section. The final step is to check on the *Captured, Recorded and Camera Popup*.



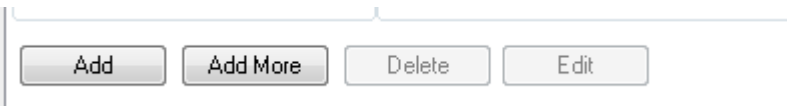
With this configuration when Door 1(002) is forced open then Camera 1 of the Demo DVR will take a snap shot and also record a Pre and Post event recording for 10 seconds. Also the Camera will pop up on the Video window of the screen.



Note: In order for the pop ups to be displayed the Auto Switchover and the Auto Play check boxes have to be checked, and to see the Popup right click on card events and select "Personal Photo Viewer"



If you click the *Add more* button from the *Channel Mapping* tab you can add more events as the event source.



Any event will trigger the action.

Channel to Door Mapping

Door
Controller: 8D8T IN Door: WAR-EH0-NAB01

Event
 Armed
 Aux Input Closed
 Aux Input Opened
 Aux Output Closed
 Aux Output Opened
 Disarmed
 Door Closed by Force
 Door Closed Normally
 Door Forced Open
 Door Opened by Boss/Master Card
 Door Opened by Card + PIN
 Door Opened by Duress PIN
 Door Opened by First Card
 Door Opened by Handicap Card
 Door Opened by PIN
 Door Opened by Super PIN
 Door Opened by Valid Card
 Door Opened by Valid Card + Fingerprint
 Door Opened by Valid Fingerprint
 Door Opened by Valid PIN + Fingerprint
 Door Opened Normally
 Door Opened Too Long
 Error PIN For Temporary Card
 Exit Button Action
 Exit Button Release
 Expired Card
 Hardware Trouble
 Invalid Area
 Invalid Area For Boss/Master Card
 Invalid Area For Temporary Card
 Invalid Card
 Invalid Confirmed PIN
 Invalid Door/Time
 Invalid Fingerprint

Channel
DVR: Channel: Sharing

Captured
 Captured Folder: C:\Program Files (x86)\WatchNET\WatchNET Access Integrated Security Systems\Snapshots
 Second Of Delay: 0
 Capture Times: 1
 Continuous Capture
 Capture Interval (S): 1

Recorded
 Recorded Folder: C:\Program Files (x86)\WatchNET\WatchNET Access Integrated Security Systems\recording
 Pre_Event Rec (Sec): 10
 Post_Event Rec (Sec): 10

Camera Popup

OK Cancel

Delete the channel mapping by clicking the *Delete* button and then *OK*.

WatchnetAccess

Are you sure you would like to delete the selected Door Mapping Condition?

OK Cancel

To edit the mapping select the corresponding record and then click the *Edit* button.

Door
Controller: Lift controller(001)
Door: Lift controller(001)
Event: Valid Card

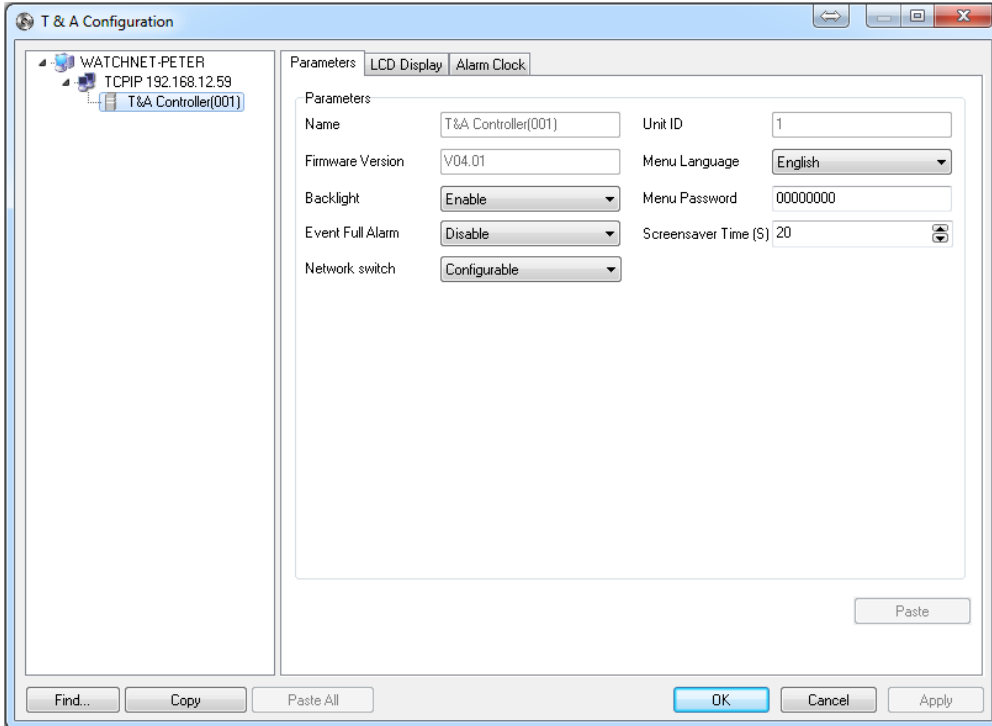
Channel
DVR: CCTV DVR(8) Channel: IPC
 Captured Captured Folder: C:\Program Files (x86)\WatchNET\WatchNET Access Integrated Se
 Recorded Recorded Folder: C:\Program Files (x86)\WatchNET\WatchNET Access Integrated Se
 Second Of Prerecording: 10 Second Of Posting: 10
 Camera Popup

Add Add More Delete Edit Paste Set All

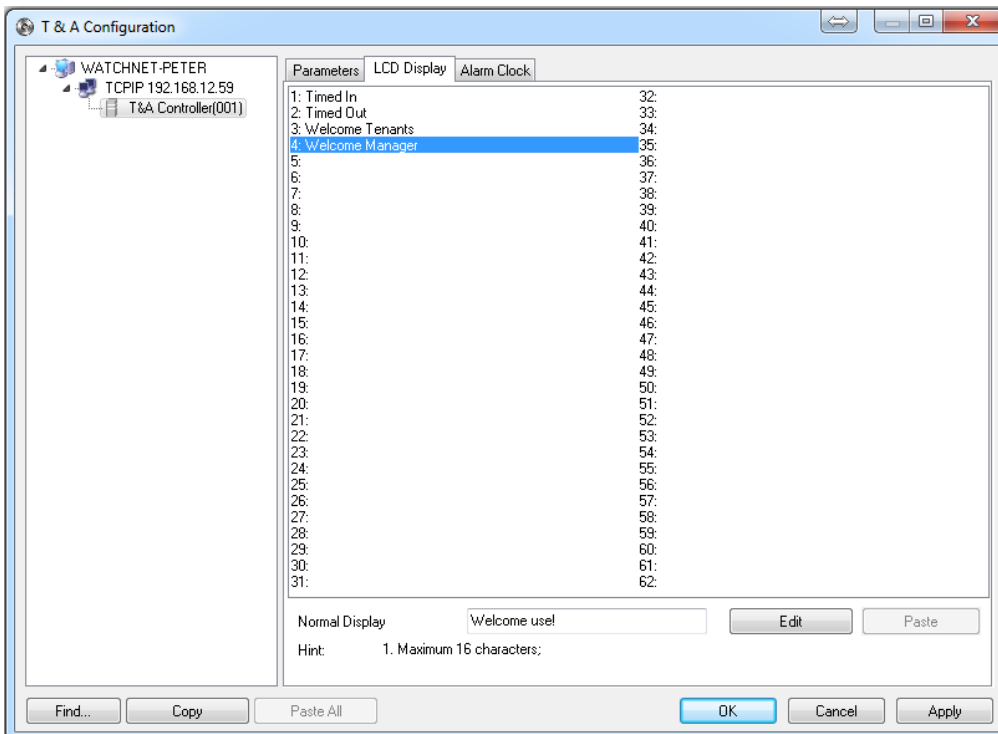
4.1.5 T & A – this can configure parameters, LCD display, Alarm clock settings.

Note: this feature can only be used in WAC-1D2T-Micro.

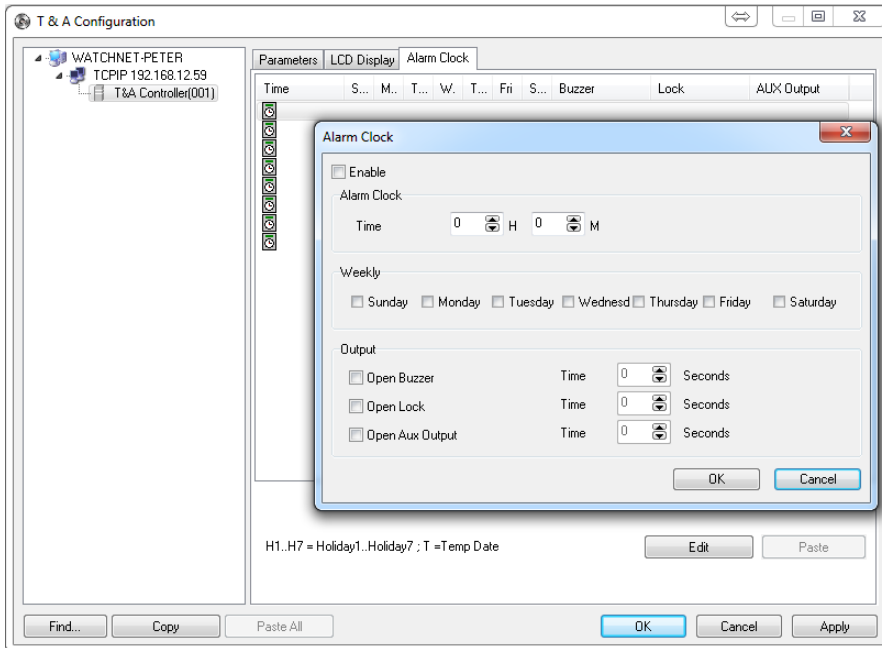
- **Parameters** - Can modify below configuration



- **LCD Display** - Can modify Display message on LCD display of the 1D2T Micro

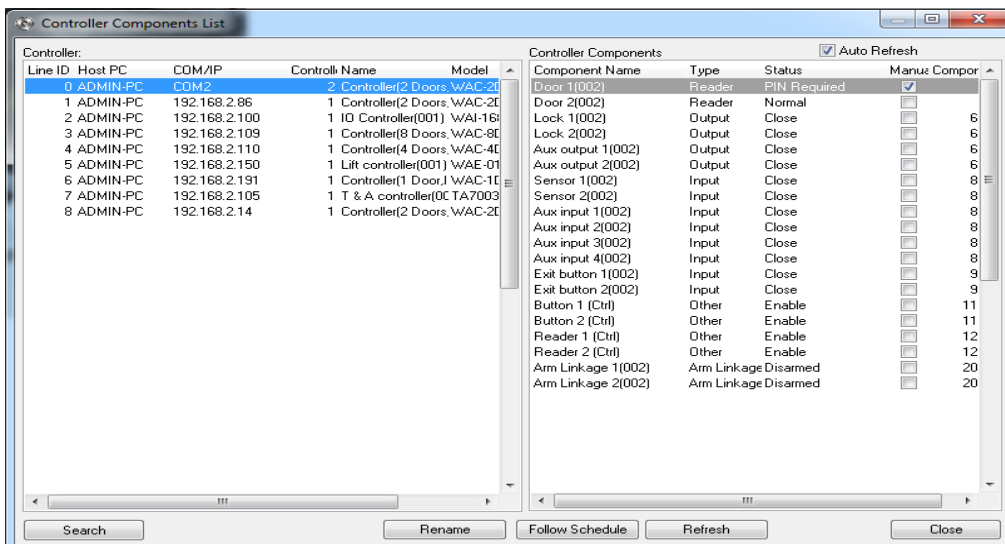


Alarm Clock - Setup alarm or buzzer for a specific period of time using auxiliary output



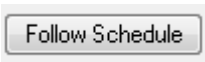
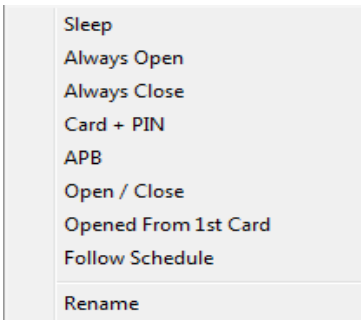
4.1.6 Standalone Controller Configuration – Currently not supported.

4.1.7 Controller Components - To configure the Control Components select *Setup -> Hardware* menu and then *Controller Configuration*. This will open the *Controller Components List*. **Controller Component consists of (Doors, Locks, Door Sensors, Exit buttons, Aux Inputs, Aux Outputs, and Readers).** These components can be renamed by highlighting the Component and by right clicking and then selecting *Rename* or alternatively clicking on the *Rename* button



Other functions are available depending upon the type of Components. For example highlighting on a door and then right clicking will launch a menu that allows the user to force open the door manually. Right clicking on a Door sensor

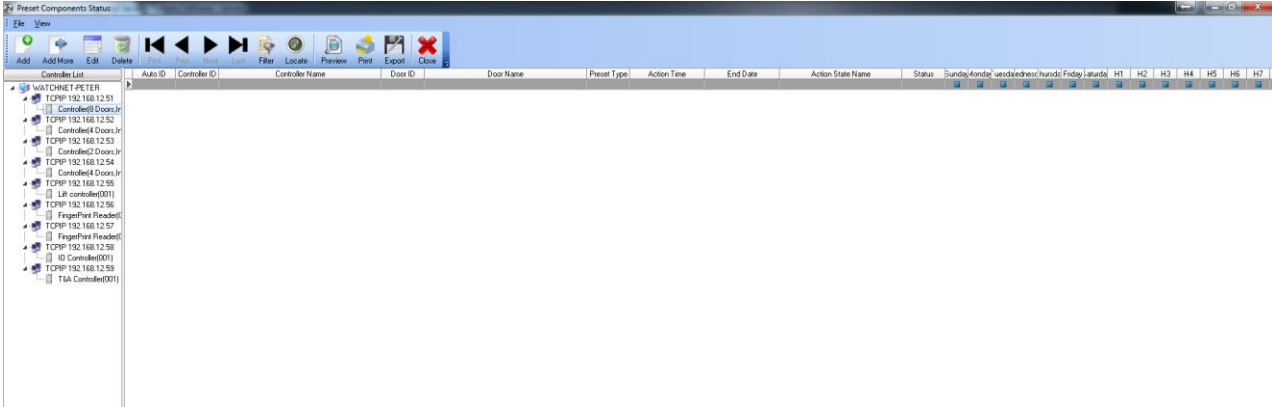
allows the door status to be changed.



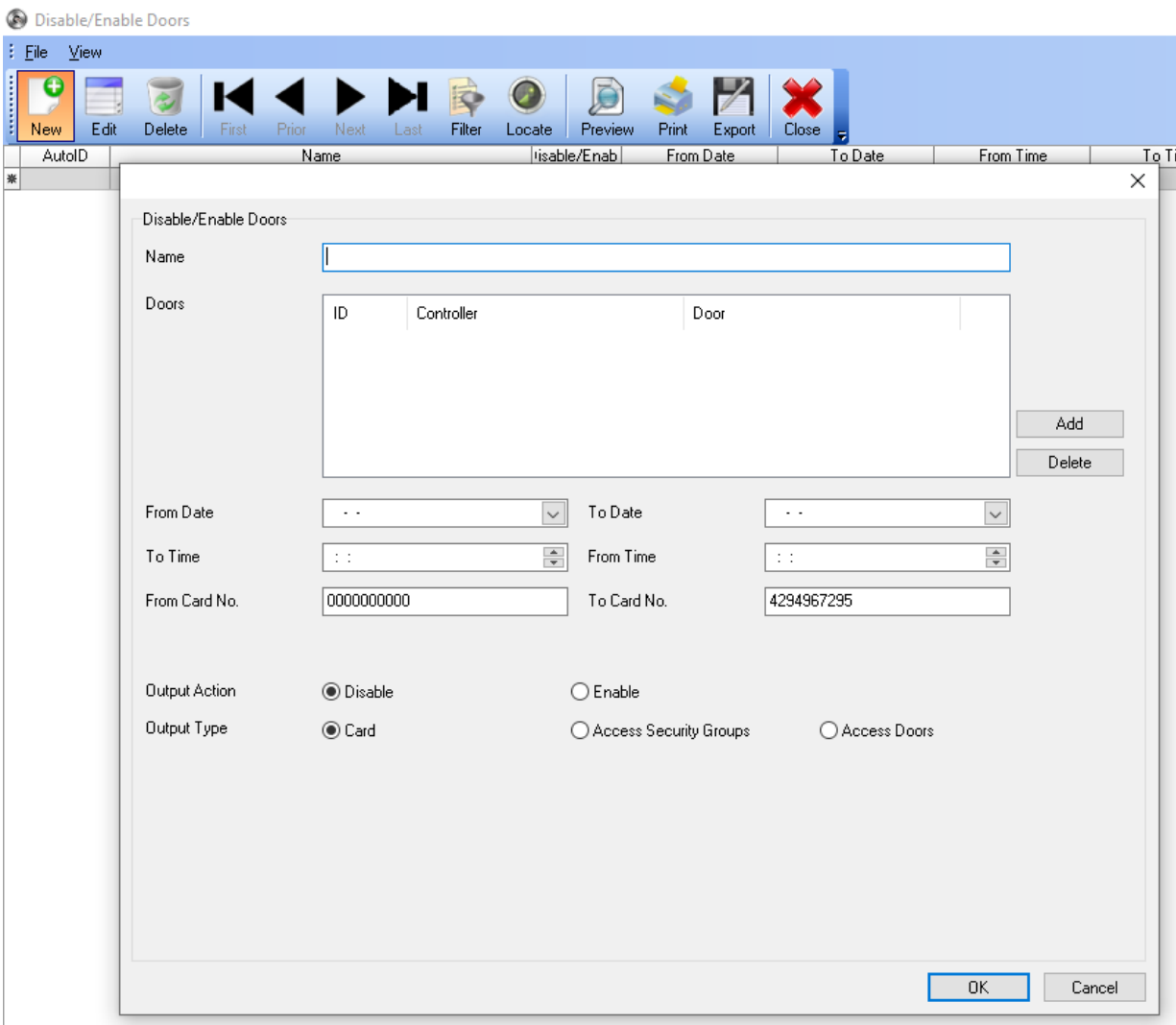
The *Follow Schedule* button downloads the schedules from the WAC software on the Server to the panels. For example, if the schedules were set with a Server that has been replaced and the schedules have been updated on the new Server then clicking on the *Follow Schedule* will download the new schedules to the panels.

4.1.8 Preset Components Status - Pre-set configuration allows the user to set a temporary components

schedule

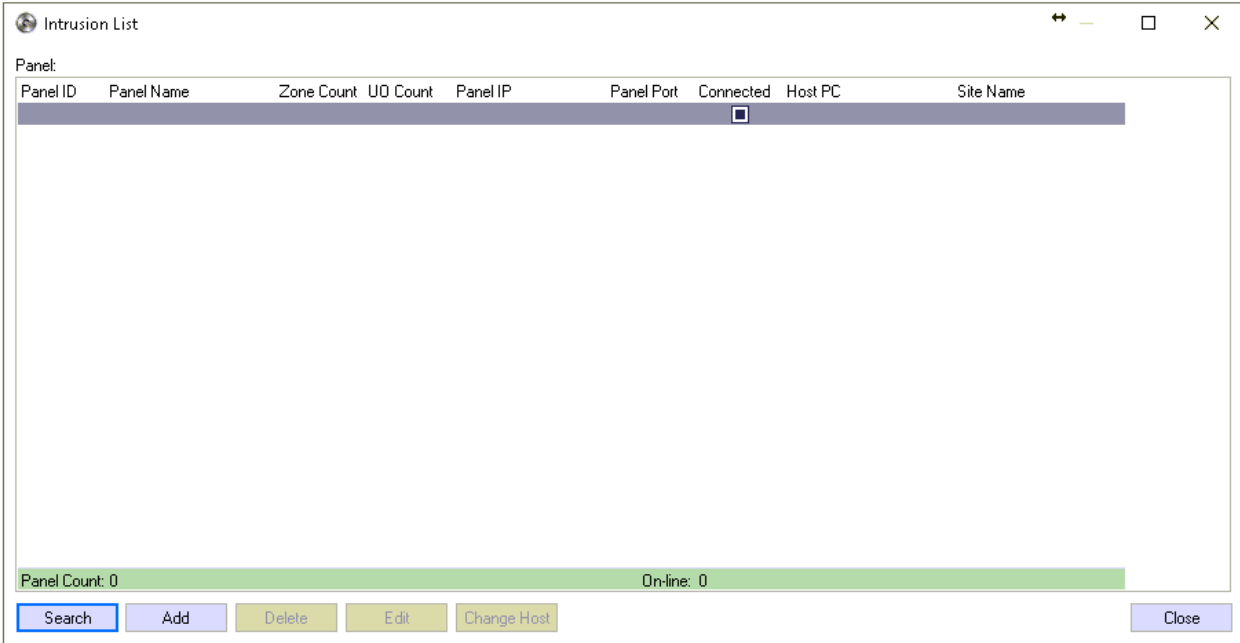


4.1.9 Disable/Enable Doors – Enable/disable the door on certain date or time.

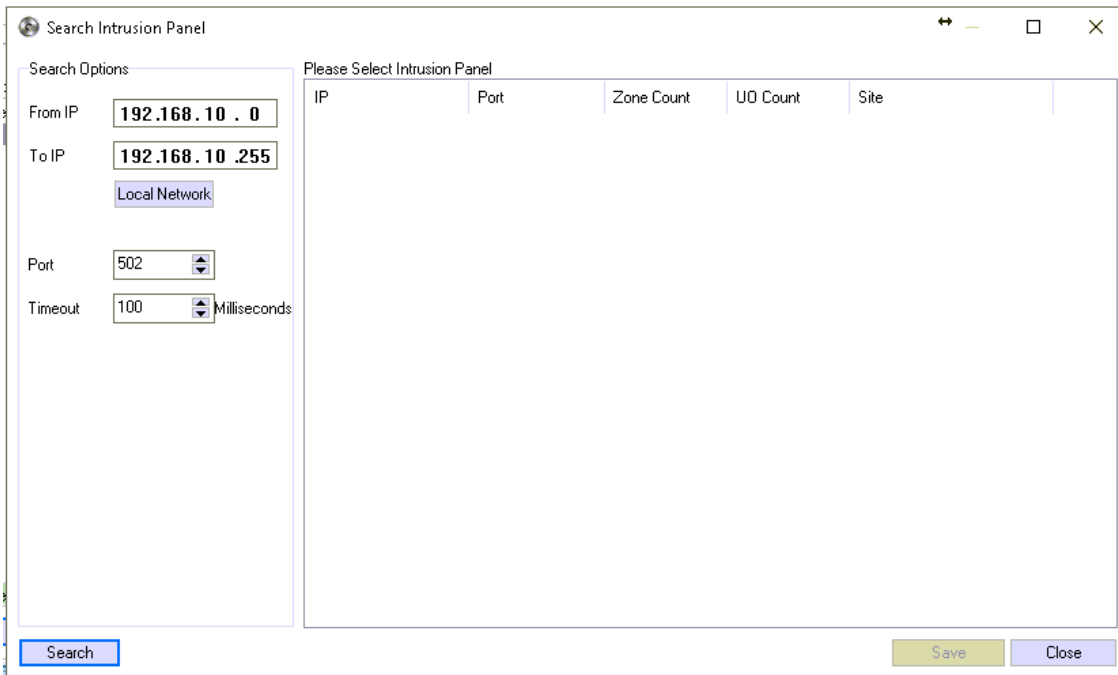


4.1.10 Prosys Intrusion

- **Panel Configuration - Click search or add to add a prosys panel.**



- **Search Panel - Click search to find a prosys panel on the network**



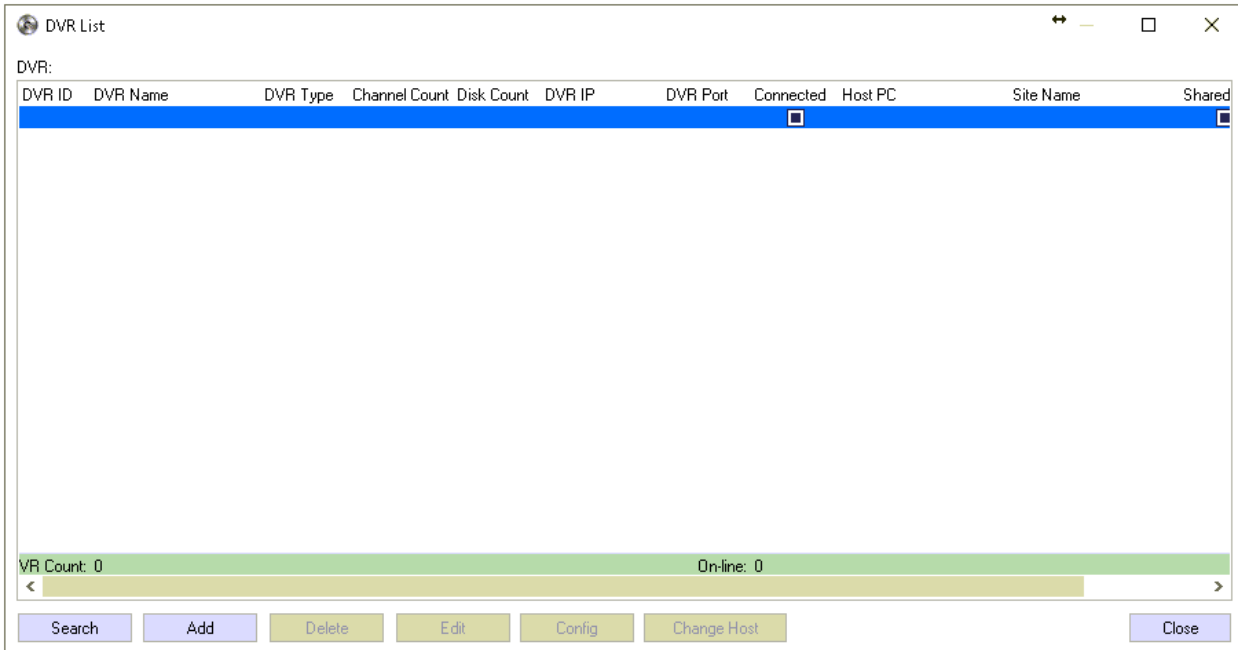
- **Panel Components - To configure the prosys components.**

4.1.11 Prosys Plus Intrusion – Adding and searching is the same process from prosys intrusion

4.1.12 DSC Intrusion – Adding and searching is the same process from prosys intrusion

4.1.13 PIMA Intrusion – Adding and searching is the same process from prosys intrusions

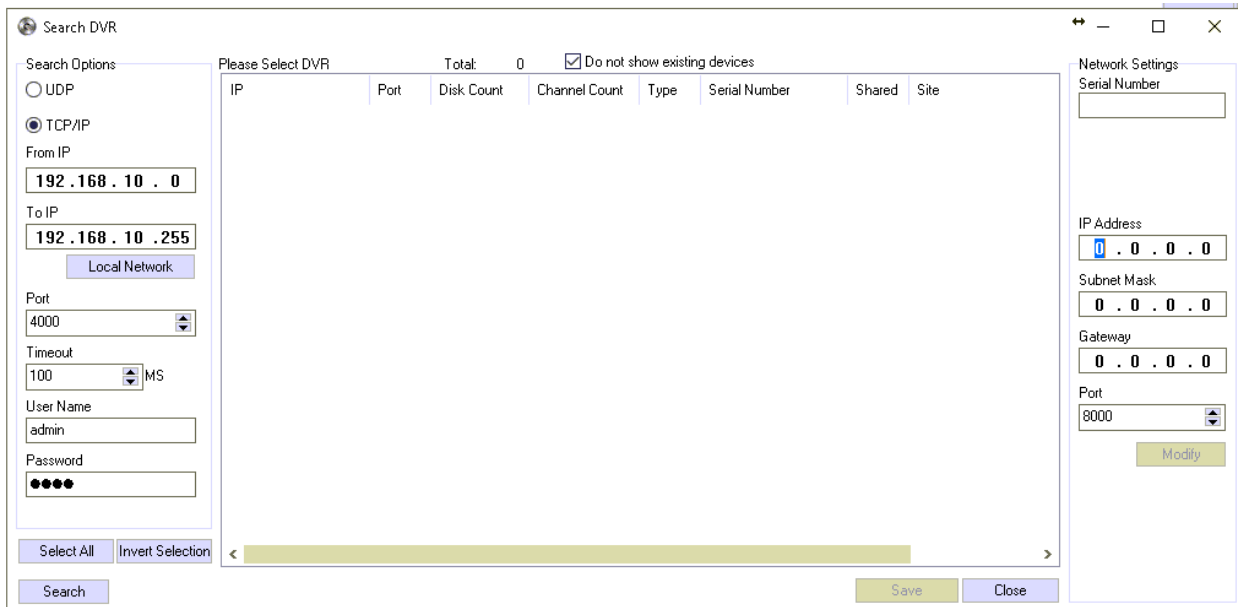
4.1.14 DVR Configuration - to start to search for DVR's select *Setup -> Hardware -> DVR Configuration.*



Click on the *Search* button to launch the *Search DVR* window.

Search

To search for DVR's click on *Local Network* to set the IP range.



Once the IP range is set click on the *Search* button to start the search.

Search DVR

Search Options
 UDP
 TCP/IP

From IP:
 To IP:

Port:
 Timeout: MS
 User Name:
 Password:

Please Select DVR Total: 2 Do not show existing devices

IP	Port	Disk Count	Channel Count	Type	Serial Number	Shared	Site
<input type="checkbox"/> 192.168.10.31	4000	1	8	31	1D0338BPALZZGG8	<input type="checkbox"/>	WatchnetAccess Group
<input type="checkbox"/> 192.168.10.73	4000	1	8	27	PA1HQ01100209	<input type="checkbox"/>	WatchnetAccess Group

Network Settings
 Serial Number:
 IP Address:
 Subnet Mask:
 Gateway:
 Port:

Check the DVR's that you want to add and then click the *Save* button to add the selected DVR's.

Search DVR

Search Options
 UDP
 TCP/IP

From IP:
 To IP:

Port:
 Timeout: MS
 User Name:
 Password:

Please Select DVR Total: 3 Do not show existing devices

IP	Port	Disk Count	Channel Count	Type	Serial Number	Shared	Site
<input checked="" type="checkbox"/> 192.168.10.31	4000	1	8	31	1D0338BPALZZGG8	<input type="checkbox"/>	WatchnetAccess Group
<input checked="" type="checkbox"/> 192.168.10.73	4000	1	8	27	PA1HQ01100209	<input type="checkbox"/>	WatchnetAccess Group
<input type="checkbox"/> 192.168.10.162	4000	1	8	31	PA3MF126D00278	<input type="checkbox"/>	WatchnetAccess Group

Network Settings
 Serial Number:
 IP Address:
 Subnet Mask:
 Gateway:
 Port:

Adding DVR's manually

Click the Add button to launch the *ADD CCTV DVR* window.

Add CCTV DVR

DVR

DVR ID: 1

DVR Name:

Site: WatchnetAccess Group

DVR IP: 0 . 0 . 0 . 0

DVR Port: 4000

User Name: admin

PassWord: ●●●●

Share DVR: Other client can watch cameras

Snap/Capture Picture

Snap shot with supported models of devices

Snap shot with connected devices in video display

OK Cancel

Enter the DVR information and then click the *OK* button to add the DVR.

Delete

Click the *Delete* button to delete the selected DVR.

DVR List

DVR ID	DVR Name	DVR Type	Channel Count	Disk Count	DVR IP	DVR Port	Connected	Host PC	Site Name	Shared
1	CCTV DVR(1)		8	1	192.168.10.31	4000	<input checked="" type="checkbox"/>	WATCHNETACCESS	WatchnetAccess Group	<input type="checkbox"/>

VR Count: 1 On-line: 1

Search Add **Delete** Edit Config Change Host Close

WatchNET Access 1.0 (NoCardList)

Are you sure you want to delete the selected CCTV DVR?
CCTV DVR(1)

OK Cancel

Click *OK* to delete selected DVR.

Edit

Click the *Edit* button the edit the selected DVR.

Edit CCTV DVR

DVR:

DVR ID: 1

DVR Name: CCTV DVR(1)

DVR IP: 192 . 168 . 1 . 241

DVR Port: 8000

User Name: admin

PassWord: ●●●●

Share DVR: Other client can watch cameras

OK Cancel

Change Host

Click the *Change Host* button to change the DVR host.

4.1.15 Search DVR - Refer to Search.

4.1.16 DVR Channel - The *DVR Channels List* displays the entire channel mapping information. Click Setup->Hardware->DVR Channels.

DVR Channels List

DVR:					Channels:			
Line ID	Host PC	DVR ID	DVR Name	DVR IP	Visible	Channel Name	Num	Motion Detection Capture
0	WATCHNETAC	1	ENMR2(1)	192.168.10.49	<input checked="" type="checkbox"/>	Camera1	0	<input type="checkbox"/>
					<input checked="" type="checkbox"/>	Camera2	1	<input type="checkbox"/>
					<input checked="" type="checkbox"/>	Camera3	2	<input type="checkbox"/>
					<input checked="" type="checkbox"/>	Camera4	3	<input type="checkbox"/>

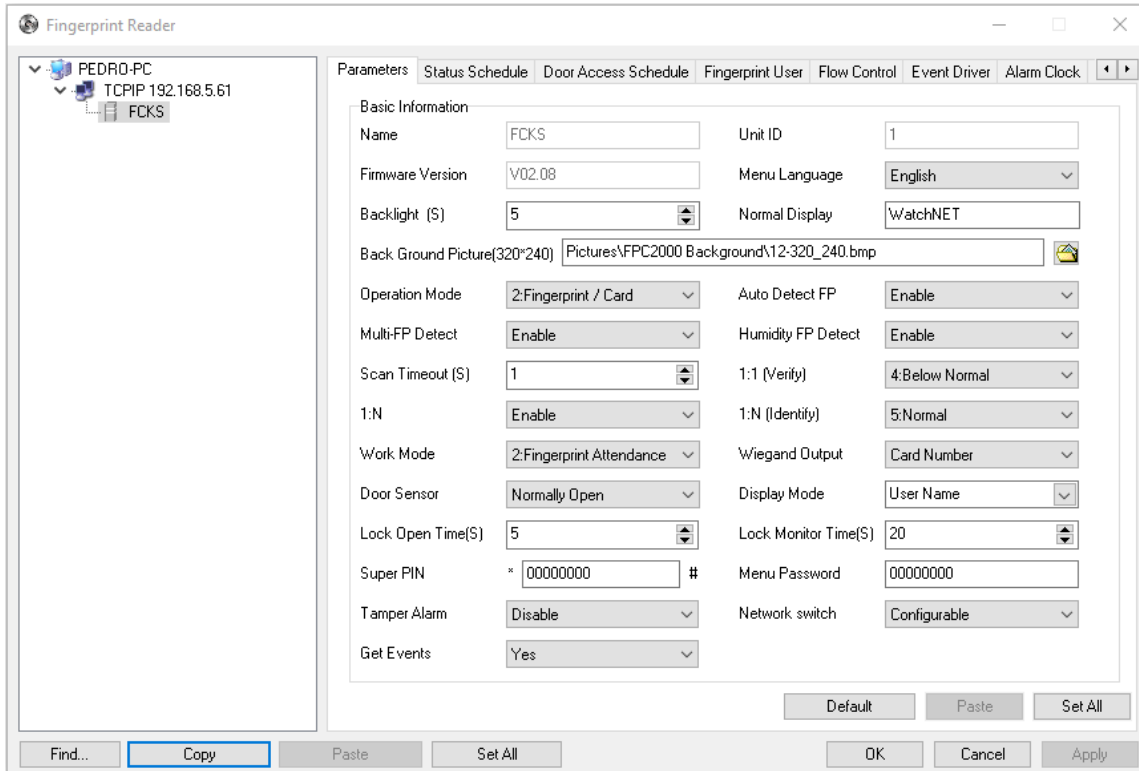
Read Channel Info from DVR next time

Refresh Close

4.1.17 Channel to Doors/Zones Mapping – See sections Channel Mapping

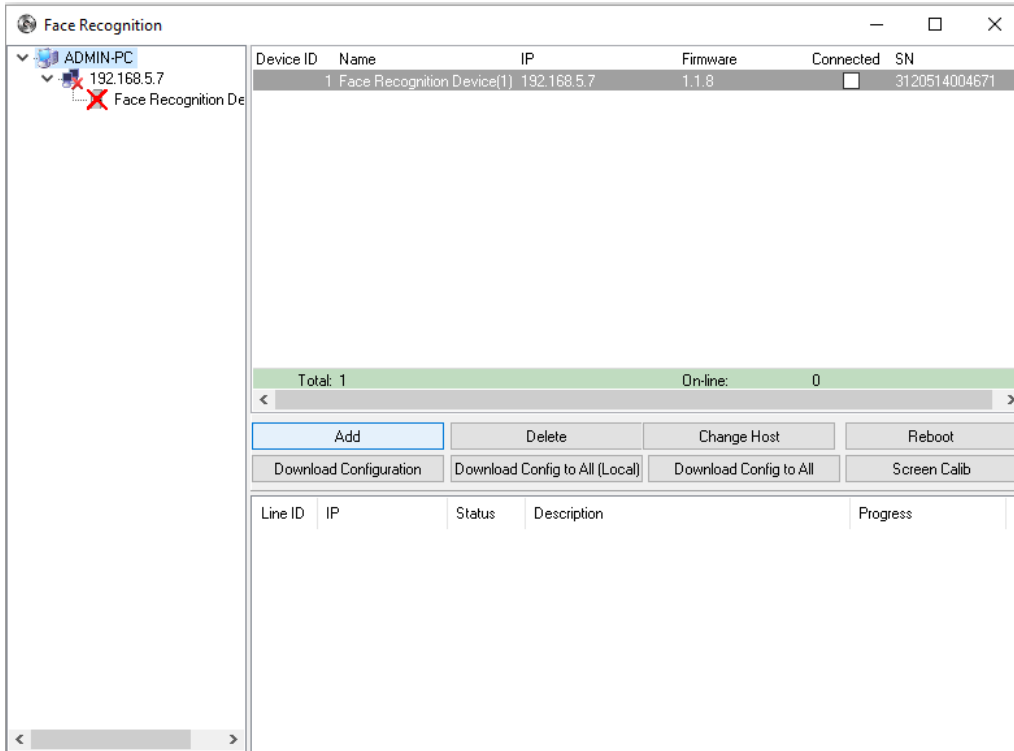
4.1.18 Fingerprint Reader - Click Setup->Hardware->Fingerprint Reader to open configuration.

Note: Before opening configuration make sure fingerprint parameters are set, sample below is showing WAB-P-FCKS configuration.



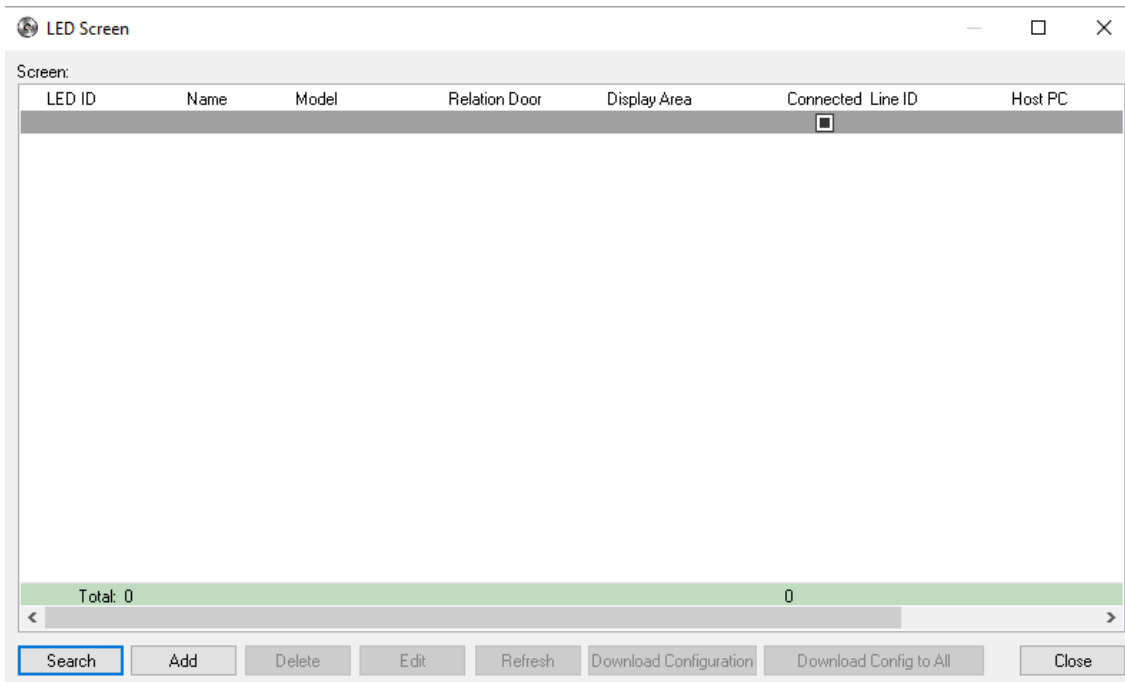
4.1.19 Face Recognition - Click Setup->Hardware then Face Recognition to add face recognition device.

Note: Before adding a face recognition device make sure the face device parameters are set



4.1.20 LED Screen - Click Setup->Hardware then LED Screen to add LED Screen, this option is used to set up an

external, serial or TCP/IP connected LED display screen. Click *Add* to add LED screen.

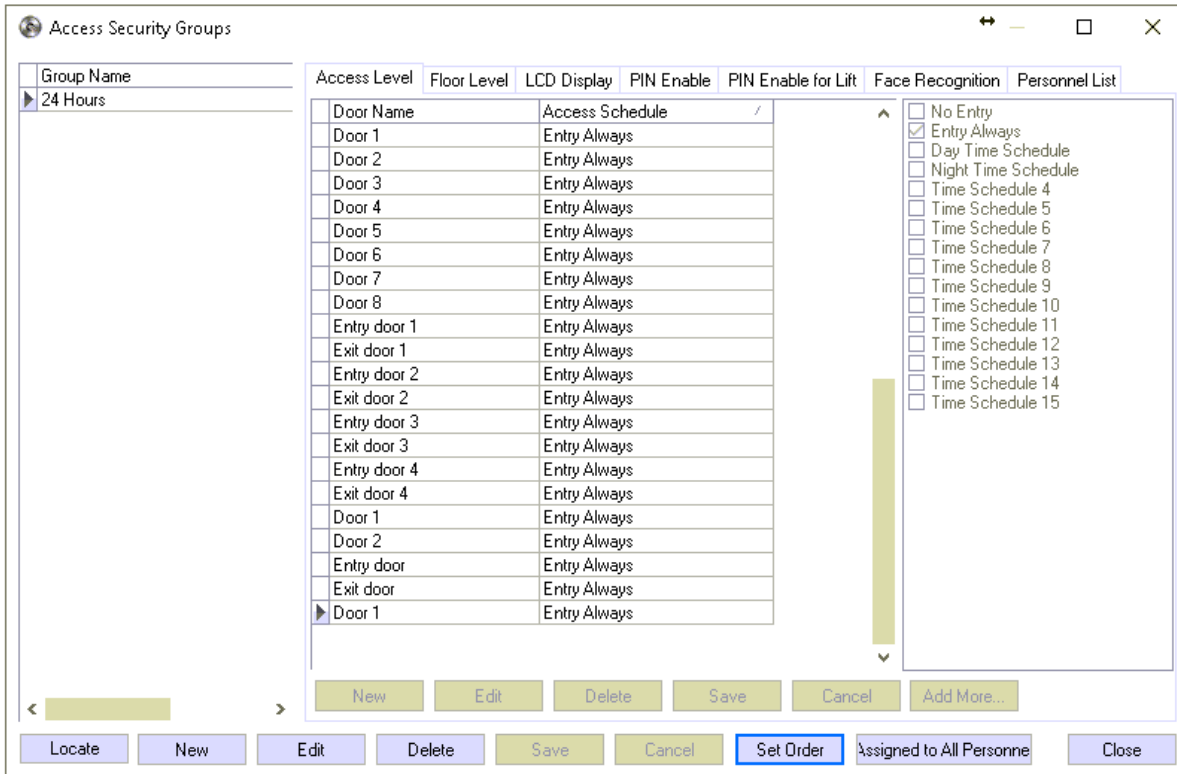


4.2 Cards

4.2.1 Access Security Groups

Access Security Groups is where you can create different group of access levels, either per departments or just per personnel


To start adding cards click on *Setup -> Cards -> Access Security Groups*

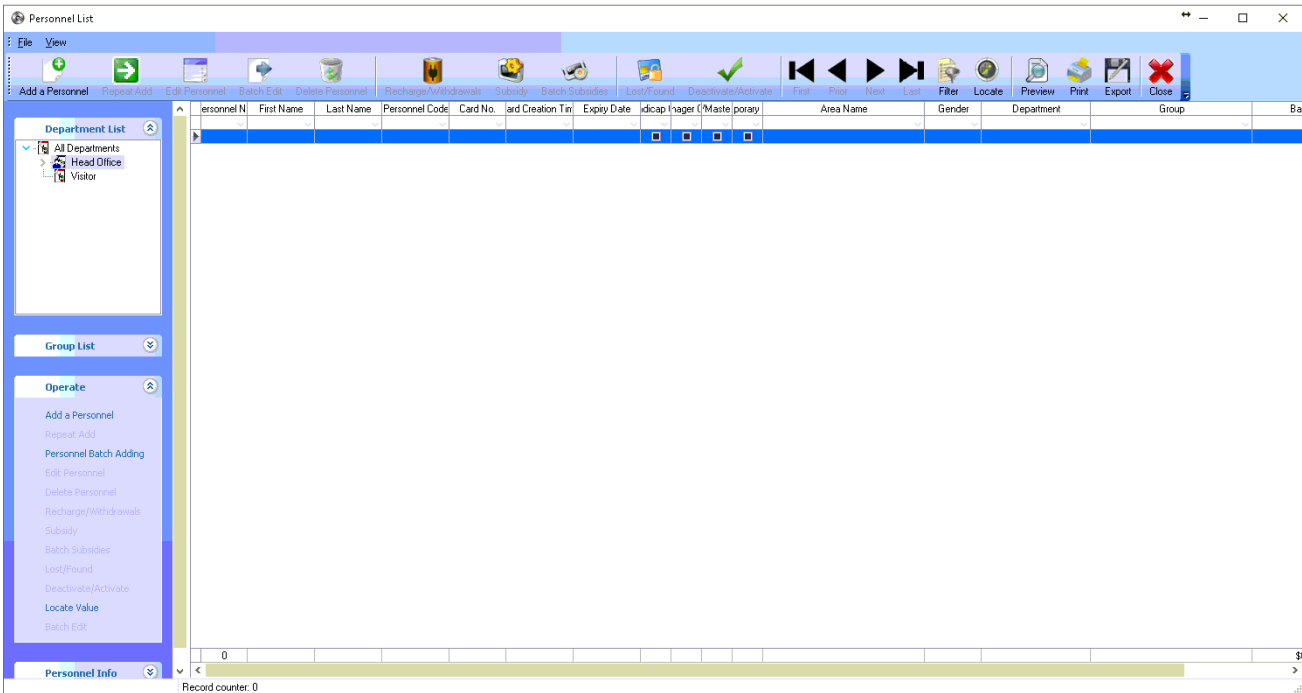


By default, a 24 Hours access group is configured on the system

Note: A group must be created depending on the access level of the department of the personnel.

4.2.2 Personnel List

The *Personnel List* is where the main user information is entered. Select *Personnel List*  from the main menu bar or choose *Personnel List* from the *Setup -> Card* sub-menu. All the individual Personnel information can be found in this window. Personnel can be added and modified or deleted. From the *Personnel List* window Personnel records can also be exported into Excel, Text, Html or MS-Word file.



Adding a Personnel




Click on the *Add a Personnel* button to launch the *Personnel Information* window. Enter the card user's information.

Basic Information – input first name last name and other information needed

Note: The first and the Department are mandatory fields and must be filled out in order to proceed to

the Card tab.

There are three options for obtaining a photo image.

1. The folder icon  adds a saved photo image from the C:\Program Files (x86)\WatchNET\WatchNET Access Integrated Security Systems\Photos path.
2. The camera icon  adds a photo image taken from a digital camera.
3. The scanner icon  adds a scanned photo image taken from a scanner.

Click on the *Card* tab to add card information. Check the *Use Access Card* option to activate the card.

4. Card – Card tab is used to setup card parameters of personnel

Personal Information

Basic Information

Card


Access Level

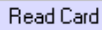
Fingerprint

Face Info

Use Access Card

Card Info

Card No.: 0001380934 

ID Card Custom ID: 0 From Reader BioUSB10 

Expiry Date 2019-06-01 Retrieve Card Number From Desktop Reader Retrieve Card Number From System

Deactivate 30 Days not used

Card Event Link to

Access Properties

Handicap Card Opens the Door for a longer time

Manager Card No Anti-Passback Limitation; Open/Sc

Boss/Master Card Can open any Door anytime; Open/Sc

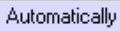
Temp Card

Temp Card Valid Time

From: . . . :

Expiration: . . . :


PIN

PIN ID 0001  PIN ●●●●

Current Area: Outside

Card Property for WAC:XDYE -----

Card Group None

Twin Card Select 

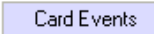





PIN Card * ●●●● # 4-8 digits

Balance

Times Card 0

Limited Times

Balance 0

*This option is used for CARD+PIN or PIN Only on keypad readers and valid only for V40.** and V45.***

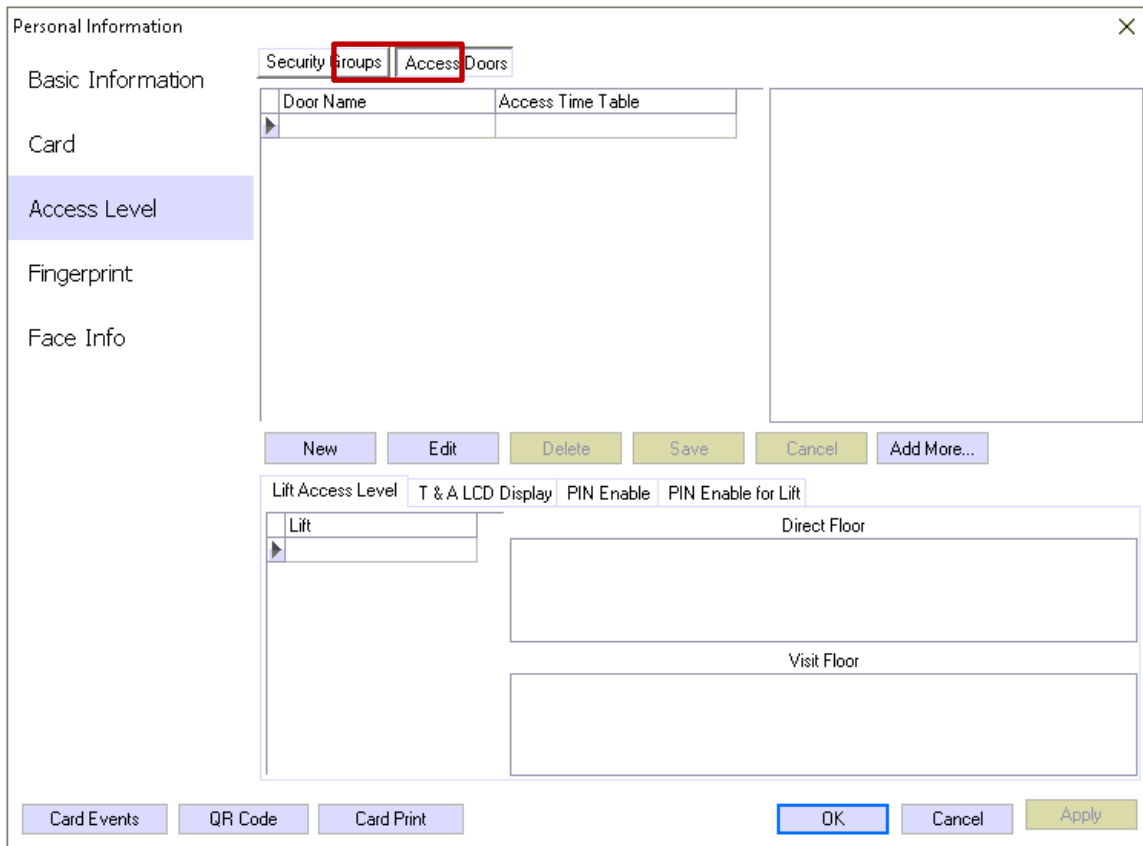
*Pin Only option is only valid for V.03.** Controllers Press*

- Use Access Card** - must be checked to activate card
- Card Info:**
- Card No.** - input card number (*sample is decimal format*)
- Vice Cards** - enable to add multiple card for the personnel
- ID card Custom ID** - additional ID number
- Expiry Date** - setup an expiry date for personnel or card
- Deactivate** - card will be automatically deactivated if not used on certain days selected
- Card Event Link to** - to link another personnel to this user
- Retrieve card number from Desktop Reader-** card number will automatically entered in *Card No.* when card is swiped in desktop reader
- Retrieve card number from System Reader-** card number will automatically entered in *Card No.* when card is swiped in the reader
- Access Properties:**
- Handicap Card- Manager Card:** door will be open for longer period of time when card is swiped
swipe card twice on a door to override door schedule to always open and swipe twice again to put back to schedule
- Boss/Master Card:** can open door anytime and have access to all doors
- Temp Card:** enable to assign the card as temporary card
- PIN:**
- Pin ID-** click *automatically* button to generate ID for pin
- PIN-** Input PIN number for personnel
- Card Property for WAC-XDYE:**
- Card Group:** select a group number for card to follow GCM(group card mode) status
- Twin Card Select:** card will be slave card and need to bind to any card when the Master-slave mode door status is enabled
- PIN Card:** pin only can be used on keypad reader when card is lost or forgotten (only work with V03.** Controller)

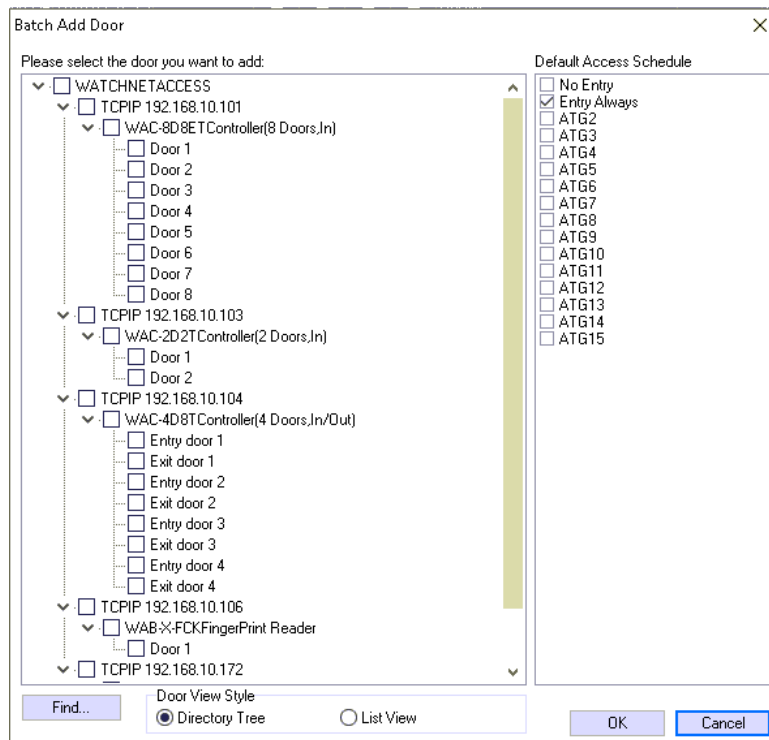
- **Access Level** – Access level tab is where you select the door access for the card holder, there are two different ways of assigning access level: **Security Groups/ Access Doors**
 - **Security Groups** – To create access security group you can go to **4.2.1**, once create you can select that access to the card holder

The screenshot shows a software window titled "Personal Information" with a close button (X) in the top right corner. The window has a left-hand navigation pane with the following items: "Basic Information", "Card", "Access Level" (highlighted in blue and enclosed in a red box), "Fingerprint", and "Face Info". At the top of the main content area, there are two tabs: "Security Groups" (highlighted in blue and enclosed in a red box) and "Access Doors". Below the tabs, there are two tables. The first table has columns "No." and "Access Security Group" and contains one row with a checkbox and the value "0" under "No.", and "24 Hours" under "Access Security Group". The second table has columns "Door Name" and "Access Time Ta...". At the bottom of the window, there are buttons for "Card Events", "QR Code", "Card Print", "OK" (highlighted in blue), "Cancel", and "Apply".

- **Access Doors** – In Access Doors you can select single door and quickly assign access schedule for the card holder.



Click *Add More* to select a door, enable the door and select access schedule for that door, then click *OK*



Lift Access Level – WatchNET Access Controllers also include Lift (Elevators) panels. *WAE-016-ENC* with built in TCP/IP communication along with *WAE-E16-PCB* expansion boards can handle up to 128 floors on each controller.

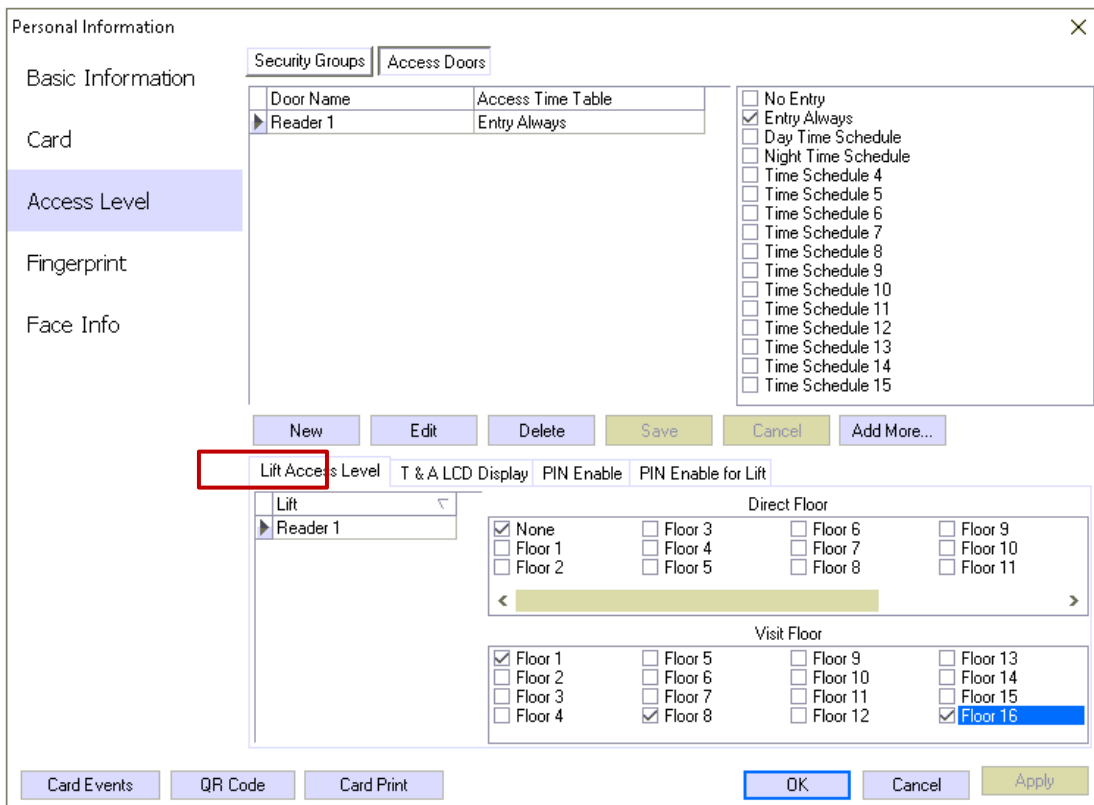
These panels can work offline as well as with the *WatchNET Access Software*.

WatchNET Access Software is intelligently integrating the *WAE-016-ENC panel*. The *WAE-016-ENC* configuration and programming is performed in a similar way to the rest of WatchNET Access panels. This creates efficiency in the setup and use of the panel. Since a Lift has a door we can treat this door like any other door and configure its Access Levels and Time Schedules.

We can see that we set the Day Time Schedule for the Lift Controller (001). This means if the person flashes their card during this time schedule then they will be able to go to each one of the floors checked in the *Lift Access Level* tab.

Direct Floor: can only select one floor

Visit Floor: can select multiple floor that a personnel has access



In the above example only Floors 1, 8 and 16 Floor Buttons will be activated.

Note: Elevator Door must be enabled first to configure floor access levels

T & A LCD Display - Can configure a display message keypad reader that has a Lcd display built in.

Personal Information

Security Groups | Access Doors

Basic Information

Door Name	Access Time Table
Entry door	Entry Always
Exit door	Entry Always
Reader 1	Entry Always

Card

Access Level

Fingerprint

Face Info

Lift Access Level | **T & A LCD Display** | PIN Enable | PIN Enable for Lift

T & A	<input checked="" type="checkbox"/> None	<input type="checkbox"/> 11:
TATP7003TT&A Controlle	<input type="checkbox"/> 1:	<input type="checkbox"/> 12:
	<input type="checkbox"/> 2:	<input type="checkbox"/> 13:
	<input type="checkbox"/> 3:	<input type="checkbox"/> 14:
	<input type="checkbox"/> 4:	<input type="checkbox"/> 15:
	<input type="checkbox"/> 5:	<input type="checkbox"/> 16:
	<input type="checkbox"/> 6:	<input type="checkbox"/> 17:
	<input type="checkbox"/> 7:	<input type="checkbox"/> 18:
	<input type="checkbox"/> 8:	<input type="checkbox"/> 19:
	<input type="checkbox"/> 9:	<input type="checkbox"/> 20:
	<input type="checkbox"/> 10:	<input type="checkbox"/> 21:

Card Events | QR Code | Card Print | OK | Cancel | Apply

Note: T & A Door must be enabled first to configure the LCD display.

PIN Enable - you can select which door has PIN required to access

Personal Information

Security Groups | Access Doors

Basic Information

Door Name	Access Time Table
Door 3	Entry Always
Entry door	Entry Always
Exit door	Entry Always
Reader 1	Entry Always

Card

Access Level

Fingerprint

Face Info

Lift Access Level | T & A LCD Display | **PIN Enable** | PIN Enable for Lift

Door Name	Open Doo
	<input type="checkbox"/>

Card Events | QR Code | Card Print | OK | Cancel | Apply

PIN Enable for Lift – Enables Pin requires on door lift controller

Personal Information

Security Groups | Access Doors

Basic Information

Card

Access Level

Fingerprint

Face Info

Door Name	Access Time Table
Door 3	Entry Always
Entry door	Entry Always
Exit door	Entry Always
Reader 1	Entry Always

No Entry
 Entry Always
 Day Time Schedule
 Night Time Schedule
 Time Schedule 4
 Time Schedule 5
 Time Schedule 6
 Time Schedule 7
 Time Schedule 8
 Time Schedule 9
 Time Schedule 10
 Time Schedule 11
 Time Schedule 12
 Time Schedule 13
 Time Schedule 14
 Time Schedule 15

Lift Access Level | T & A LCD Display | PIN Enable | **PIN Enable for Lift**

Lift	None	Floor 12
Reader 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/> Floor 1	<input type="checkbox"/> Floor 13
	<input type="checkbox"/> Floor 2	<input type="checkbox"/> Floor 14
	<input type="checkbox"/> Floor 3	<input type="checkbox"/> Floor 15
	<input type="checkbox"/> Floor 4	<input type="checkbox"/> Floor 16
	<input type="checkbox"/> Floor 5	
	<input type="checkbox"/> Floor 6	
	<input type="checkbox"/> Floor 7	
	<input type="checkbox"/> Floor 8	
	<input type="checkbox"/> Floor 9	
	<input type="checkbox"/> Floor 10	
	<input type="checkbox"/> Floor 11	

- **Fingerprint – Enrols Fingerprint for personnel**

Enable *Use Fingerprint* to enrol fingerprint.

Personal Information

Basic Information

Card

Access Level

Fingerprint

Face Info

Use Fingerprint

Fingerprint Information

Private Auth Mode: Card / Fingerprint

Fingerprint Type: Normal User

Fingerprint PIN: Use Access Card PIN

Enroll Device: WAB-X-FCKFingerPrint Reader

1:1 Security Lev: 4:Below Normal

Supports up to 3 fingerprints, has been Enrolled 0 pieces.

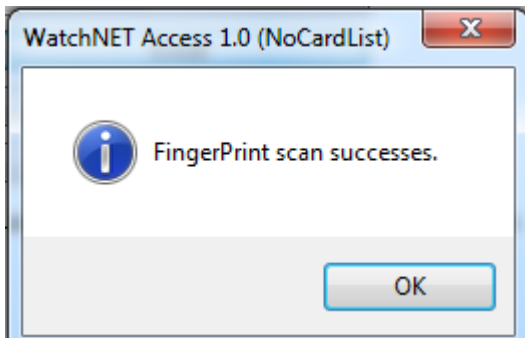
Note: you can enroll using fingerprint reader or usb fingerprint enroller (WAB-P-USB)

Enroll fingerprint using fingerprint reader



Click Enroll and wait the enroll message on the fingerprint reader

Wait for 2 beeps and message on software.

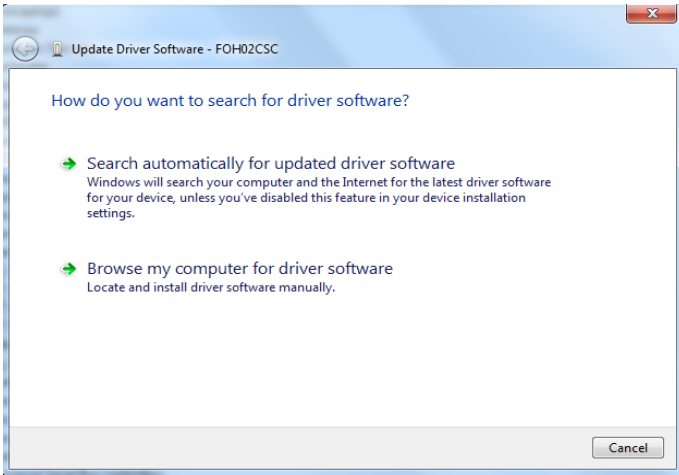


Enrol fingerprint using USB Fingerprint reader

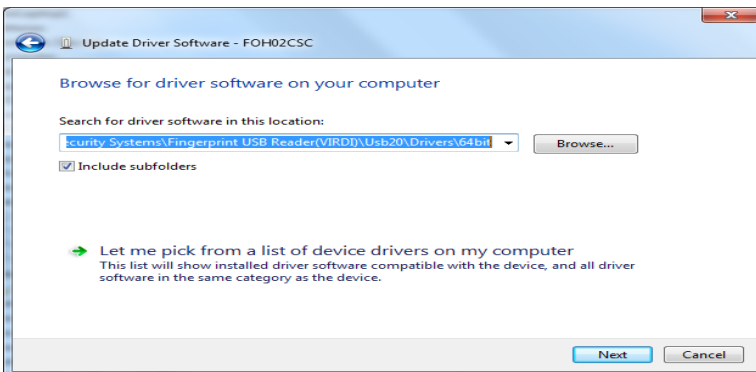
Installing USB Fingerprint Enroller

Click on the  *Windows Start* button and click on Control Panel. Click on the  *Device Manager* button.

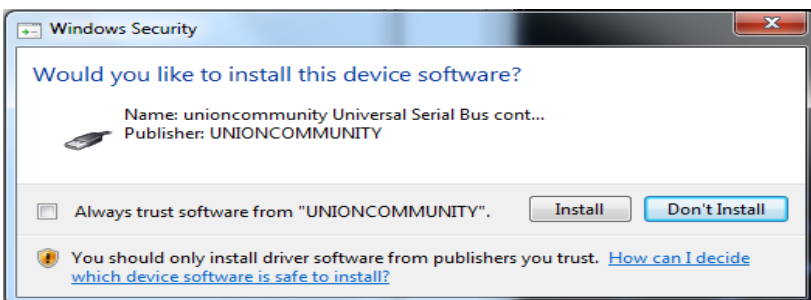
Right click on *FOH02CSC* option 



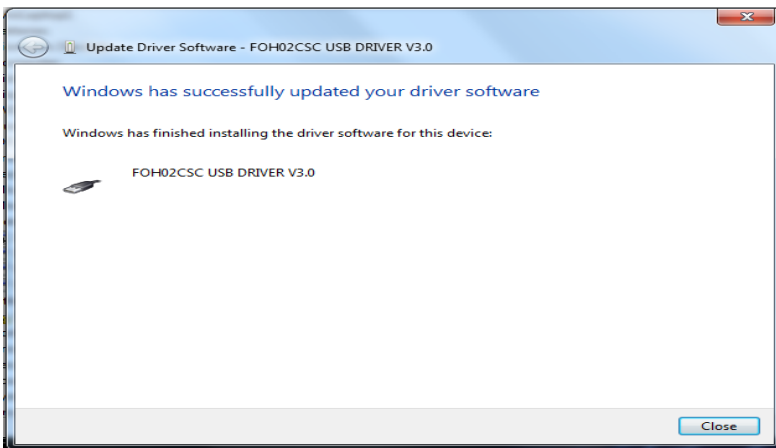
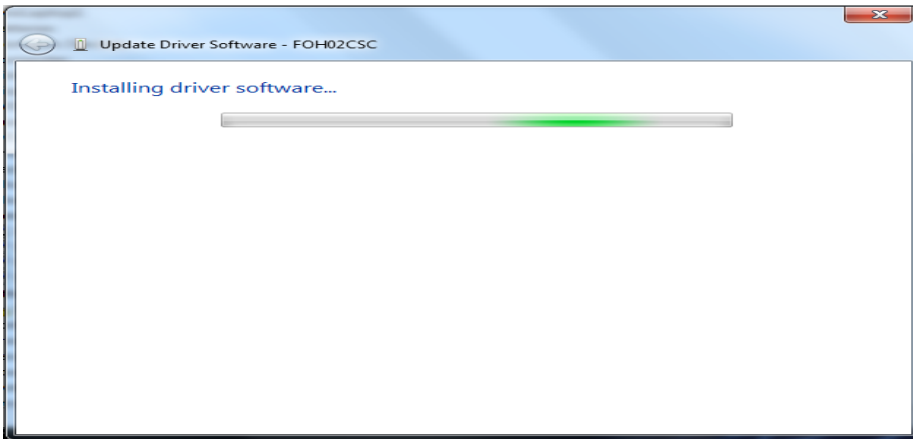
Click on *Browse my computer for driver software*.



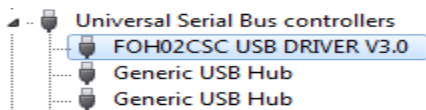
Browse to the following folder path. *C:\Program Files (x86)\WatchNET\WatchNET Access Integrated Security Systems\Drivers\BioUSB10 Enroller Driver(USB2.0)\64bit or 34bit*. And click on the *Next* button.



Click on the *Install* button.



Click on the *Close* button to complete the install.



If properly installed you will see the above driver listed.

In the *Personal Information* window click on the *Fingerprint* tab.

Personal Information
✕

- Basic Information
- Card
- Access Level
- Fingerprint
- Face Info

Use Fingerprint

Fingerprint Information

Private Auth Mode: Card / Fingerprint

Fingerprint Type: Normal User

Fingerprint PIN: Use Access Card PIN

Enroll Device: BioUSB10 Refresh

1:1 Security Lev: 4:Below Normal

Enroll

Delete

Verify

Supports up to 3 fingerprints, has been Enrolled 0 pieces.

Card Events
QR Code
Card Print

OK
Cancel
Apply

Note: Make sure that User Fingerprint is checked

Click on the *Enroll* button to start to enroll fingerprints.



Click on *Next* to start the enrollment of Fingerprints.



Select the finger to enroll.



Place finger on sensor and follow the instructions.



Click on the *Next* button to enroll another fingerprint.



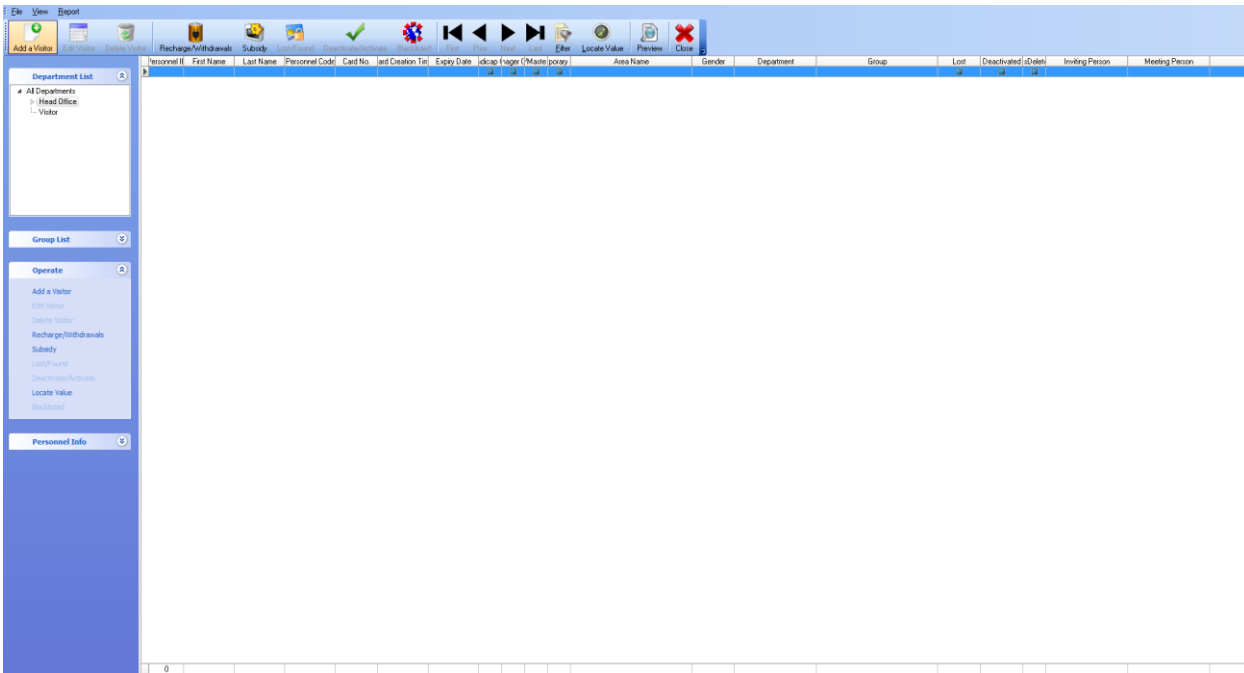
Click on *Finish* to complete Fingerprint enrollment. You will now see that the *Delete* and *Verify* buttons are enabled.

- **Face Info** – enrol face screenshot for face reader

A screenshot of a software interface titled 'Personal Information'. The interface has a sidebar on the left with menu items: 'Basic Information', 'Card', 'Access Level', 'Fingerprint', and 'Face Info'. The 'Face Info' item is highlighted with a red box. The main content area is divided into two sections. The top section, titled 'Face Info', contains a 'Use Face' checkbox, a 'User Type' dropdown menu (set to 'Normal'), a 'Time Zone' dropdown menu (set to '0'), a 'PIN' text input field, and a 'Use Access Card PIN' checkbox. Below these are a 'Face' section with a 'Face Photo' placeholder, a 'Face' dropdown menu (set to 'NF1000 Scanner'), and buttons for 'Refresh', 'Enroll', and 'Delete'. The bottom section is a table with columns for 'Device Name', 'IP', and 'Device ID'. At the bottom of the window are buttons for 'Card Events', 'QR Code', 'Card Print', 'OK', 'Cancel', and 'Apply'.

4.2.3 Visitors List

This option allows you to add/edit or delete a visitor's card



Click **Add a Visitor**

- **Basic Information** – input basic information such as *First Name, Last Name, Department* and other information below

Visitor List
✕

- Basic Information
- Card
- Access Level
- Fingerprint
- Face Info

Personal Information

ID	<input type="text" value="2"/>
Code	<input type="text"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
ID Number	<input type="text" value="3X4"/>
Gender	<input type="text"/>
Address	<input type="text"/>
TEL	<input type="text"/>
Department	<input type="text" value="Head Office"/>
Group	<input type="text" value="Group Name"/>
Visitor's Unit	<input type="text"/>
Inviting Person	<input type="text"/>
Meeting Person	<input type="text"/>
Purpose	<input type="text"/>
To Floor	<input type="text" value="1"/>
Remark	<input type="text"/>

📁
📷
🖨️
✕

Print Visitor
Visitor Ticket
Card Print

- **Card** – Input card number and select properties for the visitor’s card

Card info:

- Card No.** - input card number
- ID card Custom ID** - additional or custom card number
- Expiration Time** - select expiration date for card
- Deactivate** - card will be deactivate when not in used
- Vice Cards** - click to add multiple cards

PIN:

- PIN ID** - Unique PIN ID for each card (only works on Ver. 40.** and 45.**)
- PIN** - Pin number for card holder

Access Properties:

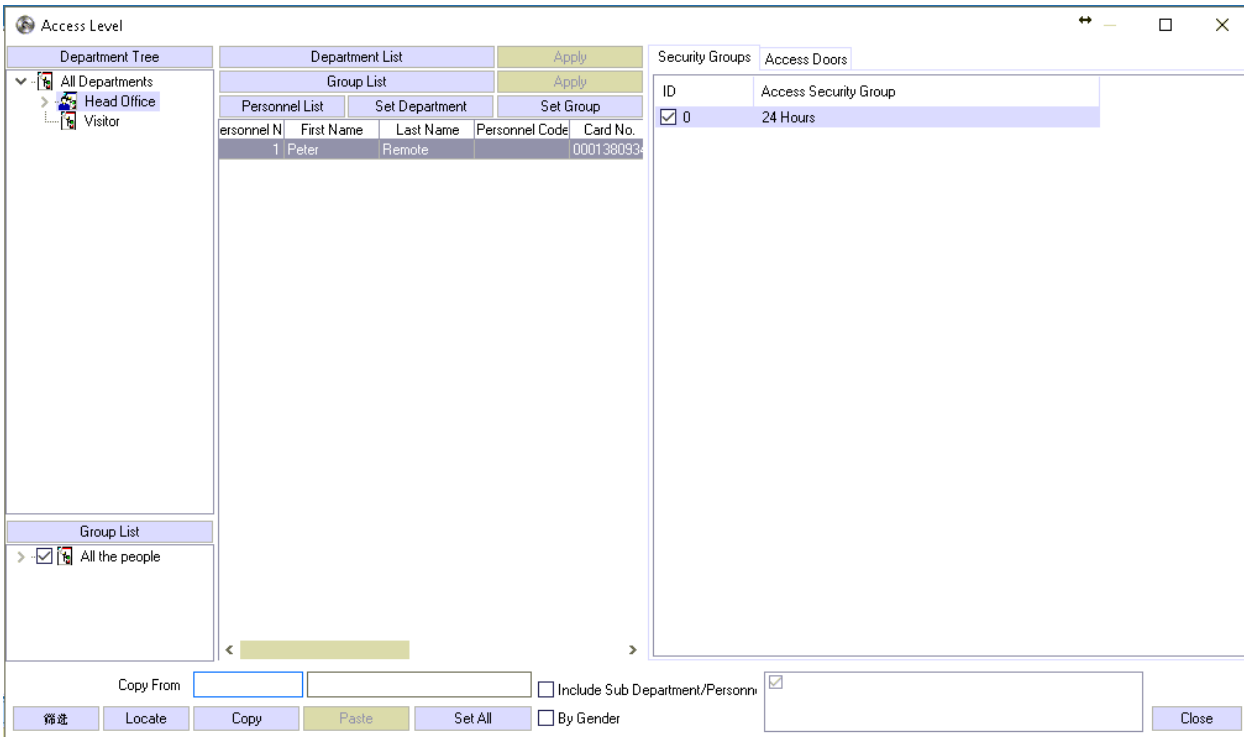
- Handicap Card** - Door will stay open longer when handicap card is enabled
- Boss/Master Card** - have access to all doors and no anti-passback limitations
- Manager Card** - have access to all door base on the department assigned
- Temp Card** - when enable, card is only a temporary card and will expire

Temp Card Valid Time:

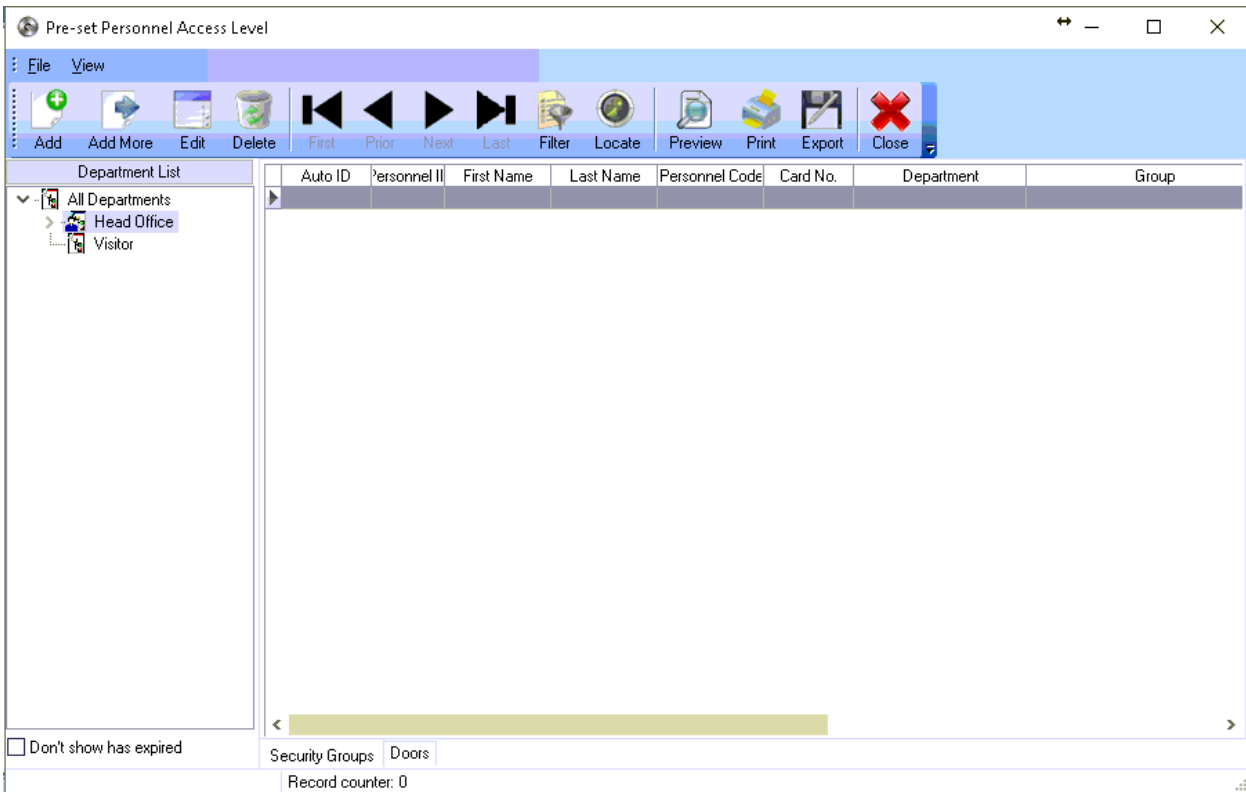
- From/Expiration:** - select a date when the card will be valid

- **Access level** – select access level for card holder, can also refer to **Access Level for Cards** for detailed information
- **Fingerprint** – Enrolls fingerprint for card holder, can also refer to **Fingerprint for Cards** for detailed information
- **Face Info** – Enrolls Face screenshot for card holder, can also refer to **Face Info for Cards** for detailed information

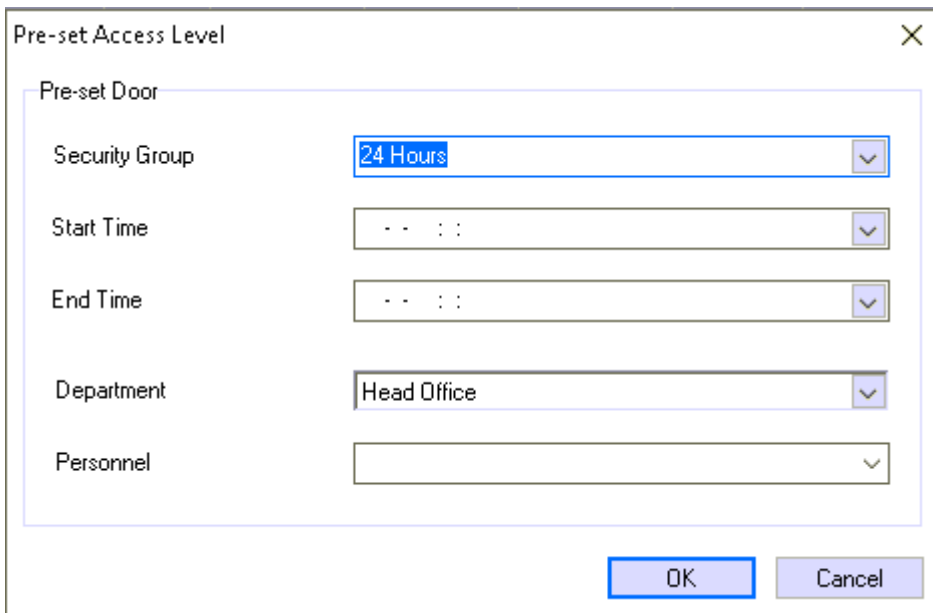
4.2.4 Access Level – Configure or create access level per departments or per personnel.



4.2.5 Pre-set Personnel Access Level – Allows you to create a temporary access level to a card holder to a door for certain period of time.

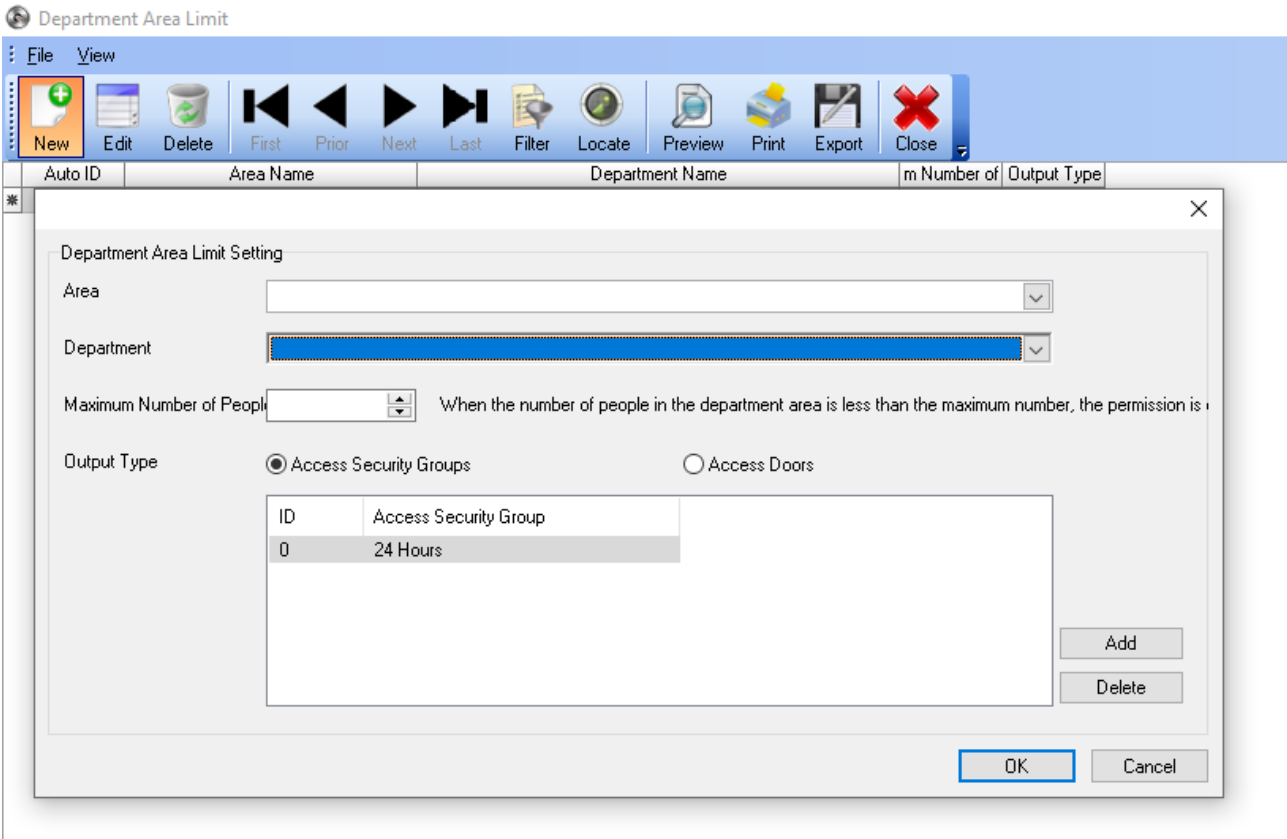


Click **Add** to input access level, you can also click **Add more** to add multiple personnel

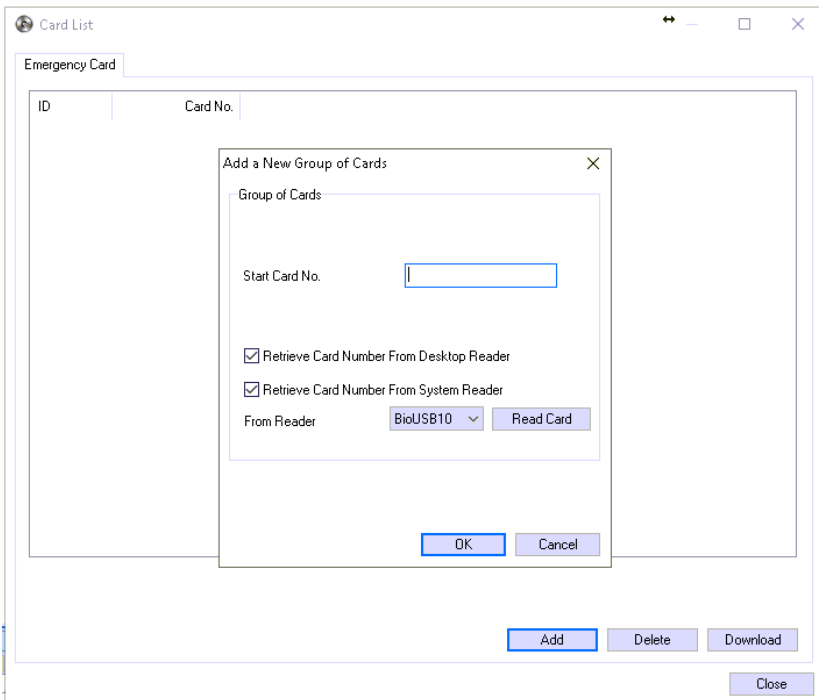


Note: Security group must be created first to create a temporary access level

4.2.6 Department Area Limit – Allows you to set a maximum entry on a specific door



4.2.7 Emergency Card – Allows you to create emergency card when needed



4.2.8 Bank Card – Settings for Bank card feature

4.3 Events Alerts –WatchNET Access Software provides powerful and flexible events handling and notification. Such as Access Event Alerts, Intrusion Event Alerts, and CCTV Event Alerts. For each type of events the user can assign a name, validation (by card number range, date and time) and background color.

4.3.1 Access Event Alerts - From the menu bar, click *Setup->Event Alerts->Access Event Alerts*. This will open the *Event Alerts* window. Access Event Alerts allows user to add, delete or modify an event also user to trigger component by card events or controller component events.

Name	Event	Controller	Dot Name	From Card No
▶ Controller Reset	Reset	ALL	ALL	0000000000
Clear up memory data	Clear All Data	ALL	ALL	0000000000
Invalid Card	Invalid Card	ALL	ALL	0000000000
Valid Card	Door Opened by Valid Card	ALL	ALL	0000000000
Invalid Door/Time	Invalid Door/Time	ALL	ALL	0000000000
Door Forced Open	Door Forced Open	ALL	ALL	0000000000
Connection Failure	Connection Failure	ALL	ALL	0000000000
Door Left Open	Door Opened Too Long	ALL	ALL	0000000000

Record counter: 8

- **Sound Hint** – Sound hit tab allows user to add a tone for that specific event that will play on the server.

Event Edit
✕

Event Source

Name

Event ▼ ...

Device Door/Zone/Channel

From Date To Date

From Time To Time

From Card No. To Card No.

Sound Hint
Popup Hint
Real-time Events
Send Event
Send Email
Send SMS
Print
Lockdown

Sound Hint

Sound File Keep Arming

📁

Sound Text Times

Play Text

<input type="checkbox"/> Beep	<input type="checkbox"/> Site Name
<input type="checkbox"/> Device Name	<input type="checkbox"/> Hardware(Door) Name
<input type="checkbox"/> Event Name	<input type="checkbox"/> Department Name
<input type="checkbox"/> Personnel Name	

- **Popup Hint** – To select the popup location, icon and map popup.

- **Real-time Events** – real time events is configuration for the card events background color and fonts styles.

- **Send Event** – Send event tab allows you to send the specific event to a different server as notification.

- **Send Email** – this tab allows you to configure an email notification for the specific event.

- **Send SMS** – This tab is to configure the send text notification for the specific event.

Event Edit

Event Source

Name

Event

Device: ALL Door/Zone/Channel

From Date To Date

From Time To Time

From Card No. 0000000000 To Card No. 4294967295

Sound Hint | Popup Hint | Real-time Events | Send Event | Send Email | Send SMS | Print | Lockdown

Send SMS

Send SMS

Phone Number

SMS Content

Default Build...

OK Cancel

- **Print** - This tab is to configure an automatic printing to a specific printer whenever this event occur.

Event Edit

Event Source

Name

Event

Device: ALL Door/Zone/Channel

From Date To Date

From Time To Time

From Card No. 0000000000 To Card No. 4294967295

Sound Hint | Popup Hint | Real-time Events | Send Event | Send Email | Send SMS | Print | Lockdown

Event Print

Event Print

Print Content

Default Build...

OK Cancel

- **Lockdown** – Lockdown tab lets you configure a component from the controller either open or close or follow schedule.

Event Edit

Event Source

Name

Event

Device: ALL Door/Zone/Channel

From Date To Date

From Time To Time

From Card No. 0000000000 To Card No. 4294967295

Sound Hint Popup Hint Real-time Events Send Event Send Email Send SMS Print Lockdown

Access Intrusion

ID	Controller	Door / Dot	Action
----	------------	------------	--------

Add Add More Delete Edit

OK Cancel

4.3.2 Prosys Intrusion Event Alerts – From the menu bar, click *Setup->Event Alerts->Prosys Intrusion Event Alerts*. This will open the *Event Alerts* window. Prosys Intrusion Event Alerts allows user to add, delete or modify an event also user to trigger component by intrusion event and component events.

Name	Event Name	Panel Name	Zone Name	From Date	To Date
Disarmed	Disarmed/Normal			2012-01-01	2050-
Tripped	Tripped			2012-01-01	2050-
Armed	Armed			2012-01-01	2050-
Alarmed	Alarmed			2012-01-01	2050-
Bypassed	Bypassed			2012-01-01	2050-
Tamper	Tamper			2012-01-01	2050-
Low battery	Low Battery			2012-01-01	2050-
AC loss	AC Loss			2012-01-01	2050-
Bell trouble	Bell Trouble			2012-01-01	2050-
Phone cut	Phone Cut			2012-01-01	2050-
Clock not set	Clock Not Set			2012-01-01	2050-
Auxiliary failed	Auxiliary Failed			2012-01-01	2050-
Default jumper set	Default Jumper Set			2012-01-01	2050-
Bus communication trouble	Bus Communication Trouble			2012-01-01	2050-
Connected fail	Connection Failure			2012-01-01	2050-
Partition armed	Armed			2012-01-01	2050-

Record counter: 19

4.3.3 Prosys Plus Intrusion Event Alerts – This is for the newer version of prosys plus intrusion

4.3.4 DSC Intrusion Event Alerts – Allows user to add, delete or modify an event, also user can trigger a component by intrusion event

Name	Event Name	Panel Name	Zone Name	From Date
Panel Battery Trouble	Panel Battery Trouble			2008-01-01
Panel AC Trouble	Panel AC Trouble			2008-01-01
System Bell Trouble	System Bell Trouble			2008-01-01
TLM Line1 Trouble	TLM Line1 Trouble			2008-01-01
TLM Line2 Trouble	TLM Line2 Trouble			2008-01-01
General System Tamper	General System Tamper			2008-01-01
Keybus Fault	Duress Alarm			2008-01-01
Connection Failure	Connection Failure			2008-01-01
Zone Alarm	Zone Alarm			2008-01-01
Zone Alarm Restore	Zone Alarm Restore			2008-01-01
Zone Tamper	Zone Tamper			2008-01-01
Zone Open	Zone Open			2008-01-01
Partition Armed Away	Partition Armed Away			2008-01-01
Partition Armed Stay	Partition Armed Stay			2008-01-01
Partition Armed Away No I	Partition Armed Away No I			2008-01-01
Partition in Ready to Force	Partition Armed Stay No D			2008-01-01

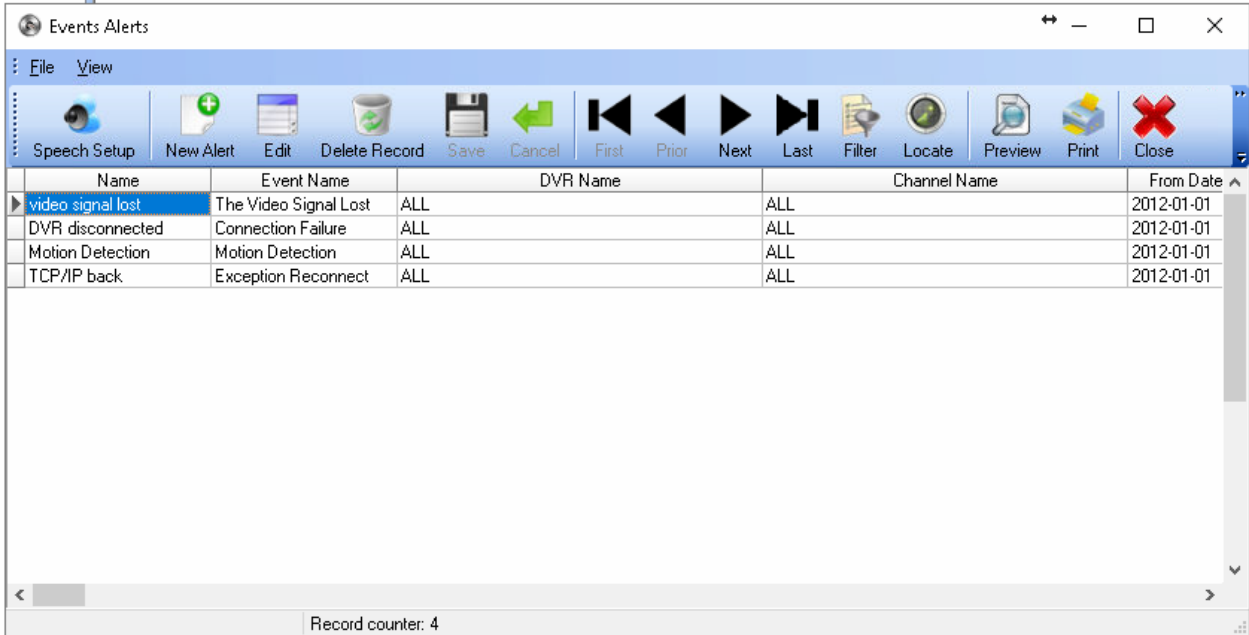
Record counter: 17

4.3.5 PIMA Intrusion Event Alerts – Allows user to add, delete or modify an event, also user can trigger a component by intrusion event

Name	Event Name	Panel Name	Zone Name	From Date
Low Battery	Low Battery			2008-01-01
Panel AC Trouble	Panel AC Trouble			2008-01-01
Siren 1 Trouble	Siren 1 Trouble			2008-01-01
Telephone Line Trouble	Telephone Line Trouble			2008-01-01
Tamper 1 Open	Tamper 1 Open			2008-01-01
Tamper 2 Open	Tamper 2 Open			2008-01-01
Network Communication	Network Communication 1			2008-01-01
Connection Failure	Connection Failure			2008-01-01
Zone Alarm	Zone Alarmed			2008-01-01
Zone Alarm Restore	Zone Alarmed Restore			2008-01-01
Zone Open	Zone Open			2008-01-01
Zone Armed	Zone Armed			2008-01-01
Partition Armed Full	Partition Armed Full			2008-01-01
Partition Armed Home 1	Partition Armed Home 1			2008-01-01
Partition Armed Home 2	Partition Armed Home 2			2008-01-01
Partition disarmed	Partition Disarmed			2008-01-01

Record counter: 16

4.3.6 CCTV Event Alerts - Allows user to add, delete or modify an event, also user can trigger a component by intrusion event



4.3.7 WFD 4 Event Alerts- Allows user to add, delete or modify an event for the face devices, also user can trigger a component by intrusion event

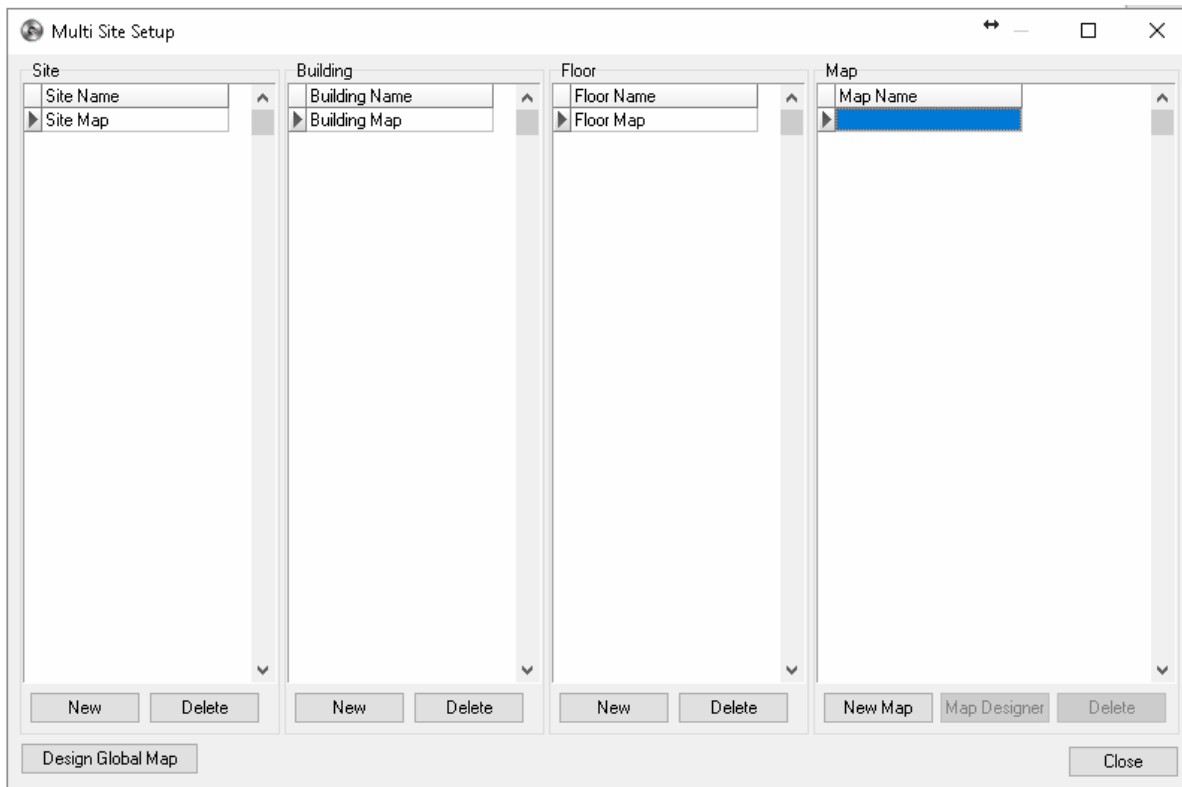
4.4 Map

WatchNET Access Software allows for multi-level mapping. Up to four levels of maps can be created and displayed. Map levels include sites, buildings and floors. User can view all controller components (locks, sensors, exit buttons, inputs, and outputs). All maps and controller components are dynamic. Components graphical icons will change according to their physical status (i.e. lock was opened).

Maps can be easily designed by dragging and dropping component icons on to the map. As mentioned in section 8.3 Maps can Popup automatically and switch from Map X to Map Y if an alerted event took place on Maps' Y controller component and Map was on Map X.

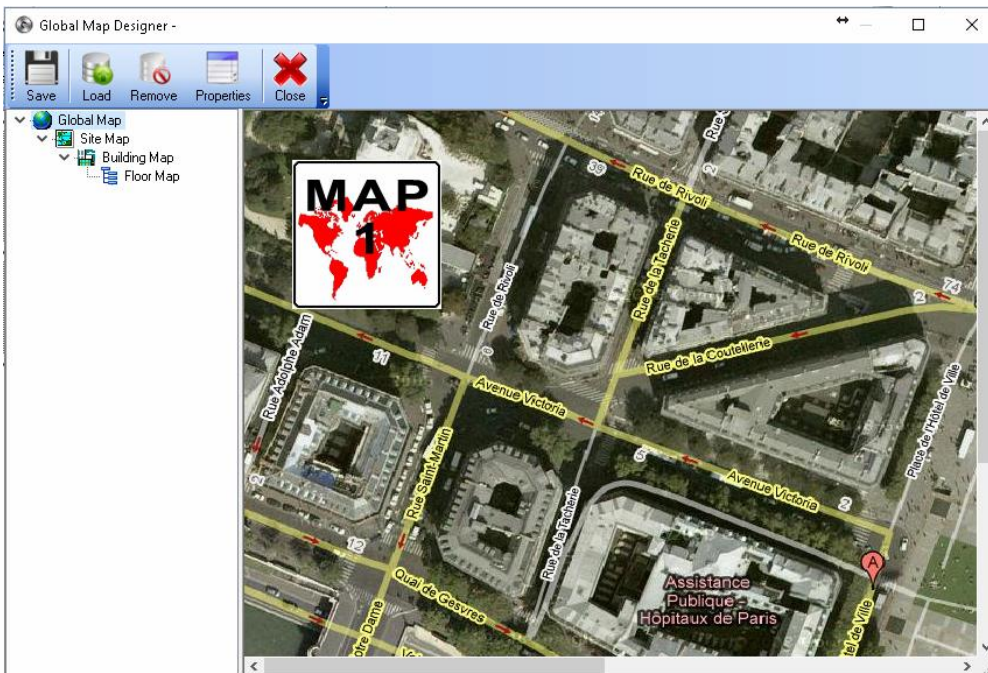
4.4.1 Multi-Site Setup

In the *Multi-Site Setup* is where the sites structure is configured. We define the sites and their names, the buildings in each site, the floors in each building and their maps (Figure 7-80). To start configuring Maps click on *Setup -> Map -> Multi Site Setup*.



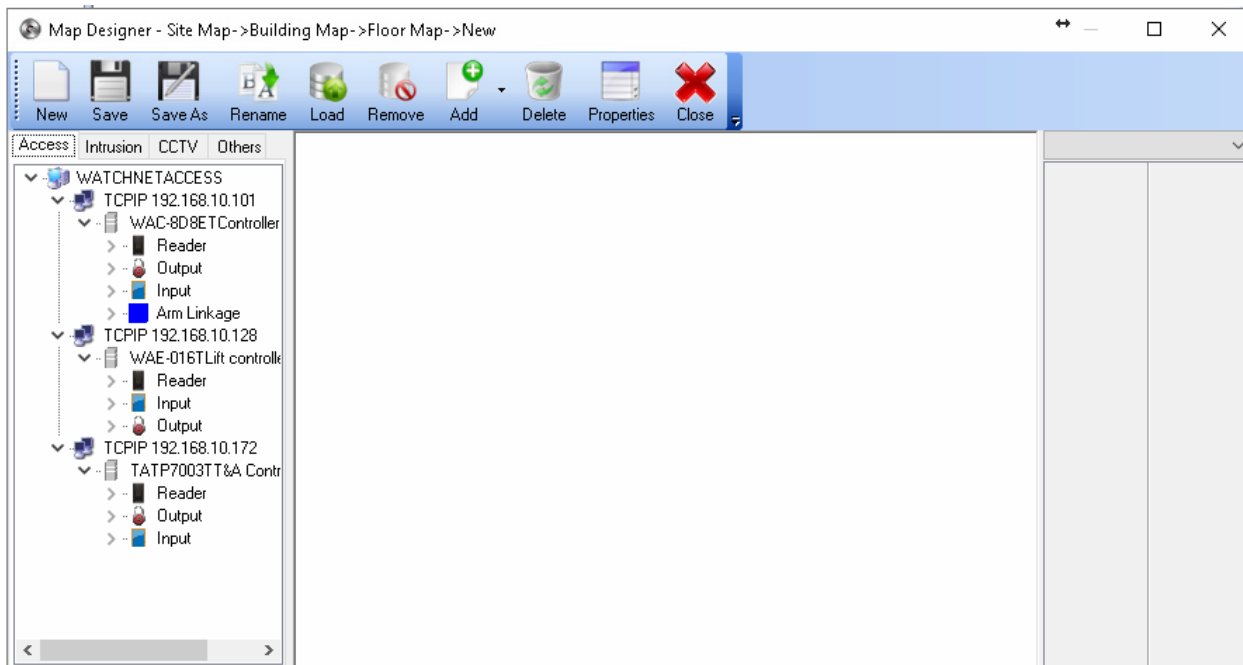
Site

The *Site* is the first level of Maps and first to be displayed and is assigned the *Map 1* icon. To load a *Global Map* click on the *Design Global Map* button. Click on the *Load* button and navigate to the path where the Map is located.



New Map

To start creating a new Map (Figure 7-81) click on the *New Map* button from the *Multi Site Setup* window.



New: Blank Canvas for creating a new map.

Save: Saving the created map.

Save As: Saving the created map under a different name and *Pic ID* (Picture ID). *Pic ID* is the unique identifier for maps. User can re-use the map name but not the *Pic ID* of the map.

Rename: Changing the map name.

Load: Loading a JPG picture to be the map usually a floor or blue print drawing.

Remove: removing the map JPG file.

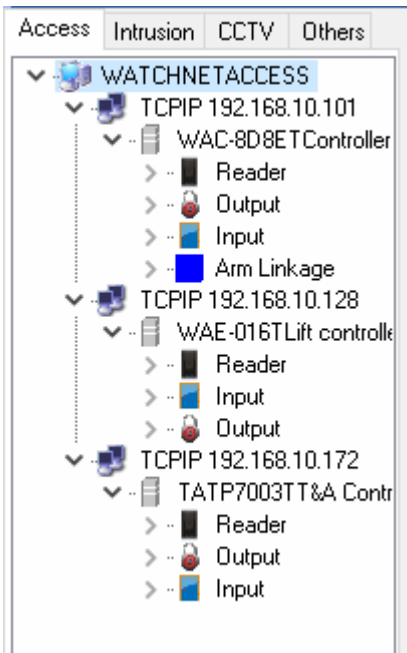
Add: Adding controller components to the map. You can select multiple components by holding the *Shift* Key and clicking on the *Down Arrow* button or by holding the *Ctrl* key and selecting multiple components using the mouse. After adding the components they will be displayed on the left upper corner of the map (overlapping each other). You may drag each one for the desired position and then click *Save* to keep them in the new position.

Delete: Select a component and click the *Delete* button to delete the component from the map.

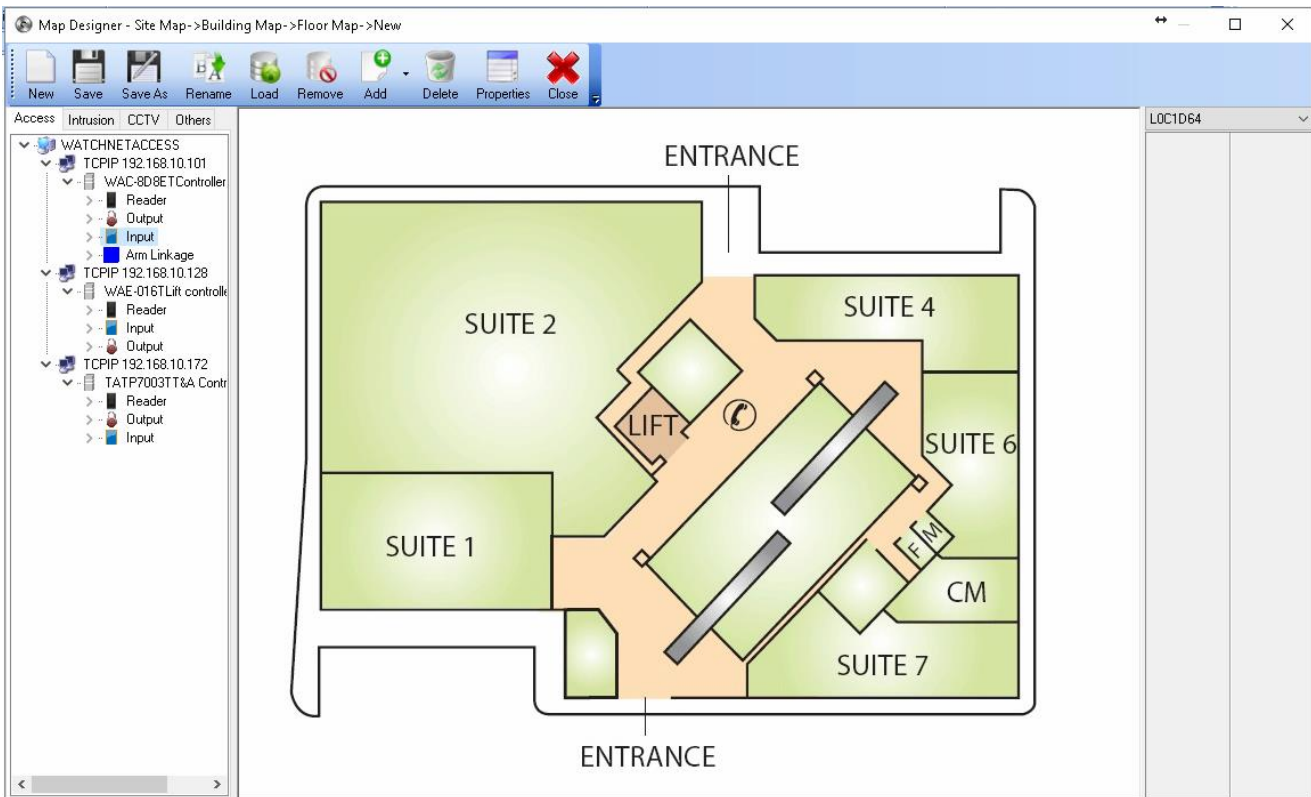
Properties: Viewing and changing the component properties.

Close: Closes the *Map Designer* window.

There are four types of components that can be added to the Map (Access, Intrusion, CCTV and Others). These components are grouped in tabs that are located on the left hand side of the *Map Designer* window.

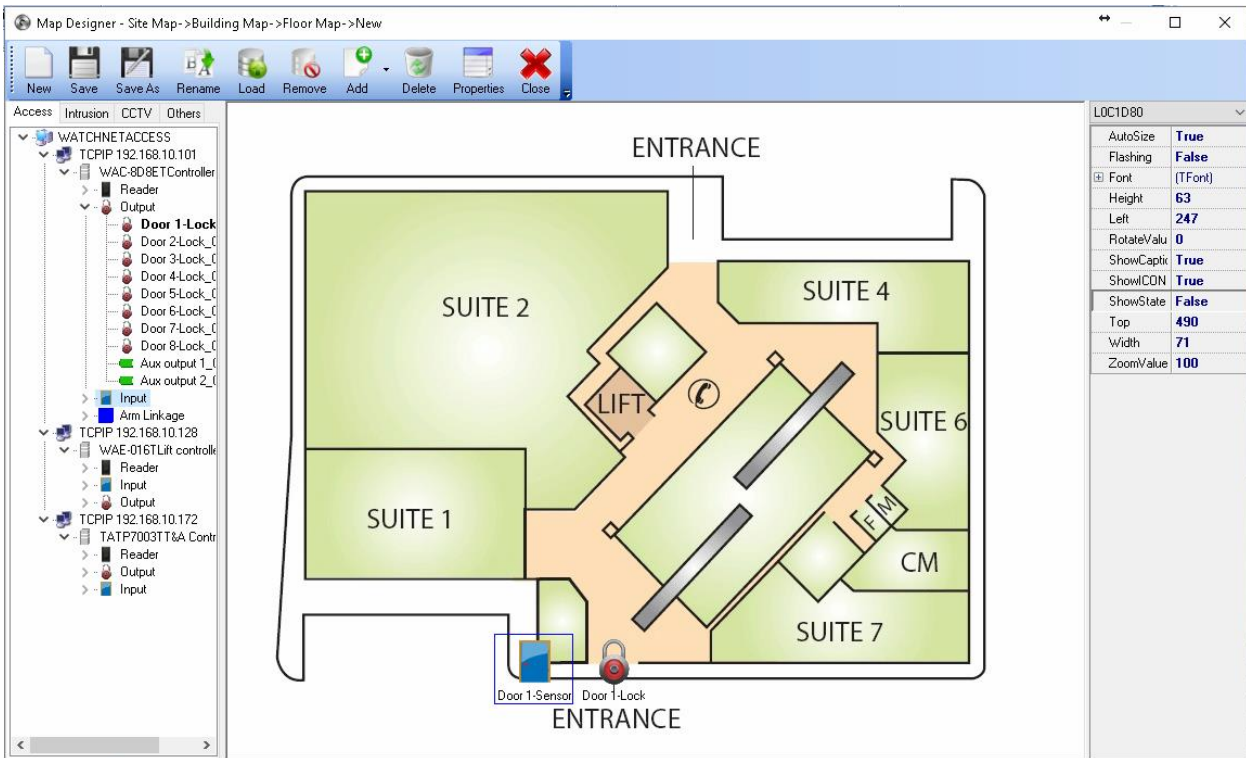


Click on the *Load* button to select a Map from the *Map* folder. The default path to the *Map* folder is C:\Program Files (x86)\WatchNET\WatchNET Access Integrated Security Systems\Maps. Select a Map and click *OK*.

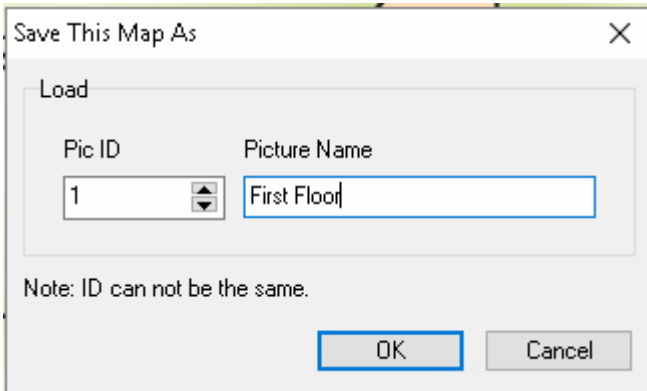


Next select the components to add to the Map by clicking on the corresponding tabs. Drag and Drop the component

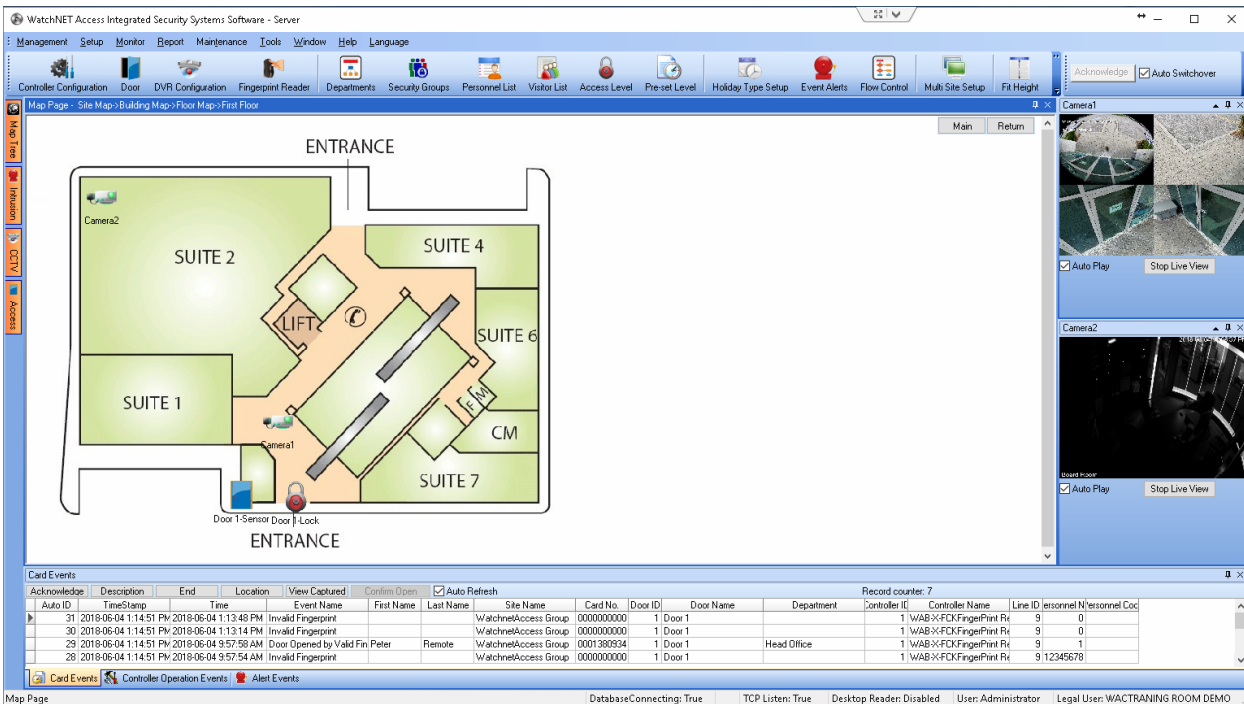
onto the desired location on the Map.



Click the *Save As* button to save the Map.



Enter the *Picture Name* and click *OK*.



The new Map is now displayed on the Main window.

4.4.2 Map Designer

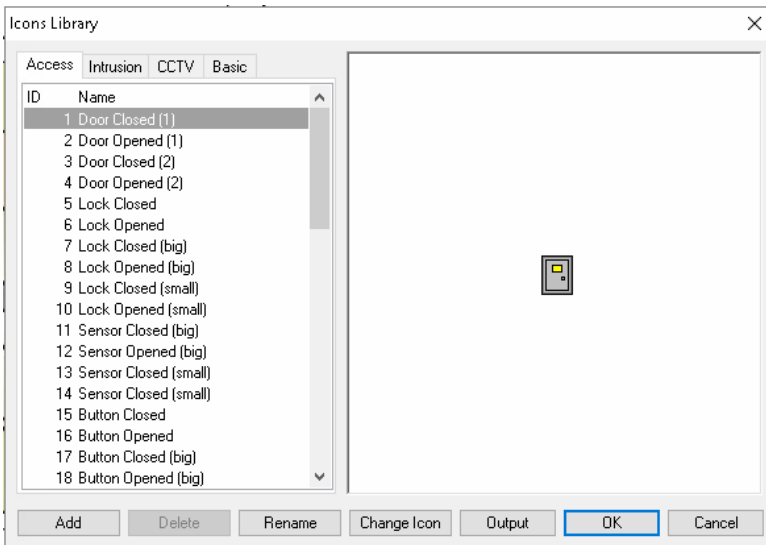
Shortcut menu to configure the map.

4.4.3 Delete Map

Delete a Map by selecting it from the list.

4.4.4 Icon Library

The Icon library offers a selection of different icons for the same component including different size (i.e. small lock icon, big lock icons etc.). This provides high flexibility for the user in respect to his map picture or blue print proportion.



- **Add:** Adding an Icon by selecting a JPG picture and entering an Icon ID and Icon name.
- **Delete:** Deleting an Icon.
- **Rename:** Chaining Icons' name.
- **Change Icon:** Changing the Icon picture (JPG file).

4.5 Flow Control

4.5.1 Access Flow Control

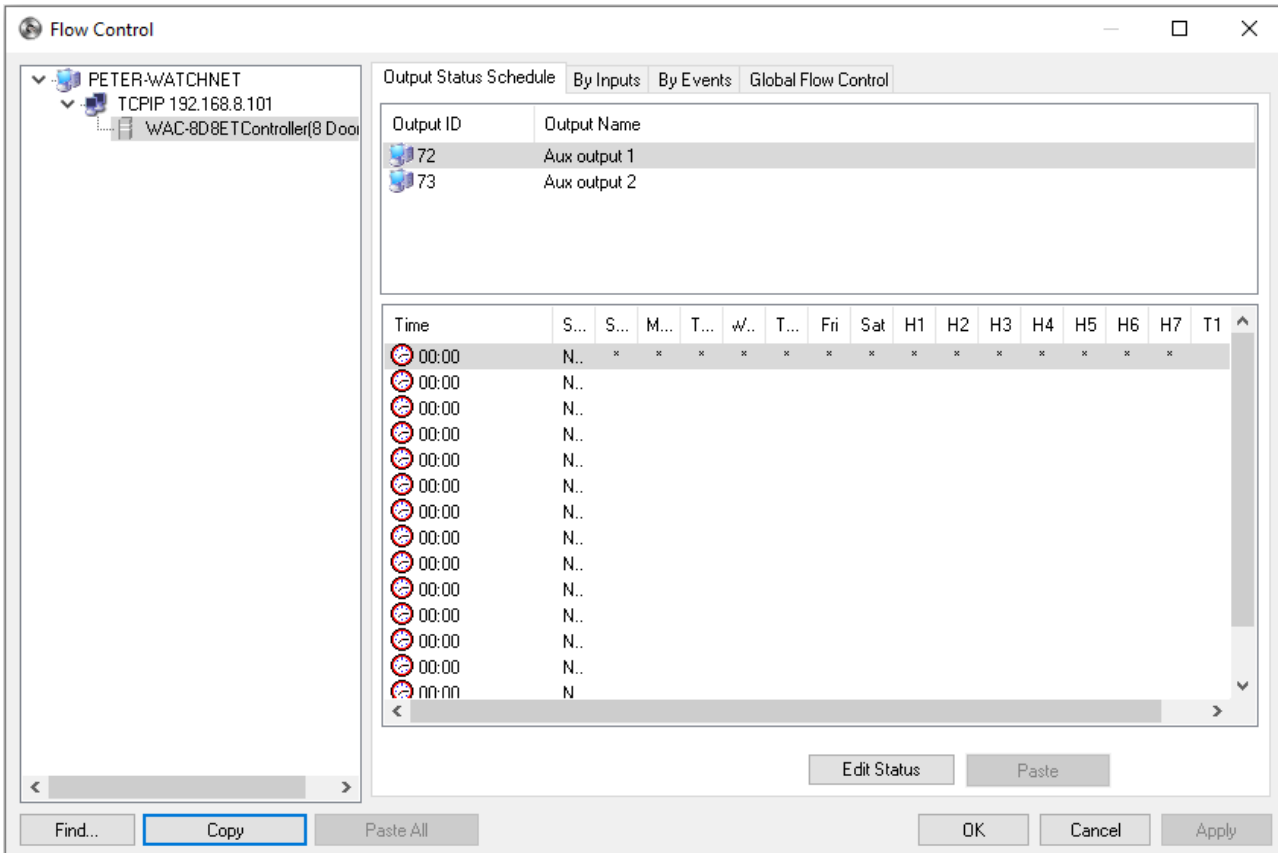
Flow Control allows for defining a logical conditioning such as *If (Condition) Then (Action)*.

AND, OR operands can be applied to create more complex conditions.

There are 3 types of the Flow Control:

1. Output Status Schedule
2. By Inputs
3. By Events
4. By Global Flow Control.

To launch the *Flow Control* window, click on *Setup -> Flow Control -> Access Flow Control*.



Output Status Schedule

On this feature you can set the additional output relay to follow open/close schedule on a certain schedule

By Inputs

Flow Control *by Inputs* means the Flow Control is done according to the physical controller components (Locks, Exit Buttons, Door Sensors, and Aux Inputs/Outputs etc.).

Condition can be created like the example below:

If (Source1) AND (Source2) AND ... (Source8) Then Activate (Relay);

We do not have to use several *Sources* with *AND*.

Flow Control allows the user to use the WatchNET Access system not only for Access Control application but also for any type of automated control like basic Building Management.

With this we can also connect to a Fire Alarm System contact and command all doors to be opened automatically.

Based on an external timer (sensor) we can turn off lights or air conditioning system in the building.

For Example; **Source** (Aux Input 1 = Open) **Output Action** (Aux Output 2 = Open) and **Action Mode**: Back to Normal, this means that if the Aux input 1 is open, Aux Output 2 will be open as well and Action mode is set to Back to Normal if source is closed.

Source	Action	Delay
88 - Aux input 1	Open	0
None		0
		0
		0
		0
		0
		0
		0

Conditional Logic: []

Output Action: 73 - Aux output 2, Open, 0

Delay Time(Sec): 0

Priority: Lowest(Level 1)

Action Mode: Keep Opened/Closed (Until next link condition, For (Sec): 0= Unlimited Time, 0) Back to Normal (Following this condition)

Type: Disable Normal Armed (Arm Linkage 1)

Buttons: OK, Cancel

By Events – Flow control by events allows you to open certain relays by using all different types of event from

the doors and relay inputs, it could be opened from first card, door forced open or invalid card. In example below, If the Door 1 is forced opened the Aux Output 1 will be open for 10 seconds and will close again after.

The 'By Events Conditions' dialog box contains the following fields:

- Event Source: Door (1 - Door 1)
- Event: 18 - Door Forced Open
- Output: 72 - Aux output 1
- Action Time(Sec): Open (10)

Buttons: OK, Cancel

Note: WatchNET Access Server will have to be online, closing the software will stop the global flow control conditions.

Global Flow Control – Allows you to trigger an output from 1 controller to another controller

The 'Global Flow Control' dialog box contains the following sections:

- Source:** Controller (Main Floor), Component (Door 1-Lock), Status (Open)
- Output:** Controller (Second Floor), Component (Door 2-Lock), Status (Open), Delay Time(Sec) (0), Priority (0)
- Enable:** Enable
- Action Mode:** Keep Opened/Closed Until next link condition, Back to Normal Following this condition
- Action Time(Sec):** 0

Buttons: OK, Cancel

For Example: If Door 1-Lock is open from Main Floor controller the Door 2-Lock from Second Floor will be

opened as well and will go Back to Normal when door 1 lock is closed.

Armed Linkage

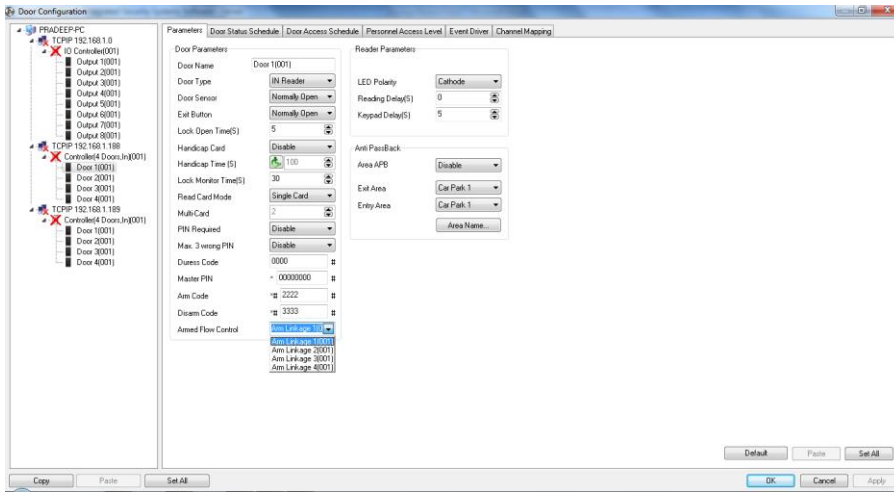
WatchNET Access software enables events to be controlled through the keypad reader by entering specific codes. Up to four linkages is possible per reader. In order to use this function, we first need to program a link through flow control. Let's assume a scenario where we have a Motion Sensor connected to Auxiliary Input 1 and we need an Alarm on Auxiliary Output 1 only when Auxiliary Input 1 is in Armed condition.

To achieve this, we need to program a flow control and enable this as Armed Linkage 1 as indicated below:

The screenshot shows the 'Add Condition' dialog box with the following configuration:

- Source:** 88 - Aux input 1 (Open, 0)
- Action Mode:** Keep Opened/Closed (Until next link condition, 0)
- Output Action:** 72 - Aux output 1 (Open, 0)
- Type:** Armed (Arm Linkage 1)

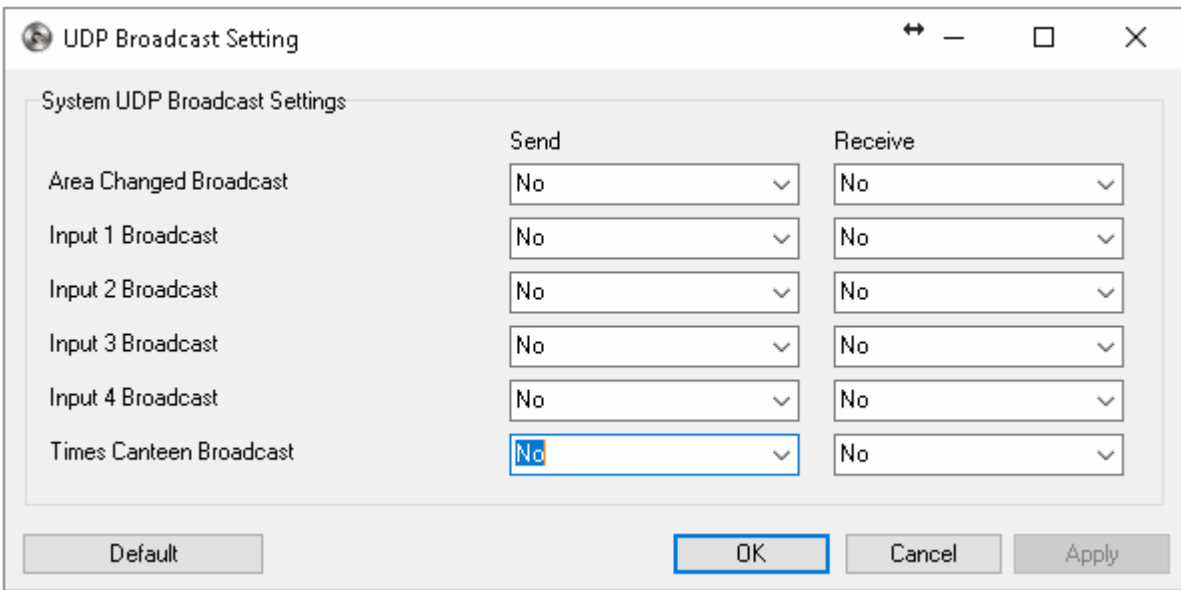
Once this is done then we need to activate this link through Keypad card readers on this controller. Let's now move to Door Parameters. In the door parameters choose the reader which has the keypad and in the door parameters tab set the Arm Code and Disarm Code as indicated below. This code is then set to Armed Linkage 1 or whatever was programmed to achieve what we need.



We can test this function by first right clicking on Armed Linkage 1 and then turning the Auxiliary Input 1 ON. The Auxiliary Output 1 will turn ON. When Armed Linkage is disarmed then turning Aux Input 1 will not turn Aux Output 1 ON. If this works then the Armed Linkage is right.

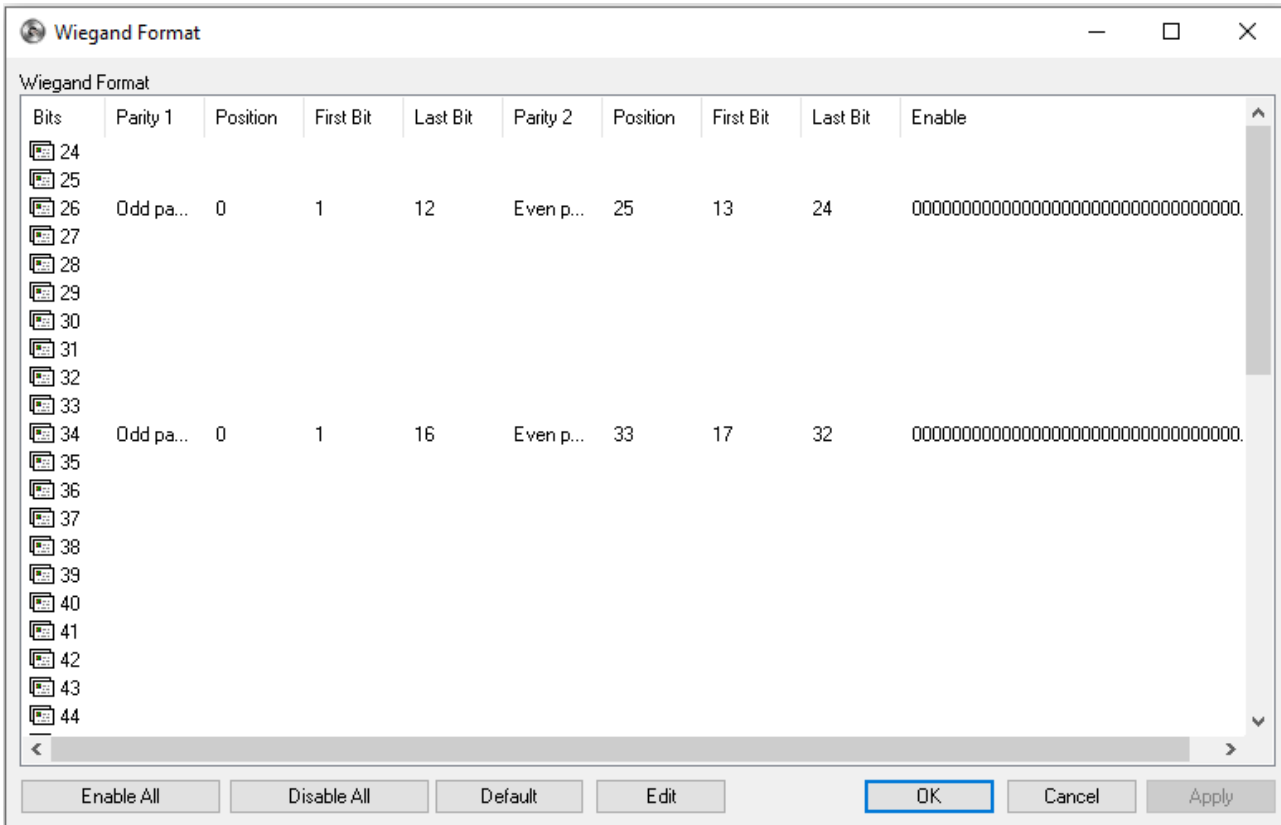
To use this function through a reader, first flash a valid card that has access to that door at that time and enter the appropriate codes to Arm and Disarm the linkage.

4.6 UPD Broadcast – UDP Broadcast is use to enable the flow control using RS485 connection, when this feature is enabled the software does not have to be online all the time to execute the flow control.



4.7 Wiegand Format

The method by which WatchNET Access panels can be configured to read multiple formats simultaneously is set up from the Wiegand Format window. By default, the system comes with four pre-defined formats. These are 26-bit & 34-bit. Any format between 24 and 72 bits can be configured from this window. If the system is required to read a card with a number of bits outside the two listed above then these formats need to be configured before a card will be able to be read by the system.



To edit a format first highlight the format and click on the *Edit* button. The Wiegand Format setup window will appear (Figure 7-95). The *Use Wiegand XX Bits Format* box must be checked if you wish the system to recognize this format

Setting Rules:

- For Wiegand format setting you should enable the format of the card you are using and disable all others.
- If the correct Wiegand format is not configured then you may get a wrong card number.

NOTE: THIS SECTION IS MEANT FOR ADVANCED USERS ONLY. PLEASE DO NOT MODIFY ANYTHING IN THIS SECTION UNLESS NEEDED. ANY ERRORS COULD AFFECT THE ABILITY OF THE READERS TO READ THE CARDS PROPERLY.

The example below is a for 34 Bits format. Initially leave the two *Parity* boxes blank and proceed to the *Data Format* section at the bottom of the window. At the *Data Format* section enter the valid bits you want to read as a 1's and any bits that you do not want to be read enter as a 0. If you only know the number of bits on a card but do not know where the parity bits are located then as a temporary measure enable all the card bits, i.e. for 34 bit, place a 1 under bits 0 to 33. At this stage close the window and flash a card with the same format that has been entered. If the card reads and creates a card event in the *Events Monitor* then the system is recognizing the card format.

Note: this is not the card number but it is just the number generated by all of the bits that have a 1 allocated to them.

Return to the *Wiegand Format* window to continue. If nothing happens when a card is flashed and the system does not recognize the card format then the card is not the same format that has been edited.

Wiegand Format

Use Wiegand 34 Bits Format.

Parity No. 1
 Parity: Odd parity
 Parity Bit: 0
 First Bit: 1
 Last Bit: 16

Parity No. 2
 Parity: Even parity
 Parity Bit: 33
 First Bit: 17
 Last Bit: 32

Filter Bits
 First Bit: 0
 Last Bit: 0
 Filter Values: 0 0 0 0 0 0 0 0

Issue Code
 First Bit: 0
 Last Bit: 0

Data Format
 "1" - Valid Bit, "0" - Invalid Bit
 00000000 00000000 00000000 00000000 00000001 11111111 11111111 11111111 11111110
 位71 Bit0

Default OK Cancel

Once the system is actually reading the card format the next step will be to set the *Data Format* box so that the system ignores any *Parity bits*. This is for the purpose of calculating the card number. Most formats but not all also have a *Parity bit* at the start of the card data and another at the end. While these bits appear on the card and form part of the bit structure and number of bits they do not contribute to the card number. The *Data Format* box now needs to be edited and a 0 placed under any bits that are *Parity bits*. In the following example the 1st (bit 0) and the

last (bit 33) are both *Parity bits* so a 0 is placed under bits 0 and 33. Click *OK* then flash the card at a valid reader. *The number that appears now is the card number.* In the following example the standard *MIFARE 34-bit* card has been used. The standard *MIFARE card* has 32 cardholder bits plus 2 x parity bits and one at each end thus giving a total of 34 bits.

Note: some readers such as Indala for example add a one-byte checksum (8 bits) onto the MIFARE card number and send the data out as 40 bits.

The next step is to enter the Parity data into the Parity 1 and Parity 2 Windows. Although the system will work without this information the parity bits protect the data being received by the system and ensure that only valid data is received. In the 34-bit example the parity bits are bit 0 for parity bit 1 and bit 33 for parity bit 2. Enter a 0 for Parity No 1 and enter a 33 for Parity No 2. If there are more than 2 parity bits then ignore them.

Parity can be either None, Odd or Even and this must be known. Parity Bits check that the data is not corrupted and will normally be calculated over a specific number of bits. In the 34-bit example the Parity No 1 (Bit 0) is Odd Parity calculated over bits 1-16. Parity No 2 (Bit 33) is Even Parity calculated over bits 17-32. The card manufacturer will normally supply the total number of bits the location of parity, whether parity is None, Odd or Even and the bits over which the parity is calculated.

Parity is very important and if both parties are set to none then you might get a wrong card number. Please ask the reader supplier to give you a correct structure of Wiegand output.

Different readers have different parities. But most of HID readers are the same. The output of HID reader is depending on the card.

Note: there are many different methods for numbering the bits. The WatchNET Access software and panels count from the right-hand side at bit 0. Some systems start counting at bit 1.

4.8 Special Date

Temp Date

Clicking on the Temporary Date sub-menu item will open the *Temporary Date Setup* Window. Two sets of Temporary Dates can be configured. The default date is the current date. Temporary dates will be cancelled after 7 days.

Temp Date ✕

Temp Date T1

Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Temp Date T2

Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Temporary dates will be cancelled after 7 days.

Holiday Type Setup

Click on *Setup -> Special Date -> Holiday Type Setup* to launch the Holiday Setup window. To select a holiday just double click on the date and the color will turn Red to indicate that this date is now a holiday. To cancel a previously selected holiday just double click the red holiday and it will return to the default color. There are seven holiday groups available from the tabs at the bottom of the Window and each group can have 365 holidays.

Holiday Type Setup ✕

2020 Su Mo Tu We Th Fr Sa Su Mo Tu We Th Fr Sa Su Mo Tu We Th Fr Sa Su Mo Tu We Th Fr Sa Su Mo Tu We Th Fr Sa Su Mo

January			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
February						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29		
March	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
April			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30				
May					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
June		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30					
July			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
August					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
September			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30				
October				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
November	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30						
December		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				

H1 H2 H3 H4 H5 H6 H7

To select/unselect a holiday double click on the date (will turn RED).
 Holiday auto add to T&A

4.9 Communication Configuration

In order for the software to communicate with the controller or converter the communication parameters need to be configured. This is done in the *Communication Configuration* window.

Server Tab

The *Server name* is the name or IP of the PC which runs the WatchNET Access Software. For PCs which are running WatchNET Access Software as Clients the Server PC name or IP should be set in this field.

The *Server Port* is 47100 by default and should only be changed if the same port is being used by another software. In this case *Server Port* will need to be changed to avoid conflicts.

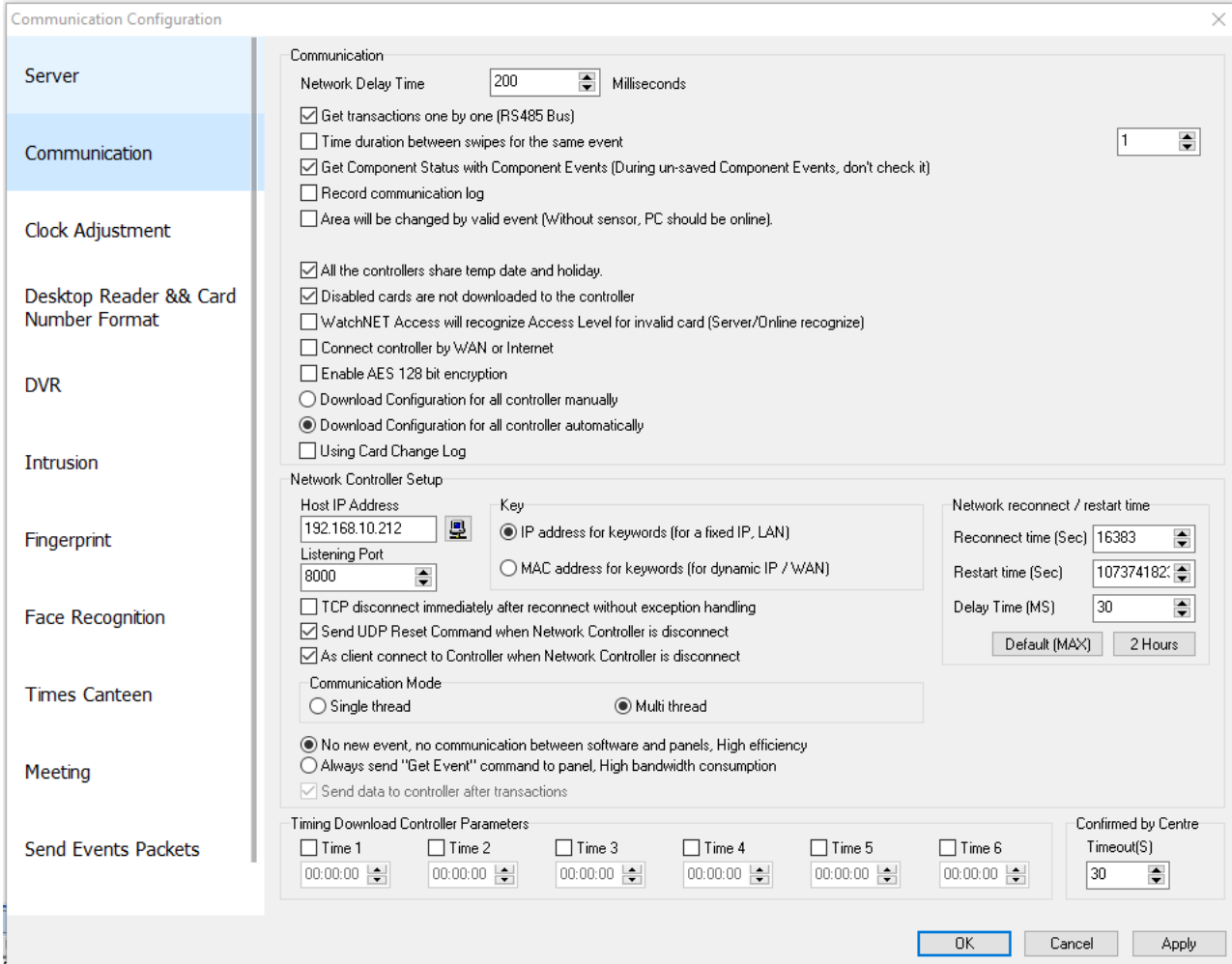
The screenshot shows the 'Communication Configuration' window with the 'Server' tab selected. The window title is 'Communication Configuration' and it has a close button (X) in the top right corner. On the left is a vertical navigation pane with the following items: Server (selected), Communication, Clock Adjustment, Desktop Reader && Card Number Format, DVR, Intrusion, Fingerprint, Face Recognition, Times Canteen, Meeting, and Send Events Packets. The main area is titled 'Server Setup' and contains the following fields and options:

- Server name / IP address:** A text box containing 'PETER-2021' with a computer icon to its right.
- Server Computer Internet IP Address:** An empty text box.
- Server Port:** A spinner box set to '47110'.
- User Name and Password Verification Required
- Publish/Subscribe communication progress reminder:**
 - Publish communication progress notification
 - Subscribe to notifications of communication progress
- Check Database:**
 - Enable
 - A spinner box set to '30' followed by the text 'Seconds/Once'.
- The First Day of Month:**
 - A dropdown menu set to '1' followed by the text 'Day as the beginning of each month'.

At the bottom right of the window are three buttons: 'OK', 'Cancel', and 'Apply'.

Communication Tab

The Communication tab is shown below.



Network Delay Time:

The maximum delay time allowed between the controller and the Host PC. If the *Network Delay* will be for more than 200 milliseconds then the WatchNET Access Software will consider the controller Offline.

User needs to adjust the value according the quality of the LAN in use.

- If panels are connected by unstable LAN then *Delay Time* should be more than 50 Milliseconds, e.g. 200 Milliseconds.
- If panels are connected through Wireless LAN then *Delay Time* should be more than 50 Milliseconds e.g. 200 Milliseconds.
- If panels are connected over WAN then *Delay Time* should be more than 50 Milliseconds e.g. 1,000 Milliseconds.

Get transaction one by one (RS486 Bus):

The software will receive the transactions (events) from each controller one at a time. It is not recommended to

leave the check box unchecked as transactions from controller to the WatchNET Access Software might be lost.

Send Data to controller after transactions:

If this option is selected then the WatchNET Access Software first gets transactions and then sends the next data packet. It is not recommended to select this option when the system is connected to many panels. Checking this option under these conditions would cause a massive amount of CPU usage.

Get component status with component events:

If this option is selected then the software will first retrieve component events from controller and then it will check for events and if the events include a change in component status then the system will retrieve the component status. The software will finally refresh the component status thus saving system resources. If you uncheck the checkbox then the software will retrieve the component status actively.

Write communication log:

When checked all the communication events will be logged in *Communication.txt* log file. The file is in the *WATCHNET ACCESS INTEGRATED SECURITY SYSTEMS* folder.

Broadcast public information:

When checked the public information (All the information which is common to all panels e.g. Card information, Holidays, Summer/Winter time etc.) will be sent to all panels at the same time. The public information will be sent only 1 time and if there is communication/network failure then some information might be lost and may not reach to the panels. If not checked then the software will send the public information to the panels one by one. If communication fails then it will send it again automatically up to 10 times. It's recommended not to check the check box.

WatchNET Access Software will broadcast the information below to all the panels which are connected to the Host PC. Otherwise the WatchNET Access Software will download the information to each controller one by one.

- Card List
- Holidays
- Temporary date
- Summer/Winter Time
- Wiegand Formats
- Saved Event


Area will be changed by valid event (without sensor, PC should be on line):

This option is checked if there are no door sensors and Anti-Pass Back (APB) function is used. The APB function by default is changing the Personnel area based on a *Valid Card* event + Door Sensor Open status. If the user checks this option then the area will change based on a *Valid Card* event only.

Note: For APB to work the server must be online.

All the panels share temp date and holiday:

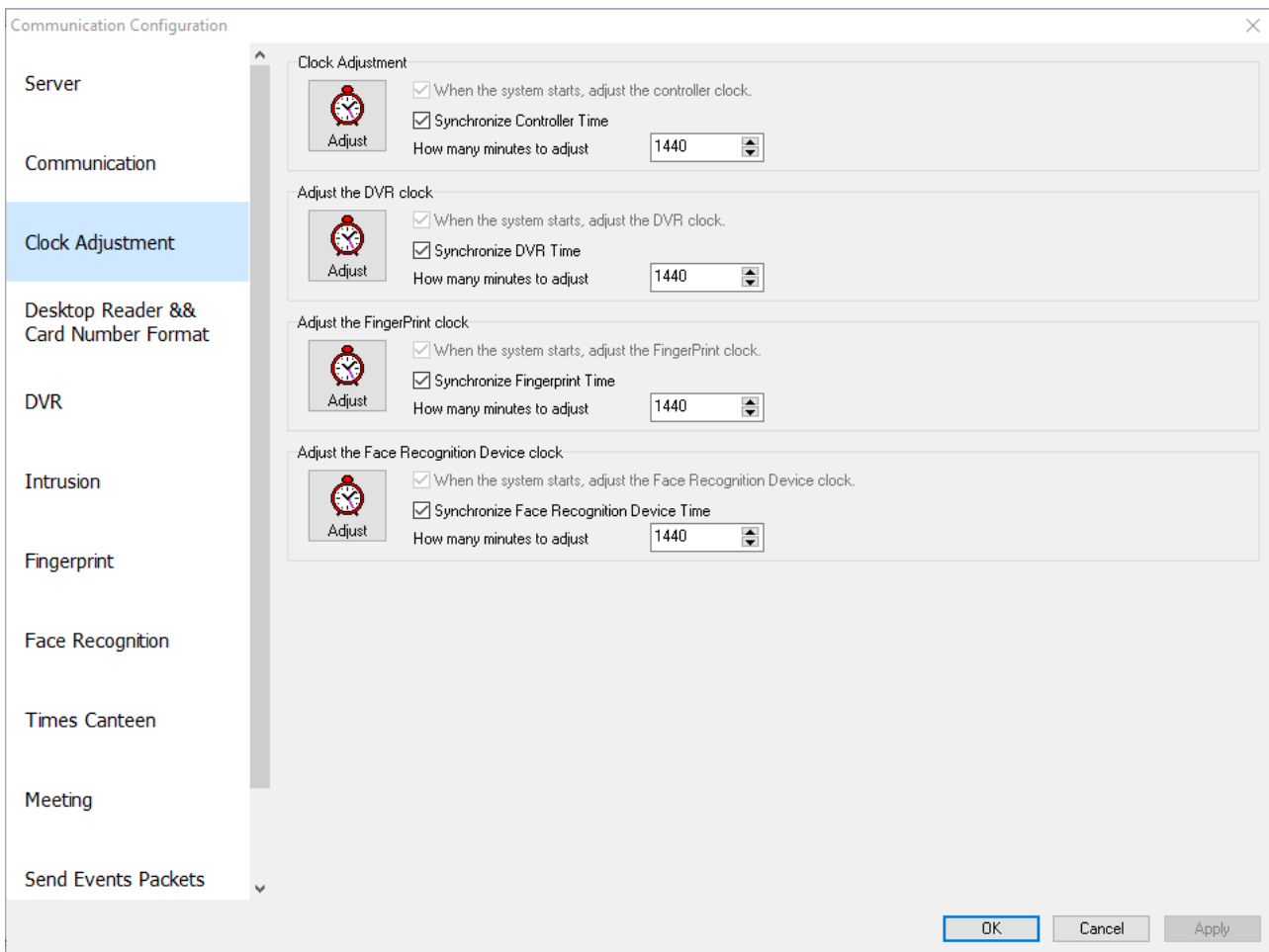
When checked all the panels will share the same group of temp date and holiday. Otherwise you should set up the temp date and holiday for different controller.

Host IP Address: The IP address of the PC which is connected to the TCP/IP panels. Click on the  button to set the correct Host IP address.

Listening Port: The PC port is used for the TCP/IP communication. The default is 8000. After setting the communication parameters click on *OK* to apply the new settings.

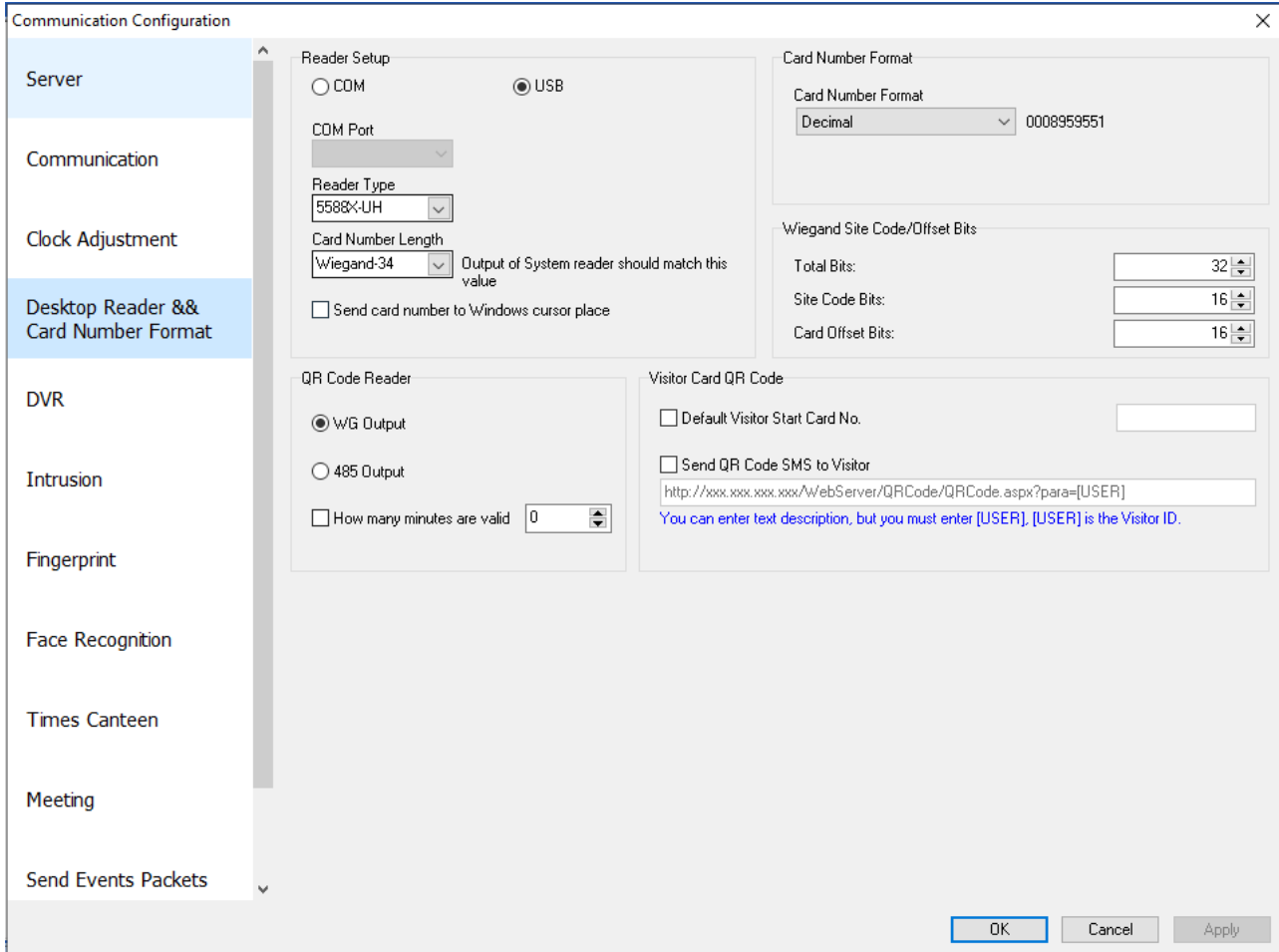
Clock Adjustment Tab

At the *Clock Adjustment* tab, clicking the *Clock Adjustment* button allows the data and time to be synced. It will sync the PC time to the panels and DVRs.



Desktop Reader & Card Number Format Tab

Users can change the number format shown in card events.



Reader Setup: User can select from COM port or USB connection for desktop reader.

Reader Type: This refers to the output type of the desktop reader. The options include HEX, ASCII, WG232, WAR-S08-232, and WAR-S08-ENC.

Card Number Length: option to select WG26 or WG34, has to match the Wiegand setting of the reader

Card Number Format: Displays the card number format.

Decimal: WatchNET Access Software will display the card number as HEX format for example 008959551.

Wiegand: The software will display the card number as Wiegand format for example 136, 46655 (The same card with 0008959551 in Decimal format).

HEX: WAC1 will display the card number as HEX format for example 88863F (The same card with 0008959551 in Decimal format).

DVR Tab

Use this tab to configure DVR's settings.

- **DVR Series:** Select the type or model depending on the DVR/NVR you wanted to connect

- **Connect Timeout**

The DVR will reconnect on the time out period set.

- **Real Play Configuration**

Can choose from Sub Stream or Main Stream when viewing the camera live.

- **Playback Configuration**

Playback Feature includes Throw no frame, throw one B frame and Throw two B frame. Network Feature includes shortest delay mode, the best real time, less latency, more fluency, and the best fluency.

- **DVR Alarm Upload Type**

There are two types of update type which is “Listen” and “Setup Alarm Channel” that allows you to select which type you prefer.

- **DVR Alarm Upload Type**

This allows you to connect also your DVR Alarm if you have one setup.

- **DVR Alarm Listen Type**

Configure the DVR’s IP and port.

- **Capture Picture Quality**

Allows you to select the quality of the picture for snapshots on events

- **Real-time capture time (in seconds)** – Description on the right side

Intrusion Tab – Intrusion tab allows you to modify the time out session for the intrusion panel.

The screenshot shows the 'Communication Configuration' window with the 'Intrusion' tab selected. The window has a title bar with a close button (X) and a menu bar with options: Server, Communication, Clock Adjustment, Desktop Reader & Card Number Format, DVR, Intrusion, Fingerprint, Face Recognition, and Times Cantee. The main content area is divided into three sections:

- Communication Setup:** Contains two spinners: 'Communication Timeout' set to 10000 MSEL and 'Communication Interval' set to 200 MSEL. A checkbox labeled 'Get Prosys status follow counters changed' is checked.
- DSC Listen Setup:** Contains a 'Host IP Address' field with '0.0.0.0' and a 'Port' spinner set to 5010.
- PIMA Listen Setup:** Contains a 'Host IP Address' field with '0.0.0.0' and a 'Port' spinner set to 5010.

At the bottom right, there are three buttons: 'OK', 'Cancel', and 'Apply'.

Fingerprint Tab - There are 5 integrated Fingerprint Readers. Select the Fingerprint Reader that is installed and

click **OK**.

Communication Configuration

Server

Communication

Clock Adjustment

Desktop Reader && Card Number Format

DVR

Intrusion

Fingerprint

Face Recognition

Times Canteen

Meeting

Send Events Packets

Download Configuration for all fingerprint reader manually
 Download Configuration for all fingerprint reader automatically
 Using Fingerprint Change Log

Fingerprint Setup

WAB BEM FCK-S1
 WAB-X:FCK/FCRS/FCKS
 DPU3000W8 Series
 SUPREMA
Timeout: 5000 Milliseconds BioStar2 Listening Port: 51212
 VIRDI
Listen Port: 9870 User ID Length (1..8): 4
UniquelD:
 None
 Personnel Code
 ID Number
Wiegand Out:
 Personnel No.
 Card Number

WatchNET
Host IP Address: 0.0.0.0 Listen Port: 5010
Timeout: 2000 Milliseconds Max Unit ID: 10
Scanner Model:
 WAB BER USB
 WAB BID USB

OK Cancel Apply

Face Recognition Tab - To Configure the Face Device Host IP must be set for the Face device and click OK

Communication Configuration

Server

Communication

Clock Adjustment

Desktop Reader && Card Number Format

DVR

Intrusion

Fingerprint

Face Recognition

Times Canteen

Meeting

Send Events Packets

Face Recognition

WFD-1 NF1500 Listening Port: 7005

WFD-2 Host IP Address: 0.0.0.0 Listening Port: 30000

WFD-3 Host IP Address: 0.0.0.0 Listening Port: 6000

WFD-4 Host IP Address: 192.168.10.212 Listening Port: 8090

WFD-5 Host IP Address: 192.168.10.212 Listening Port: 8899

WFD-6 Host IP Address: 192.168.10.212 Listening Port: 5118

Long Connection

Network Delay Time: 2000 Milliseconds Number of devices managed by each thread: 8

Save face recognition records separate Face Records Save to Access Table

Save captured picture to

Database (Not recommended, will make the dat) Share

Folder C:\Program Files (x86)\WatchNET\WatchNET Access Integrated Security Systems\FaceSnapshots

Recognition Records Color

Succeeded Font Color: clBlack Succeeded Background Color: clWhite

Failed Font Color: clGreen Failed Background Color: clWhite

Download Configuration for all face recognition automatically

Download Configuration for all face recognition manually

Using Face Change Log

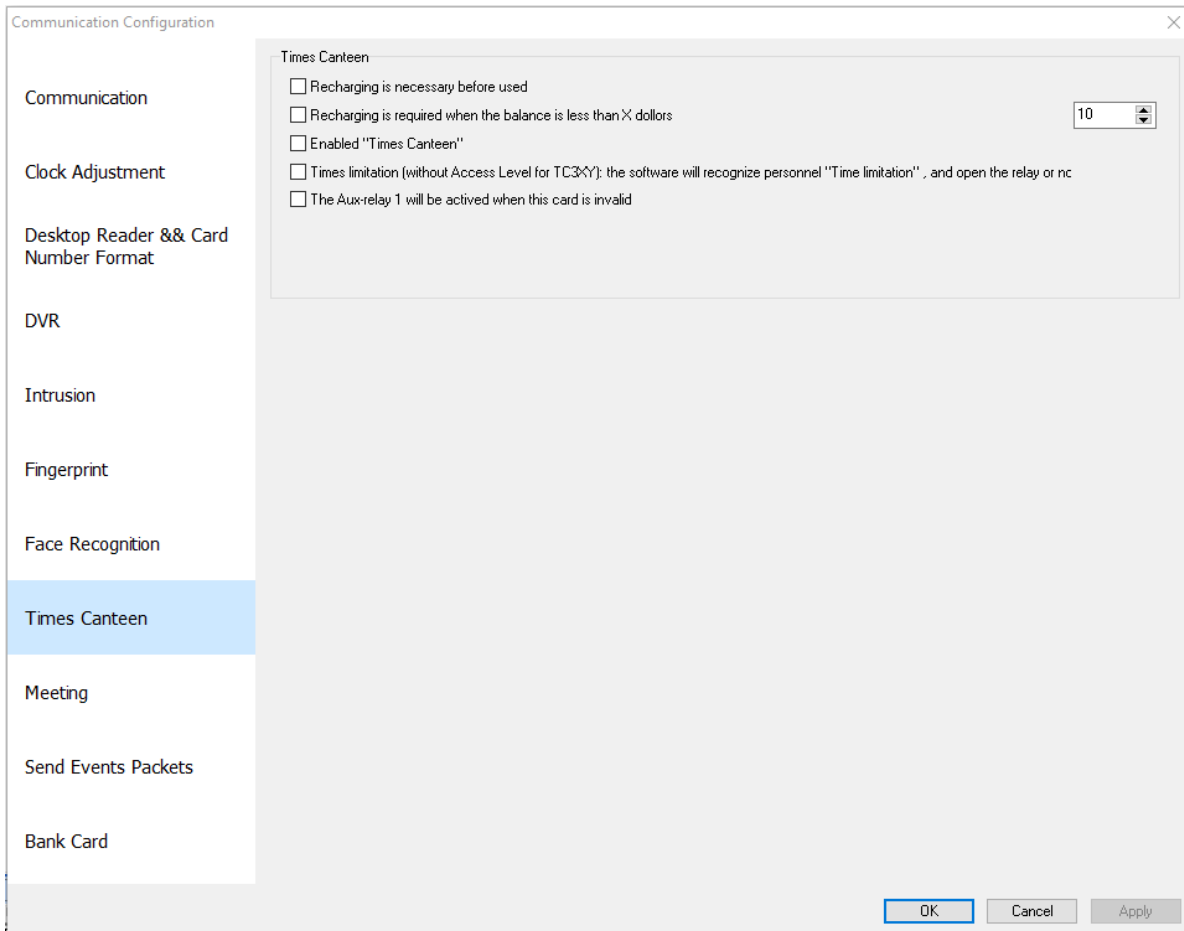
Auto Restart Face Device at 02:00 Every Day

Timing Download Controller Parameters

Time 1: 00:00:00 Time 2: 00:00:00 Time 3: 00:00:00 Time 4: 00:00:00 Time 5: 00:00:00 Time 6: 00:00:00

OK Cancel Apply

Times Canteen Tab - This feature must be enabled to use the Times Canteen Feature



Send Events Packets

This allows to send or export the events into a different server, to configure enter the *"Server name/IP"*

address” & “Server listening Port” of another server you wish to send the events

The screenshot shows a 'Communication Configuration' dialog box with a close button (X) in the top right corner. The 'Send Events Packets' tab is selected, indicated by a double-headed arrow. The dialog contains the following elements:

- Two checkboxes: Send events packets to third-party software events receiving server and Receive set dot status comand from the third-party software eventsreceiving server.
- An 'Events Receive Server Settings' section with a border, containing:
 - A text input field for 'Server name / IP address'.
 - A dropdown menu for 'Server Listening Port' with '12201' selected.
 - A dropdown menu for 'The client communication mode:' with 'Non-Blocking' selected.
- An unchecked checkbox: After get events, send message to third-party software (Message Number 0x0403).
- A 'Message Receive Settings' section with a border, containing:
 - A text input field for 'Receive the message window class name'.
 - A text input field for 'Receive the message window caption name'.
- Buttons for 'OK', 'Cancel', and 'Apply' at the bottom right.

4.10 Area Name

When using the Anti-Pass back feature then we can change the names of the different areas. Clicking *Rename* will allow us to do so.

Area Name

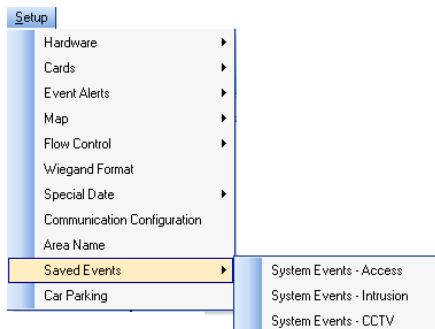
File View

Edit Save Cancel First Prior Next Last Filter Locate Preview Print Export Close

Area ID	Area Name	Total Number	Empty Num	Exit Area Relation	Entry Are
0	Outside	0	0	<input type="checkbox"/>	
1	Inside	0	0	<input type="checkbox"/>	
2	Area 2	0	0	<input type="checkbox"/>	
3	Area 3	0	0	<input type="checkbox"/>	
4	Area 4	0	0	<input type="checkbox"/>	
5	Area 5	0	0	<input type="checkbox"/>	
6	Area 6	0	0	<input type="checkbox"/>	
7	Area 7	0	0	<input type="checkbox"/>	
8	Area 8	0	0	<input type="checkbox"/>	
9	Area 9	0	0	<input type="checkbox"/>	
10	Area 10	0	0	<input type="checkbox"/>	
11	Area 11	0	0	<input type="checkbox"/>	
12	Area 12	0	0	<input type="checkbox"/>	
13	Area 13	0	0	<input type="checkbox"/>	
14	Area 14	0	0	<input type="checkbox"/>	
15	Area 15	0	0	<input type="checkbox"/>	
16	Area 16	0	0	<input type="checkbox"/>	
17	Area 17	0	0	<input type="checkbox"/>	
18	Area 18	0	0	<input type="checkbox"/>	
19	Area 19	0	0	<input type="checkbox"/>	
20	Area 20	0	0	<input type="checkbox"/>	
21	Area 21	0	0	<input type="checkbox"/>	
22	Area 22	0	0	<input type="checkbox"/>	
23	Area 23	0	0	<input type="checkbox"/>	
24	Area 24	0	0	<input type="checkbox"/>	
25	Area 25	0	0	<input type="checkbox"/>	
26	Area 26	0	0	<input type="checkbox"/>	
27	Area 27	0	0	<input type="checkbox"/>	
28	Area 28	0	0	<input type="checkbox"/>	
29	Area 29	0	0	<input type="checkbox"/>	
30	Area 30	0	0	<input type="checkbox"/>	
31	Area 31	0	0	<input type="checkbox"/>	

4.11 Saved Events

Saved Events have three types of System Event: Access, Intrusion and CCTV



This window allows the user to select or deselect any events that are not required to be saved in the memory of controller. By default all events are saved but there may be occasions when certain events are not required to be saved.

System Events - Access

System Events - Access
⏪ — □ ×

Select/Unselect Event

Event Code	Event Name	Saved	Alert	Instructions
<input type="checkbox"/>	169 More than the number of times	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	170 This Card Cannot Consume at The Cur	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	171 Subsidy Request	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	172 Subsidies Success	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	173 Subsidies Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	174 Consumer Correction	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	175 Consumer Correction Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	178 Transfer Success	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	179 Transfer Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	180 Valid Card Break In	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	181 Valid Card Break Out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	182 Valid Fingerprint Break In	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	183 Valid Fingerprint Break Out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	184 Valid Card + Fingerprint Break In	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	185 Valid Card + Fingerprint Break Out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	186 Valid PIN + Fingerprint Break In	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	187 Valid PIN + Fingerprint Break Out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	188 Card + PIN Break In	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	189 Card + PIN Break Out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	200 Hardware Short Circuit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	201 Bank card open door	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	202 Clear Subsidy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	203 Valid QR Code of Tencent Weixiao	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	204 Invalid QR Code of Tencent Weixiao	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	250 Duress Finger Used	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	254 Connected	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	255 Connection Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Select All
Unselect All
OK
Cancel
Apply

System Events – Prosys

System Events - Intrusion

Select/Unselect Event

Code	Type	Event Name	Saved	Alert	Instructions
1	Prosys Panel	FireKey Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Prosys Panel	FireKey Restore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Prosys Panel	AmbulanceKey Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Prosys Panel	AmbulanceKey Restore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Prosys Panel	PoliceKey Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Prosys Panel	PoliceKey Restore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Prosys Panel	Auxiliary Input Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Prosys Panel	Auxiliary Input Alarm Restored	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Prosys Panel	Panel Battery Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Prosys Panel	Panel Battery Trouble Restore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Prosys Panel	Panel AC Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Prosys Panel	Panel AC Restore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
13	Prosys Panel	System Bell Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
14	Prosys Panel	System Bell Trouble Restore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
15	Prosys Panel	TLM Line1 Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
16	Prosys Panel	TLM Line1 TroubleRestore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
17	Prosys Panel	TLM Line2 Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
18	Prosys Panel	TLM Line2 TroubleRestore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
19	Prosys Panel	FTC Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
21	Prosys Panel	Wireless Key Low Battery Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
22	Prosys Panel	Wireless Key Low Battery Trouble Res	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
23	Prosys Panel	Handheld Keypad Low Battery Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
24	Prosys Panel	Handheld Keypad Low Battery Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
25	Prosys Panel	General System Tamper	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
26	Prosys Panel	General System Tamper Restore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
27	Prosys Panel	Home Automation Trouble	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
28	Prosys Panel	Home Automation Trouble Restore	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Select All Unselect All OK Cancel Apply

System Events – DSC – Same as Prosys

System Events – PIMA - Same as Prosys

System Events - CCTV

System Events - CCTV					
Select/Unselect Event					
Event Code	Type	Event Name	Saved	Alert	Instructions
0	Alarm	Input Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1	Alarm	HDD is Full	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Alarm	The Video Signal Lost	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Alarm	Motion Detection	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Alarm	HDD Not Formatted	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Alarm	Failed to Read And Write HDD	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Alarm	Video Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Alarm	Input and Output Bideo Standard Mism	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Alarm	Illegal Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Alarm	Serial Port State	<input type="checkbox"/>	<input type="checkbox"/>	
10	Alarm	GPS Location Information	<input type="checkbox"/>	<input type="checkbox"/>	
254	Exception	Connected	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
255	Exception	Connection Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32768	Exception	Exception Exchange	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32769	Exception	Exception Audio Exchange	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32770	Exception	Exception Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32771	Exception	Exception Preview	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32772	Exception	Exception Serial	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32773	Exception	Exception Reconnect	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32774	Exception	Exception Alarm Reconnect	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32775	Exception	Exception Serial Reconnect	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32784	Exception	Exception Play Back	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
32785	Exception	Exception DISK FMT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Select All Unselect All **OK** Cancel Apply

4.12 Car Parking

Control a parking lot by counting the number of cars entering and leaving while limiting the maximum number. Once the maximum number is reached an Output will be activated. This feature requires WatchNET Access Software run all the time.

Car Parking Settings

Enable Car Parking Function

Entry Door/Gate

Controller

Door

Exit Door/Gate

Controller

Door

Counter

Maximum Number of Cars

0

Current Number of Cars

0

Parking Full Output Action

Controller

Output

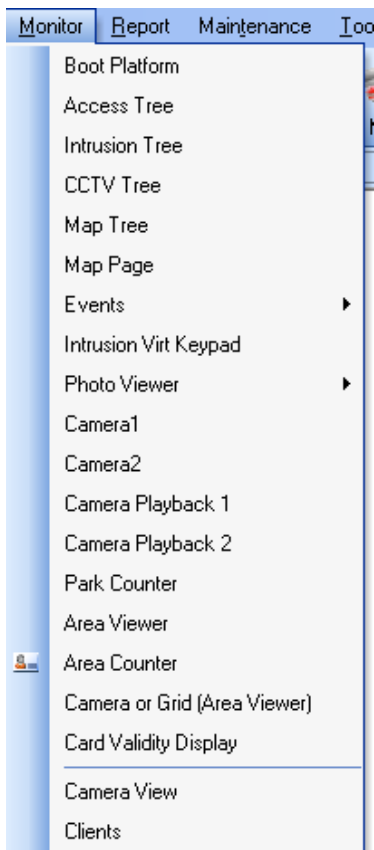
Deny Access When Full

OK Cancel

The example above shows that cars will be entered the parking lot through Door 1(001) of Controller 001. Maximum number of cars allowed is 5 while currently there are 2 cars in the parking lot. The cars are leaving through Door 2(001) of Controller 001. If the Car Park has reached the max capacity then you have a choice of outputs that can be activated. This can turn on a red traffic light and/or close the Main Entrance gate.

Chapter 5 Monitor

This section allows the user to choose what they want on the window. This could vary from operator to operator depending on the role they play in the organizations security needs. Clicking on the *Access Tree* will launch a tab on the left hand side of the window. Clicking on the tree again will make it disappear. If the operator just needs to access it temporarily then all he has to do is to move the mouse over the tab and the tree will slide in to the view. If he needs to lock it for viewing it permanently then he should click on the pin which locks it in place.



5.1 Boot Platform

The *Boot Platform* allows you to display and open shortcut items, see below image



5.2 Access Tree

The *Access Tree* displays all the panels their components on the system. You can operate the devices connected to the panel by right clicking on it and performing the required actions. If the controller is offline then you will see a red X mark.

5.3 Intrusion Tree

Same concepts as the *Access Tree*, this displays all the intrusion panels and their components such as Zone, Partitions, and status of each.

5.4 CCTV Tree

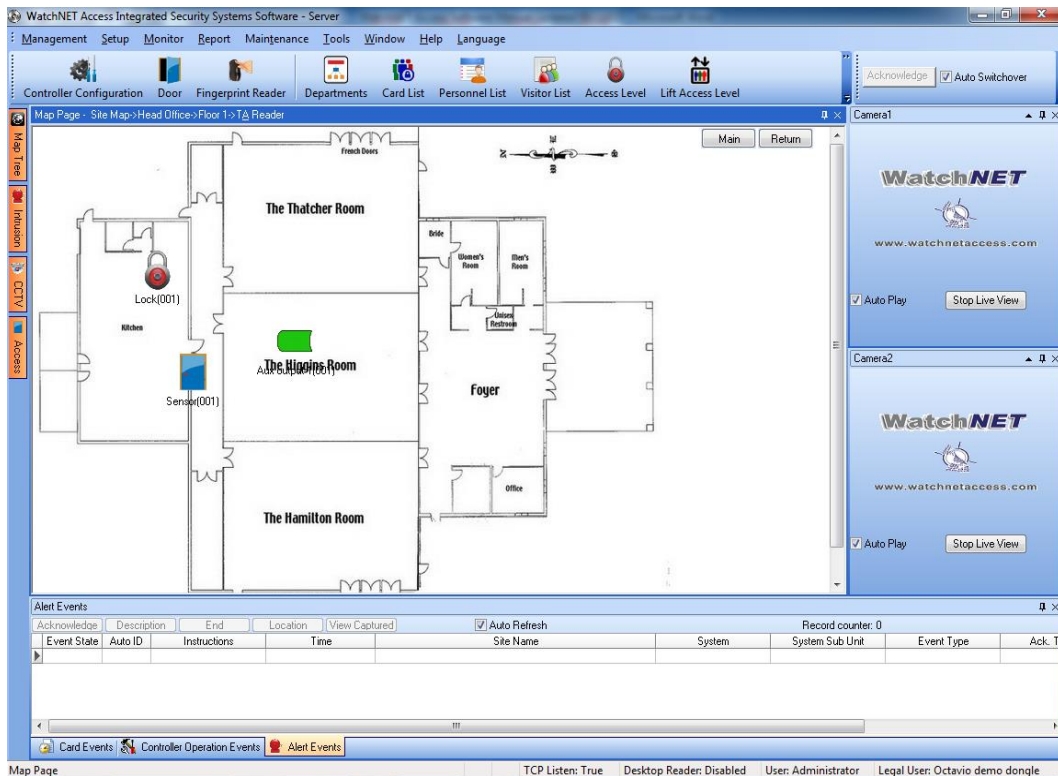
CCTV Tree displays all the DVR and the Camera that are connected to the system.

5.5 Map Tree

Allows you to open and close Map Tree on the left side

5.6 Map Page

If you want to design a map then refer to 8.4. Double Click on the map name in the map tree to launch the map page window.



Main: Click the button to go to the *Main map*.

Return: Click the button to go to the prior map.

Acknowledge: If the WatchNET Access Software receives alert event then the button flashes to remind you to acknowledge the event.

Auto Switch over: When checked the map will switch automatically when an event relating to the map occurs.

5.7 Events

The Events Monitor presents all the Events divided into 11 categories: Alert Events, Card Events, Face Recognition Records, Bank Card Events, Controller Operation Events, Area Changed Events, Intrusion Events, Intrusion System Status, CCTV Events, Canteen Records and System Log. The Area Changed events are created only if we activate the Anti-Pass back. We can see all events information. Double clicking on an event will open the relevant *Personnel Information* as described in Section 8.2.2. It allows the user to change the information or even enroll a new card and personnel to WatchNET Access Software.

5.8 Intrusion Virt keypad – This will display a virtual DSC Keypad for arming and disarming the alarm

system from the software.

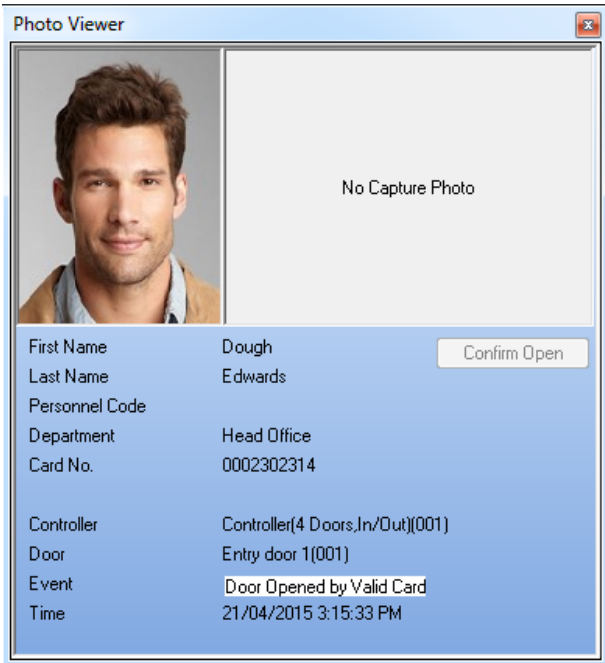


5.9 Photo Viewer

This shows the details for the card holder with the phone. For example their badge picture as well as a snapshot from a camera and has 6 different views.

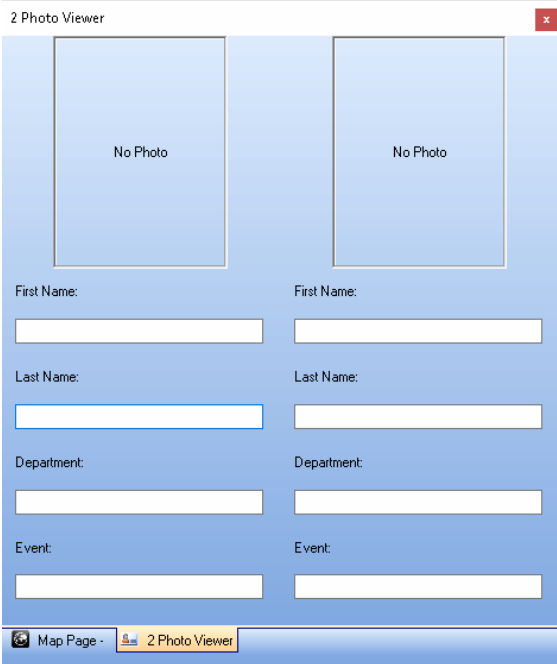
- **1 Photo Viewer**

This will open *Single Photo Viewer* window as indicated in the picture below and displays the Photo and credential of the card holder, also shows a snapshots of the event if a camera is connected



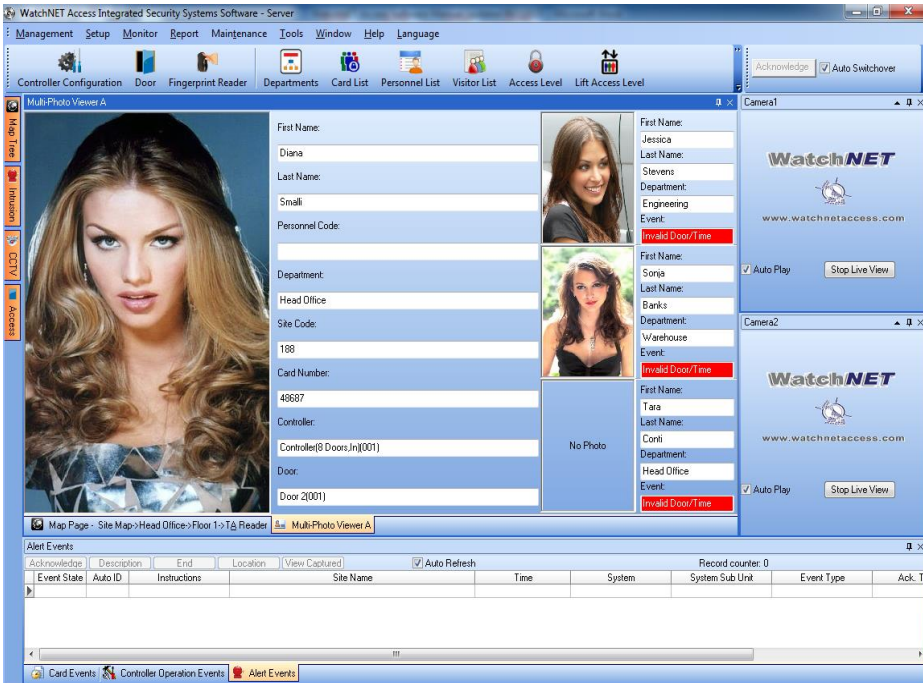
- **2 Photo Viewer**

This opens 2 photo viewers, two transactions.



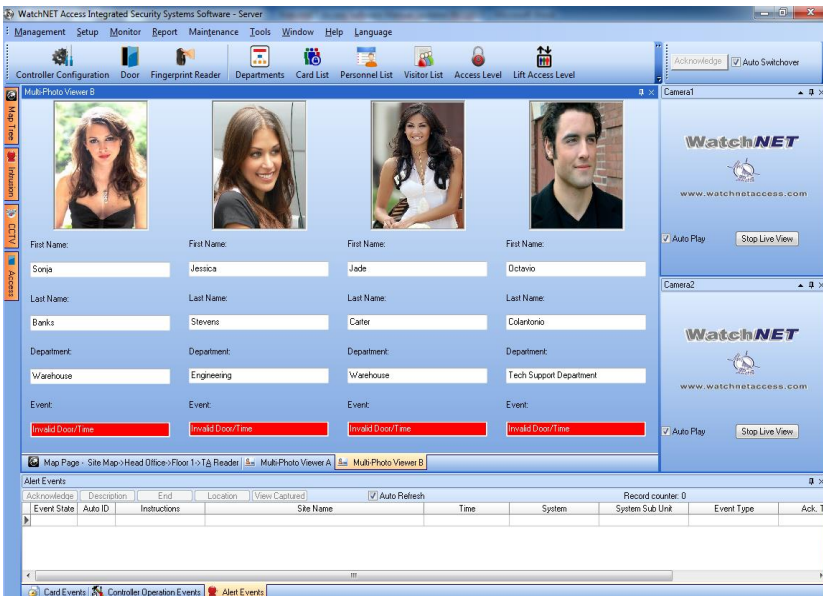
- **4 Photo Viewer A**

This opens 4 photos at the same time.



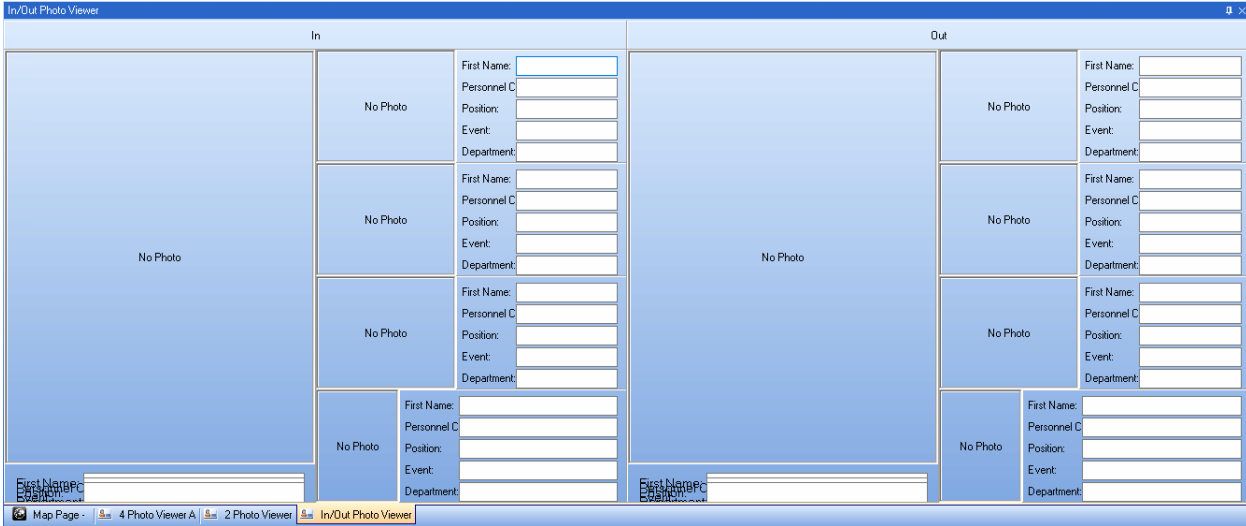
- **4 Photo Viewer B**

This will open *Multi-Photo Viewer B* window as indicated in the picture below. The latest entry is displayed in the left hand side slot picture area whereas the previous ones move to the right hand side.



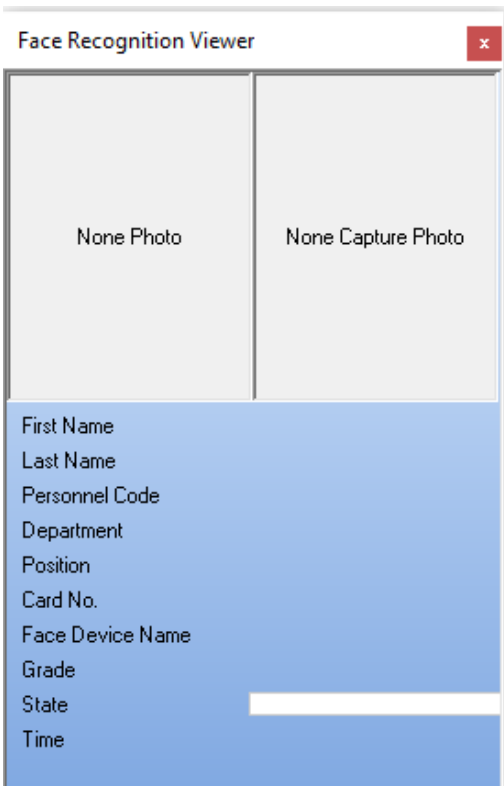
- **In/Out Photo Viewer**

This opens the view for area where it the personnel coming in and out of a building.



- **Face Recognition Viewer**

This will open a new window that monitors the face recognition device events.



5.10 Camera 1

Camera 1 allows you to view one camera only on the live view

5.11 Camera 2

Camera 2 allows you to view one camera only on the live view

5.12 Camera Playback 1

Opens/close the camera playback window on the right side.

5.13 Camera Playback 2

Opens/close the camera playback window on the right side.

5.14 Park Counter

Click *Monitor-> Park Counter* and this will open the *Park Counter* window. See Figure 8-6



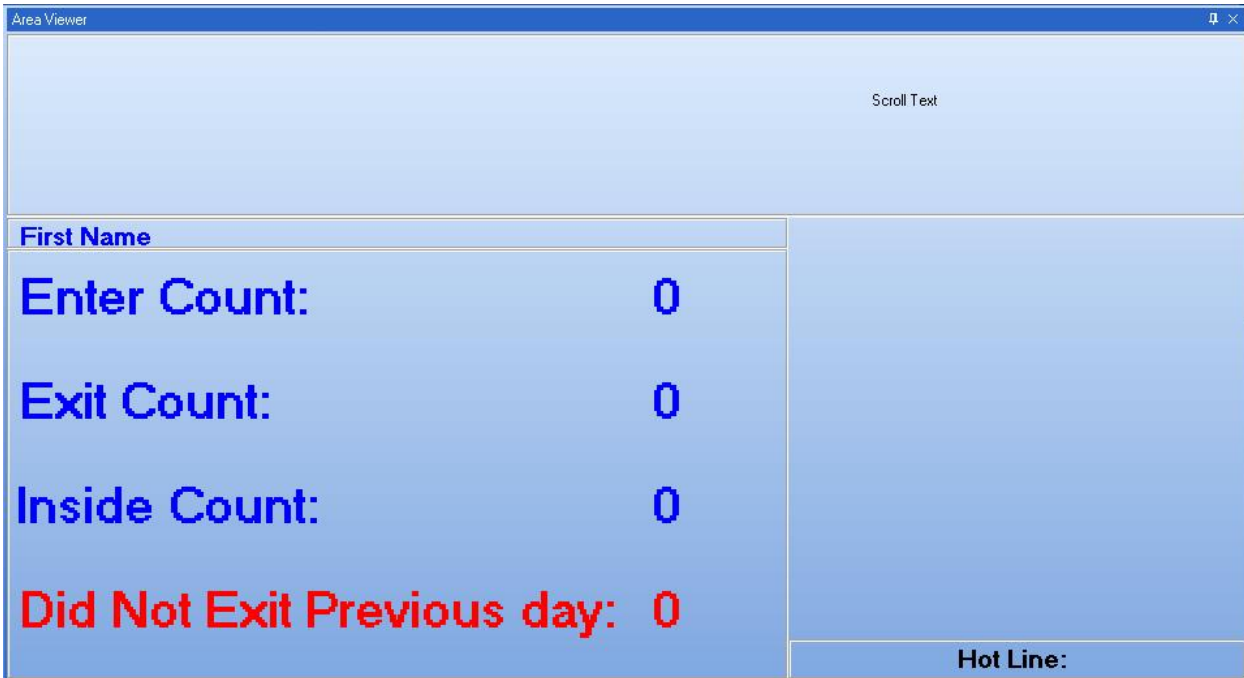
5.15 Area Viewer

This real time event viewer shows the record count for a door or building and displays how many personnel are inside or outside.

Scroll Text

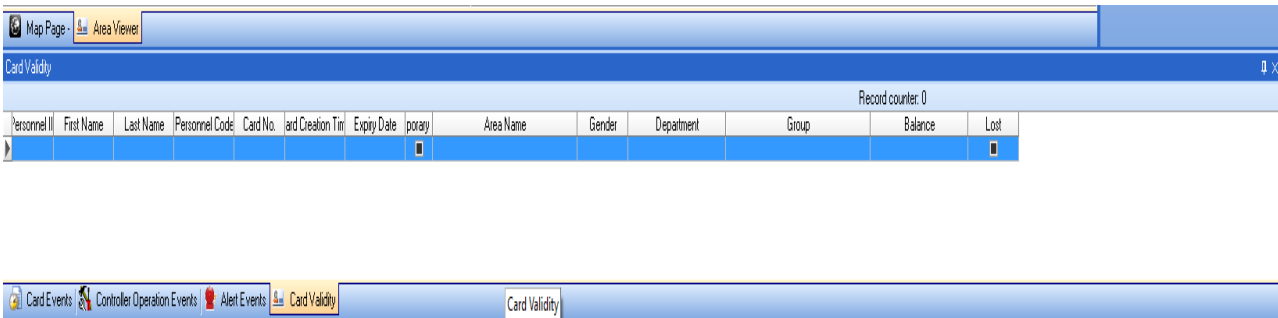
First Name	Area Personnel In					Record counter: 0	
	Personnel ID	First Name	Last Name	Personnel Code	Card No.	Update Card Time	Las
Enter Count:							0
Exit Count:							0
Inside Count:							0
Did Not Exit Previous day:							0
Hot Line:							

5.16 Camera or Grid (Area Viewer) – If enabled, instead of grid view on area viewer it will display photos



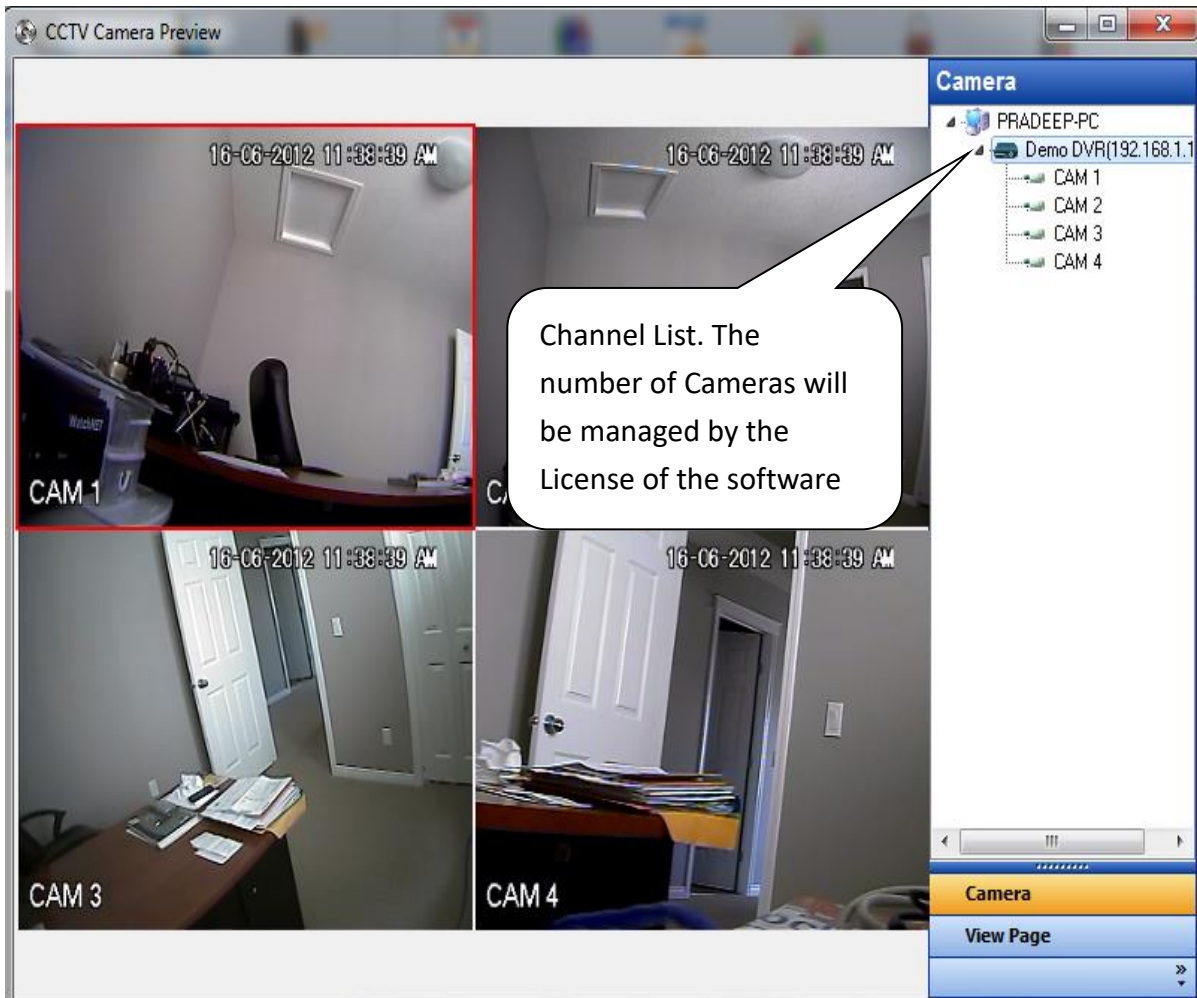
5.17 Card Validity Display

This real time event viewer allows you to monitor a card that is expiring or expired.



5.18 Camera View

Click *Monitor-> Camera Viewer* and the will CCTV Camera Preview window open.



5.19 Clients

Shows the WatchNET Access Software Clients which are currently connected to WatchNET Access Software Server.

Clients					
Client	Application Name	User	Login Time	The Last Time	

Chapter 6 Report

All type of reports listed below

Report	Maintenance	Tools	Windo
All Cards Events			
Quick Query Cards Events			
Cards Events Filter			
All Hardware Events			
Face Recognition Records			
Bank Card Events			
Area Report			
Personnel Area Report			
Area Changed Report			
Personnel In/Out Reports			▶
Access Level Report			
Access Security Group Report			
Time Attendance			
Times Canteen Report			▶
All Intrusion Events			
All Intrusion System Status			
All CCTV Events			
All Alert Events			
Alert Events Filter			
System Log			

6.1 All Cards Events

Generate reports with all the cards events.

Auto ID	Time	Event Name	Site Name	Line ID	Controller ID	Controller Name	Door ID	Door Name	Site Code	Card Number	Department	Personnel
877	11/21/2013 3:48:59 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	12	48852	Warehouse	40
876	11/21/2013 3:48:51 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	188	48685	Engineering	9
875	11/21/2013 3:48:42 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	225	34682	Warehouse	16
874	11/21/2013 3:48:34 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	225	36820	Tech Support Department	8
873	11/21/2013 3:48:13 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	12	48513	Head Office	41
872	11/21/2013 3:48:09 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	12	48852	Warehouse	40
871	11/21/2013 3:48:05 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	188	48685	Engineering	9
870	11/21/2013 3:48:02 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	188	48687	Head Office	19
869	11/21/2013 3:45:28 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	188	48687	Head Office	19
868	11/21/2013 3:45:24 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	188	48685	Engineering	9
867	11/21/2013 3:45:19 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	12	48852	Warehouse	40
866	11/21/2013 3:45:15 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	12	48513	Head Office	41
865	11/21/2013 3:45:11 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	225	36820	Tech Support Department	8
864	11/21/2013 3:45:05 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	225	34682	Warehouse	16
863	11/21/2013 3:45:01 PM	Invalid Card	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	13	26351		0
862	11/21/2013 3:40:57 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	225	54530	Tech Support Department	2
861	11/21/2013 3:40:53 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	226	888	Tech Support Department	3
860	11/21/2013 3:40:50 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	77	55714	Tech Support Department	1
859	11/21/2013 3:40:43 PM	Invalid Card	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	13	22237		0
858	11/21/2013 3:40:01 PM	Invalid Card	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	13	26351		0
857	11/21/2013 3:39:57 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	225	34682	Warehouse	16
856	11/21/2013 3:39:54 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	225	36820	Tech Support Department	8
855	11/21/2013 3:39:49 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	2	Door 2(001)	12	48513	Head Office	41
854	11/21/2013 3:39:44 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	6	Door 6(001)	12	48852	Warehouse	40
853	11/21/2013 3:39:36 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	6	Door 6(001)	188	48685	Engineering	9
852	11/21/2013 3:39:30 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)	6	Door 6(001)	188	48687	Head Office	19
851	11/21/2013 1:42:25 PM	Invalid Door/Time	WatchnetAccess Group	1	1	Controller(2 Doors.In)(001)	2	Door 2(001)	0	1234	Tech Support Department	30
850	11/21/2013 1:42:21 PM	Valid Card	WatchnetAccess Group	1	1	Controller(2 Doors.In)(001)	2	Door 2(001)	0	1	Tech Support Department	34
849	11/21/2013 11:15:51 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
848	11/21/2013 11:15:50 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
847	11/21/2013 11:15:50 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
846	11/21/2013 11:15:49 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
845	11/21/2013 11:15:48 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
844	11/21/2013 11:15:47 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
843	11/21/2013 11:14:19 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
842	11/21/2013 11:14:18 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
841	11/21/2013 11:14:14 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
840	11/21/2013 11:14:13 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
839	11/21/2013 11:14:12 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
838	11/21/2013 11:14:11 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16
837	11/21/2013 11:14:10 AM	Invalid Door/Time	WatchnetAccess Group	7	1	T & A controller(001)	1	Entry door(001)	81	20493	Warehouse	16

In the View menu we can use a *Filter* to search for certain records and we can export the report to an MS-Excel file and we can show it in a preview mode so it will be suitable for printing.

Records can be Filtered or Located.

Clicking on the *Filter* in View menu brings up the *Filter* window. To locate a record click on the field that you wish to search by and then enter a *starting date* and an *ending date* then click *OK*. Any records that exist conforming with your search criteria will be listed.

The screenshot shows a 'Filter' dialog box. On the left, a list of fields includes 'Controller ID', which is highlighted in blue. Below the list are buttons for 'All' and 'Searched', and radio buttons for 'Fields Order' set to 'Logical'. On the right, the 'Controller ID' section has 'Starting Range' and 'Ending Range' input fields, each with a 'Clear' button. At the bottom right are 'OK' and 'Cancel' buttons, and at the bottom center are 'View Summary' and 'New Search' buttons.

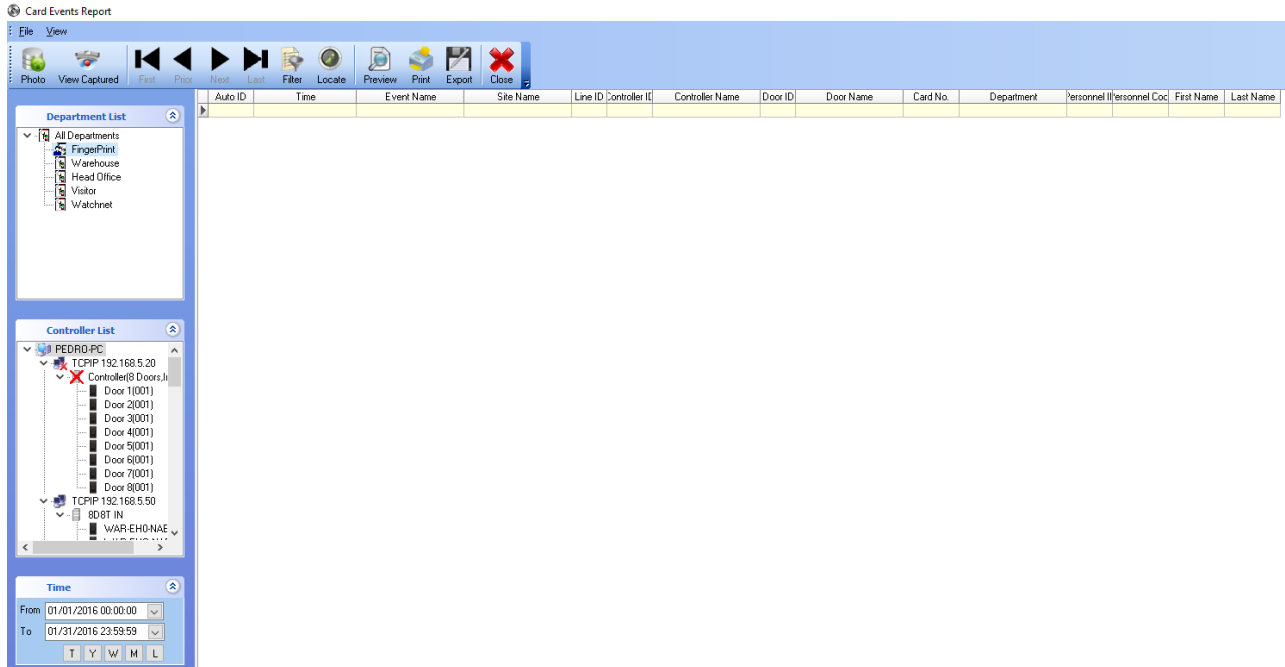
This screenshot shows the 'Filter' dialog box with 'Time' selected in the fields list. The 'Starting Range' and 'Ending Range' dropdown menus are populated with the date '11/17/2011'. The 'OK' button is highlighted in blue. The rest of the interface, including the 'Fields Order' and search options, remains the same as in the previous screenshot.

A record can be searched for a particular value. Click on *Locate* in View menu and the Locate window will display. Clicking on the drop down box under the *Fields* label will list the fields on which a search can be made. Enter your data and check the required boxes then click *First* to find the 1st entry conforming to the data then *Next* to find any subsequent matches.

The 'Locate Value' dialog box features a 'Fields' dropdown menu at the top. Below it is a 'Field Value' text input field. The 'Search Type' section includes a 'Case-sensitive' checkbox and three radio buttons: 'Exact Match', 'Partial Match at Beginning' (which is selected), and 'Partial Match Anywhere'. At the bottom, there are 'First', 'Next', and 'Cancel' buttons.

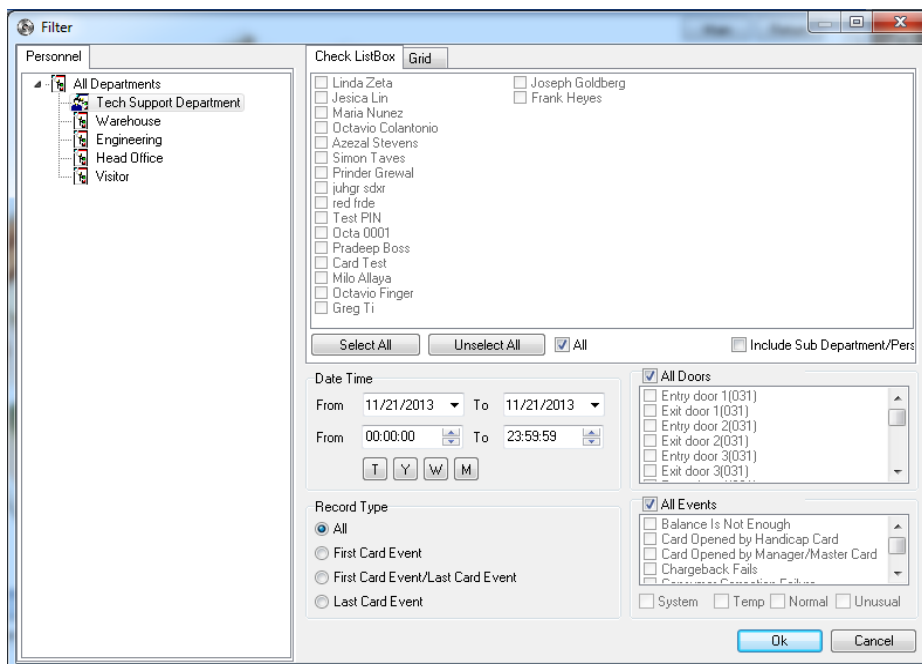
6.2 Quick Query Card Events

Run and view card events via departments or via door card events



6.3 Cards Events Filter

We can run different queries to get specific events records regarding different personnel, departments events etc. Similarly to 10.1 the *View* menu allows us to export the result to an MS-Excel file or previewing it in a printable mode.



Preview - Query Result

Print Stop Page Setup Scale Previous Page Next Page Close

Octavio demo dongle 1

Query Result

Auto ID	Time	Event Name	Site Name	Line ID	Controller ID	Controller Name
874	11/21/2013 3:48:34 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)
865	11/21/2013 3:45:11 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)
862	11/21/2013 3:40:57 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)
861	11/21/2013 3:40:53 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)
860	11/21/2013 3:40:50 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)
856	11/21/2013 3:39:54 PM	Invalid Door/Time	WatchnetAccess Group	3	1	Controller(8 Doors.In)(001)
851	11/21/2013 1:42:25 PM	Invalid Door/Time	WatchnetAccess Group	1	1	Controller(2 Doors.In)(001)
850	11/21/2013 1:42:21 PM	Valid Card	WatchnetAccess Group	1	1	Controller(2 Doors.In)(001)
836	11/21/2013 8:49:46 AM	Valid Card	WatchnetAccess Group	1	1	Controller(2 Doors.In)(001)
835	11/21/2013 8:49:30 AM	Invalid Door/Time	WatchnetAccess Group	1	1	Controller(2 Doors.In)(001)
834	11/21/2013 8:48:08 AM	Invalid Door/Time	WatchnetAccess Group	1	1	Controller(2 Doors.In)(001)

6.4 All Hardware Events

This report will display all the hardware events. In the View menu we will find the Filter to search and find certain records only such as the *Locate Value* for a certain value and select the Fields to be presented and Preview in a printable mode.

Hardware Events Report

File View

Hardware Events Filter View Captured Delete Record First Page Prior Page First Prior Page Size Next Next Page Last Page Filter Locate Preview Print Export

Auto ID	Time	Event Code	Event Name	Status	Ack. Time	Acked By	Description	End Time	Ended By	Site Name	Line
45126	11/21/2013 3:40:41 PM	23	Lock Closed	V						WatchnetAccess Group	
45125	11/21/2013 3:40:41 PM	115	Hardware Trouble	V						WatchnetAccess Group	
45124	11/21/2013 3:40:41 PM	69	Exit Button Release	V						WatchnetAccess Group	
45123	11/21/2013 3:40:40 PM	23	Lock Closed	V						WatchnetAccess Group	
45122	11/21/2013 3:40:38 PM	23	Lock Closed	V						WatchnetAccess Group	
45121	11/21/2013 3:40:36 PM	22	Lock Opened	V						WatchnetAccess Group	
45120	11/21/2013 3:40:36 PM	21	Exit Button Action	V						WatchnetAccess Group	
45119	11/21/2013 3:40:35 PM	22	Lock Opened	V						WatchnetAccess Group	
45118	11/21/2013 3:40:34 PM	23	Lock Closed	V						WatchnetAccess Group	
45117	11/21/2013 3:40:34 PM	115	Hardware Trouble	V						WatchnetAccess Group	
45116	11/21/2013 3:40:34 PM	69	Exit Button Release	V						WatchnetAccess Group	
45115	11/21/2013 3:40:34 PM	23	Lock Closed	V						WatchnetAccess Group	
45114	11/21/2013 3:40:31 PM	22	Lock Opened	V						WatchnetAccess Group	
45113	11/21/2013 3:40:29 PM	22	Lock Opened	V						WatchnetAccess Group	
45112	11/21/2013 3:40:29 PM	21	Exit Button Action	V						WatchnetAccess Group	
45111	11/21/2013 3:40:29 PM	22	Lock Opened	V						WatchnetAccess Group	
45110	11/21/2013 3:40:29 PM	23	Lock Closed	V						WatchnetAccess Group	
45109	11/21/2013 3:40:29 PM	115	Hardware Trouble	V						WatchnetAccess Group	
45108	11/21/2013 3:40:29 PM	69	Exit Button Release	V						WatchnetAccess Group	
45107	11/21/2013 3:40:28 PM	23	Lock Closed	V						WatchnetAccess Group	
45106	11/21/2013 3:40:24 PM	22	Lock Opened	V						WatchnetAccess Group	
45105	11/21/2013 3:40:24 PM	21	Exit Button Action	V						WatchnetAccess Group	
45104	11/21/2013 3:40:24 PM	22	Lock Opened	V						WatchnetAccess Group	
45103	11/21/2013 3:40:24 PM	115	Hardware Trouble	V						WatchnetAccess Group	
45102	11/21/2013 3:40:24 PM	69	Exit Button Release	V						WatchnetAccess Group	
45101	11/21/2013 3:40:23 PM	23	Lock Closed	V						WatchnetAccess Group	
45100	11/21/2013 3:40:19 PM	23	Lock Closed	V						WatchnetAccess Group	
45099	11/21/2013 3:40:14 PM	22	Lock Opened	V						WatchnetAccess Group	
45098	11/21/2013 3:40:14 PM	21	Exit Button Action	V						WatchnetAccess Group	
45097	11/21/2013 3:40:14 PM	22	Lock Opened	V						WatchnetAccess Group	
45096	11/21/2013 1:42:26 PM	23	Lock Closed	V						WatchnetAccess Group	
45095	11/21/2013 1:42:21 PM	22	Lock Opened	V						WatchnetAccess Group	
45094	11/21/2013 1:24:56 PM	254	Connected	V						WatchnetAccess Group	
45093	11/21/2013 1:24:56 PM	255	Connection Failure	!						WatchnetAccess Group	
45092	11/21/2013 1:24:22 PM	254	Connected	V						WatchnetAccess Group	
45091	11/21/2013 1:24:21 PM	255	Connection Failure	!						WatchnetAccess Group	
45090	11/21/2013 12:00:08 PM	254	Connected	V						WatchnetAccess Group	
45089	11/21/2013 12:00:05 PM	255	Connection Failure	!						WatchnetAccess Group	
45088	11/21/2013 11:44:15 AM	23	Lock Closed	V						WatchnetAccess Group	
45087	11/21/2013 11:44:10 AM	69	Exit Button Release	V						WatchnetAccess Group	
45086	11/21/2013 11:44:10 AM	22	Lock Opened	V						WatchnetAccess Group	

Preview - Hardware Events Report

Print Stop Page Setup Scale Previous Page Next Page Close

Octavo demo dangle 1

Hardware Events Report

Auto ID	Time	Event Code	Event Name	Status	Ack. Time	Acked By
45126	11/21/2013 3:40:41 PM	23	Lock Closed	V		
45125	11/21/2013 3:40:41 PM	115	Hardware Trouble	V		
45124	11/21/2013 3:40:41 PM	69	Exit Button Release	V		
45123	11/21/2013 3:40:40 PM	23	Lock Closed	V		
45122	11/21/2013 3:40:36 PM	23	Lock Closed	V		
45121	11/21/2013 3:40:36 PM	22	Lock Opened	V		
45120	11/21/2013 3:40:36 PM	21	Exit Button Action	V		
45119	11/21/2013 3:40:35 PM	22	Lock Opened	V		
45118	11/21/2013 3:40:34 PM	23	Lock Closed	V		
45117	11/21/2013 3:40:34 PM	115	Hardware Trouble	V		
45116	11/21/2013 3:40:34 PM	69	Exit Button Release	V		
45115	11/21/2013 3:40:34 PM	23	Lock Closed	V		
45114	11/21/2013 3:40:31 PM	22	Lock Opened	V		
45113	11/21/2013 3:40:29 PM	22	Lock Opened	V		
45112	11/21/2013 3:40:29 PM	21	Exit Button Action	V		
45111	11/21/2013 3:40:29 PM	22	Lock Opened	V		
45110	11/21/2013 3:40:29 PM	23	Lock Closed	V		
45109	11/21/2013 3:40:29 PM	115	Hardware Trouble	V		
45108	11/21/2013 3:40:29 PM	69	Exit Button Release	V		
45107	11/21/2013 3:40:28 PM	23	Lock Closed	V		
45106	11/21/2013 3:40:24 PM	22	Lock Opened	V		
45105	11/21/2013 3:40:24 PM	21	Exit Button Action	V		
45104	11/21/2013 3:40:24 PM	22	Lock Opened	V		

6.5 Face Recognition Records

View Captured Face device records

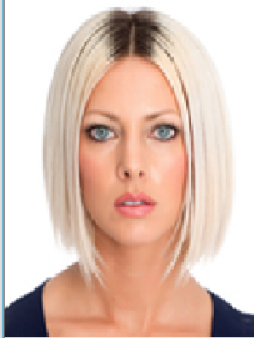
Face Recognition Records

File View

Photo First Page Prior Page First Prior Page Size Next Last Next Page Last Page Filter Locate Preview Print Export Close

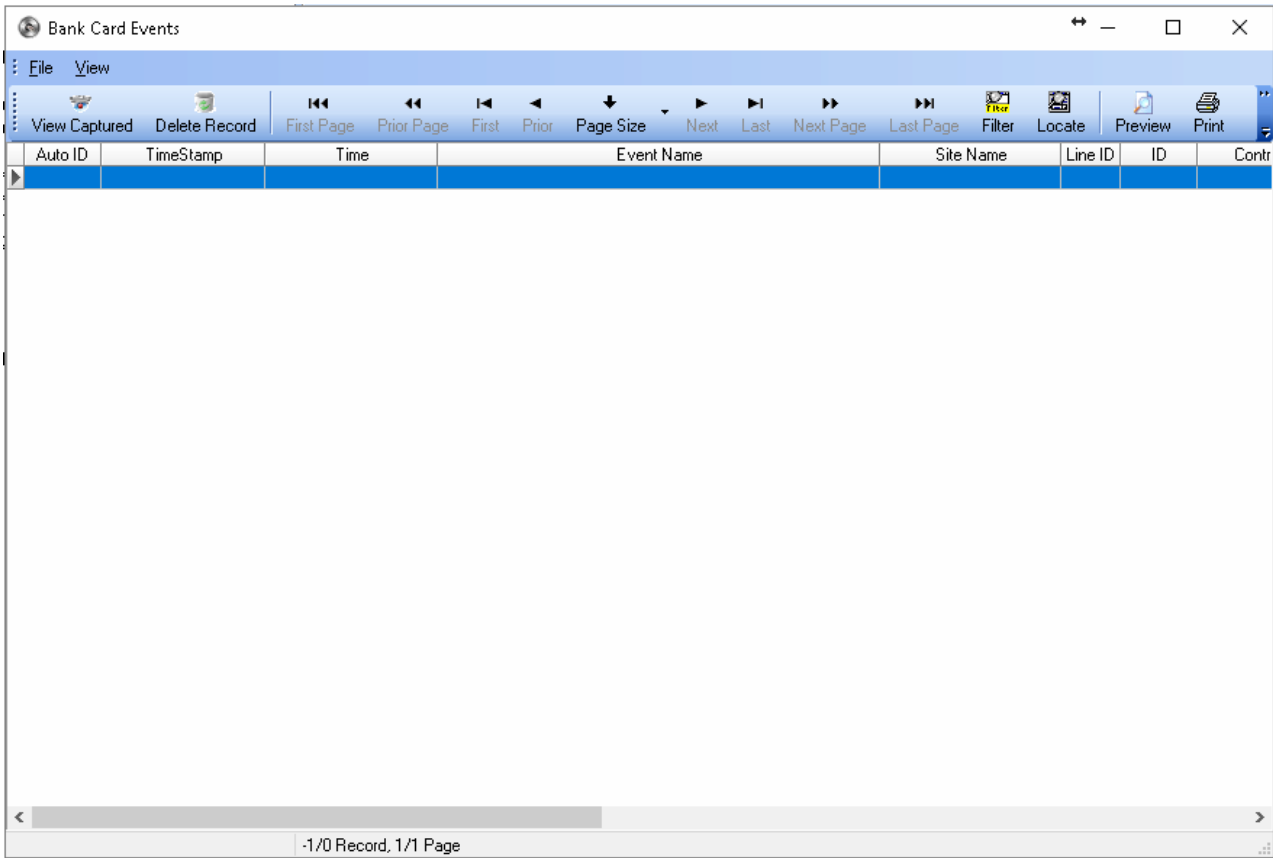
Auto ID	Time	Device Name	Card No.	Department	Personnel ID/Personnel Coc	First Name	Last Name
72	4/3/2015 12:07:27 AM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
71	4/3/2015 12:07:18 AM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
70	4/3/2015 12:07:14 AM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
69	4/3/2015 12:10:43 AM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
68	4/3/2015 12:07:27 AM	Face Recognition Device			0		
67	4/3/2015 12:07:18 AM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
66	4/3/2015 12:07:14 AM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
65	3/25/2015 4:29:10 AM	Face Recognition Device			0		
64	3/25/2015 4:29:01 AM	Face Recognition Device			0		
63	3/25/2015 4:29:10 AM	Face Recognition Device			0		
62	3/25/2015 4:29:01 AM	Face Recognition Device			0		
61	3/11/2015 11:20:01 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
60	3/11/2015 11:19:09 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
59	3/11/2015 11:18:44 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
58	3/11/2015 11:18:08 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
57	3/11/2015 11:20:01 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
56	3/11/2015 11:19:09 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
55	3/11/2015 11:18:44 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
54	3/11/2015 11:18:08 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
53	2/28/2015 5:58:03 AM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
52	2/28/2015 5:58:03 AM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
51	2/13/2015 12:47:24 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
50	2/13/2015 12:46:24 PM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
49	2/13/2015 12:46:23 PM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
48	2/13/2015 12:46:18 PM	Face Recognition Device 0013482062	FingerPrint		521	Peter	Punzalan
47	2/13/2015 12:45:44 PM	Face Recognition Device			0		
46	2/13/2015 12:45:07 PM	Face Recognition Device			0		
45	2/13/2015 12:45:00 PM	Face Recognition Device			0		
44	2/13/2015 12:44:57 PM	Face Recognition Device			0		
43	2/13/2015 12:44:51 PM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
42	2/13/2015 12:44:49 PM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
41	2/14/2015 1:44:30 AM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
40	2/14/2015 1:44:29 AM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
39	2/14/2015 1:44:12 AM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
38	2/14/2015 1:44:11 AM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
37	2/14/2015 1:44:02 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
36	2/14/2015 1:43:46 AM	Face Recognition Device 0014787674	Watchnet		533	ashwin	bil
35	2/14/2015 1:43:35 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
34	2/14/2015 1:27:56 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
33	2/14/2015 1:27:44 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
32	2/14/2015 1:25:20 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
31	2/14/2015 1:20:04 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
30	2/14/2015 1:27:56 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
29	2/14/2015 1:27:44 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
28	2/14/2015 1:25:20 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
27	2/14/2015 1:20:04 AM	Face Recognition Device	Watchnet		517	Peter	Punzalan
26	2/6/2015 10:52:41 PM	Face Recognition Device			0		
25	2/6/2015 10:52:33 PM	Face Recognition Device			0		
24	2/6/2015 10:52:41 PM	Face Recognition Device			0		

Face Recognition Viewer



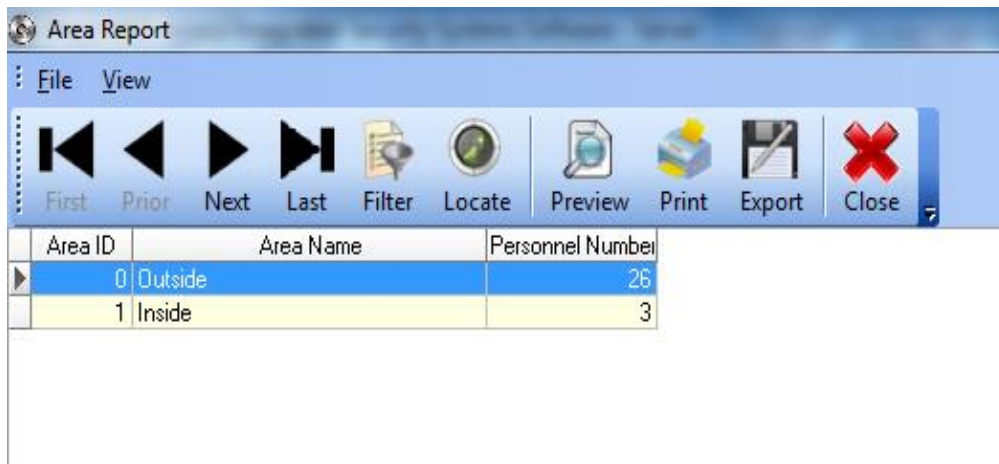
None Capture Photo

6.6 Bank Card Events – Displays all the bank card events on the software.



6.7 Area Report

In some cases we would like to know how many *Personnel* are in each area. The *Area Report* provides us with this kind of information. It has the same features in its *View* menu like the report above. Please note that Anti-Pass back feature must be active and used properly for the information in this report to be accurate.



6.8 Personnel Area Report

Personnel Area Report allows for the viewing of Personnel currently in each area. It has the same features in its View menu like the reports above (Sections 10.1 – 10.3). Please note that Anti Pass back feature must be active and used properly for the information in this report to be accurate. Both this report and the Area Report (Section 10.4) can be used in emergency cases where security personnel would like to evacuate the building immediately. They can know where personnel are and whether all the areas are empty.

Personnel N	First Name	Last Name	Personnel Code	Site Code	Card Num	Temporary Card	Gender	Department
1	Linda	Zeta		77	55714		Female	Tech Support Department
2	Jesica	Lin		225	54530			Tech Support Department
3	Maria	Nunez		226	888			Tech Support Department
5	Shawn	German		403	47854			Head Office
8	Octavio	Colantonio		225	36820		Male	Tech Support Department
9	Jessica	Stevens		188	48685			Engineering
10	Azezal	Stevens		225	34756			Tech Support Department
12	Octavio	Fobe		98	31379		Male	Head Office
13	Simon	Taves		0	10			Tech Support Department
14	Greg	Hysak		127	65535			Head Office
15	Pria	Nedal		168	28370			Warehouse
17	Prinder	Grewal		168	32990			Tech Support Department
22	juhgr	sdxr		0	3			Tech Support Department
23	red	lrde		0	4			Tech Support Department
32	Test	PIN		0	4321			Tech Support Department
33	Octa	0001		0	1234			Tech Support Department
34	Pradeep	Boss		0	1			Tech Support Department
35	Card	Test		201	810			Tech Support Department
36	Milo	Allaya		201	808			Tech Support Department
38				100	12345	<input checked="" type="checkbox"/>		Head Office
39	Octavio	Finger		1	2			Tech Support Department
40	Sonja	Banks		12	48852		Female	Warehouse
41	Tare	Conti		12	48513			Head Office
42	Greg	Ti		0	8888			Tech Support Department

6.9 Area Changed Report

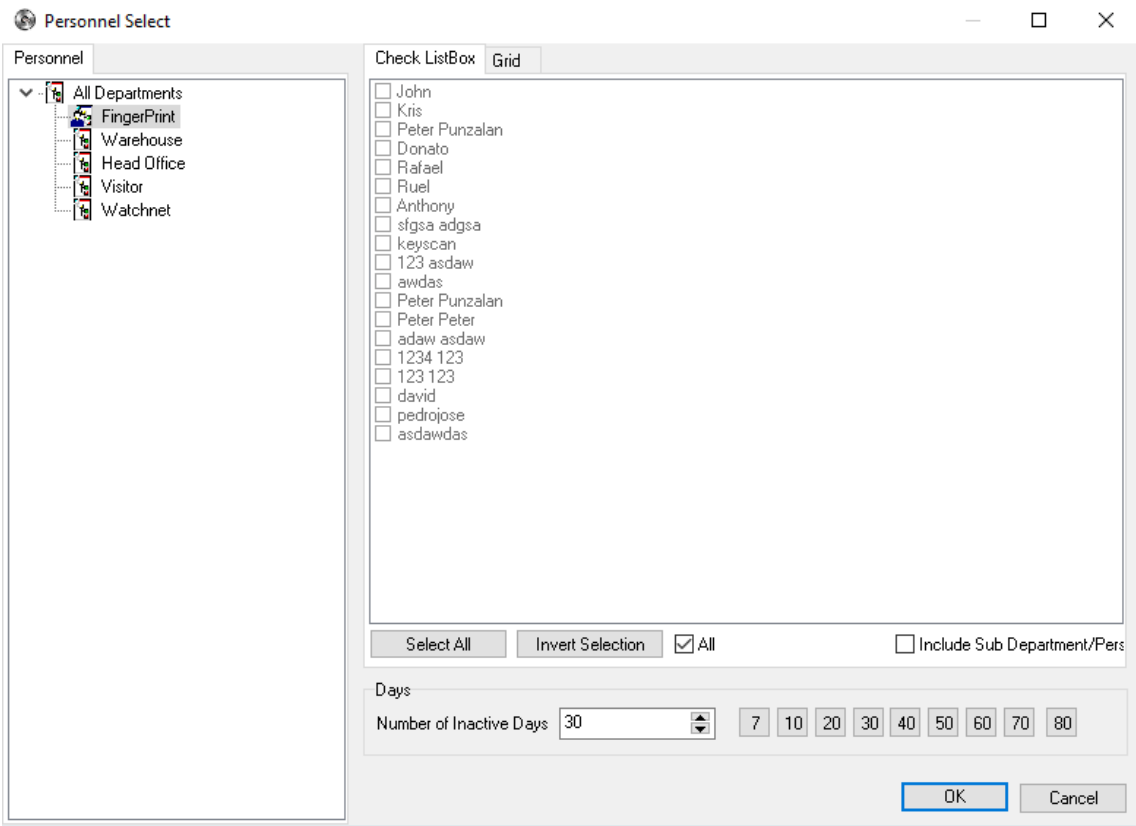
This report tracks how the Personnel are moving inside the buildings/offices from one area to the other. This can help to trace certain personnel and see where they were and at what time they were there. It has the same features in its View menu like the reports already described in Sections 10.4 - 10.5. Anti-Pass back must be activated and properly used.

Auto ID	TimeStamp	Department	Personnel N	Personnel Code	First Name	Last Name	Card No.	Entry Time of Exit Area	Entry Controller Name	Entry Door Name	Time	Entry Area Name	Exit
---------	-----------	------------	-------------	----------------	------------	-----------	----------	-------------------------	-----------------------	-----------------	------	-----------------	------

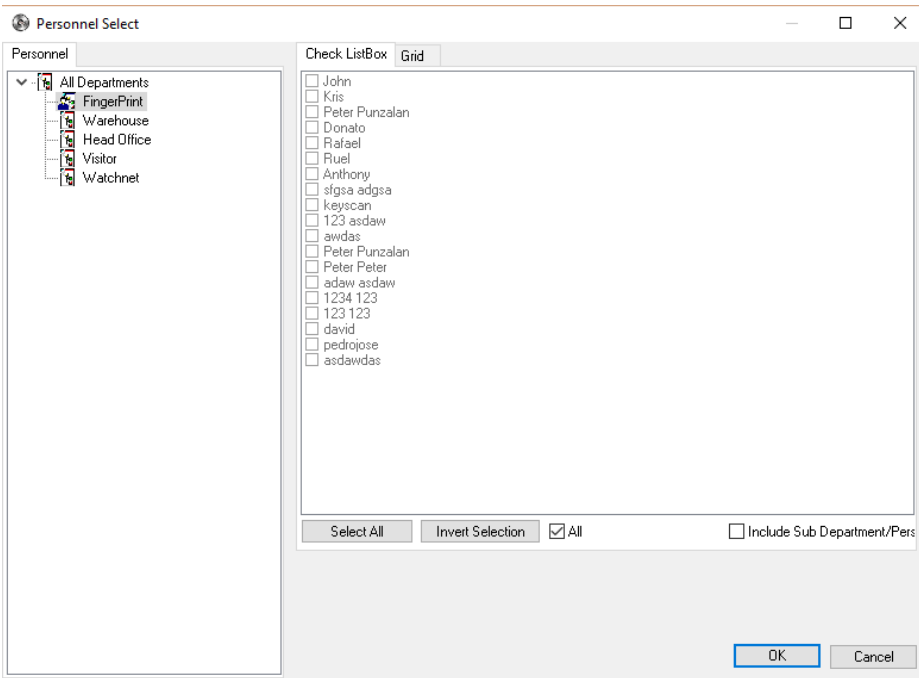
6.10 Personnel In/Out Reports – Consist of two types of reports.

- **Card Not Used Long time**

Displays Cards that are not used



- **Personnel Not Out of Designated Area** - To show report if personnel are not yet out of the building



6.11 Access Level Report

Access Level Report displays all the personnel's access level. It has the same features in its *View* menu like the report below.

Preview - Personnel Access Level Report

Print Stop Page Setup Scale Previous Page Next Page Close

Octavio demo dongle 1

Personnel Access Level Report

Personnel N	First Name	Last Name	Personnel Code	Site Cod	rd Num1	Department	Controller ID	Door ID
1	Linda	Zeta		77	55714	Tech Support Departmen	31	1
1	Linda	Zeta		77	55714	Tech Support Departmen	31	2
1	Linda	Zeta		77	55714	Tech Support Departmen	31	3
1	Linda	Zeta		77	55714	Tech Support Departmen	31	4
1	Linda	Zeta		77	55714	Tech Support Departmen	31	5
1	Linda	Zeta		77	55714	Tech Support Departmen	31	6
1	Linda	Zeta		77	55714	Tech Support Departmen	31	7
1	Linda	Zeta		77	55714	Tech Support Departmen	31	8
1	Linda	Zeta		77	55714	Tech Support Departmen	1	1
1	Linda	Zeta		77	55714	Tech Support Departmen	1	2
1	Linda	Zeta		77	55714	Tech Support Departmen	1	1
1	Linda	Zeta		77	55714	Tech Support Departmen	1	2
1	Linda	Zeta		77	55714	Tech Support Departmen	1	3
1	Linda	Zeta		77	55714	Tech Support Departmen	1	4
1	Linda	Zeta		77	55714	Tech Support Departmen	1	5
1	Linda	Zeta		77	55714	Tech Support Departmen	1	6
1	Linda	Zeta		77	55714	Tech Support Departmen	1	7
1	Linda	Zeta		77	55714	Tech Support Departmen	1	8
1	Linda	Zeta		77	55714	Tech Support Departmen	1	1
1	Linda	Zeta		77	55714	Tech Support Departmen	1	2
1	Linda	Zeta		77	55714	Tech Support Departmen	1	3
1	Linda	Zeta		77	55714	Tech Support Departmen	1	4
1	Linda	Zeta		77	55714	Tech Support Departmen	1	5
1	Linda	Zeta		77	55714	Tech Support Departmen	1	6

6.12 Access Security Group Report

Access Security Group Report displays all personnel's access levels via security groups.

Personnel ID	First Name	Last Name	Personnel Code	Card No.	Department	Security Group Name
1	Peter	Remote		0001380934	Head Office	24 Hours
3	Peter	Mifare		0858594193	Head Office	24 Hours
4	peter	fob		0003681360	Head Office	24 Hours
5	peter			0012648040	Head Office	24 Hours
6	F0obbb			0001775205	Head Office	24 Hours

Record counter: 5

6.13 Time Attendance

The System displays an attendance report in accordance with the condition such as personnel, department, and record type. The condition is described via the follow illustration.

6.14 Time Canteens Report

Times Canteen report is consisting of different types of reports.

6.15 All Intrusion Events

This report displays all different reports from intrusion panels.

6.16 All Intrusion system status

This report displays all the status of the zones for the intrusion.

6.17 All CCTV Event

The System displays all the events relating to CCTV. It has the same features in its *View* menu like the report below.

Auto ID	DVR Name	Channel Name	Time	Status	Ack. Time
822	CCTV DVR(8)		11/21/2013 7:00:59 AM	✓	
821	CCTV DVR(10)		11/21/2013 7:00:57 AM	✓	
820	CCTV DVR(7)		11/21/2013 7:00:57 AM	✓	
819	CCTV DVR(9)		11/21/2013 7:00:55 AM	✓	
818	CCTV DVR(8)		11/21/2013 2:01:12 AM	✓	
817	CCTV DVR(6)		11/21/2013 2:01:12 AM	✓	
816	CCTV DVR(2)		11/21/2013 12:00:57 AM	✓	
815	CCTV DVR(9)		11/20/2013 9:56:03 PM	✓	
814	CCTV DVR(9)		11/20/2013 1:22:52 PM	✓	
813	CCTV DVR(9)		11/20/2013 8:07:03 AM	✓	
812	CCTV DVR(9)		11/20/2013 6:24:03 AM	✓	
811	CCTV DVR(9)		11/20/2013 5:11:02 AM	✓	
810	CCTV DVR(8)		11/20/2013 2:01:19 AM	✓	
809	CCTV DVR(6)		11/20/2013 2:01:09 AM	✓	
808	CCTV DVR(9)		11/19/2013 5:32:59 PM	✓	
807	CCTV DVR(9)		11/19/2013 1:11:56 PM	✓	
806	CCTV DVR(14)		11/19/2013 1:09:50 PM	✓	
805	My DVR Cube(13)		11/19/2013 1:09:50 PM	✓	
804	CCTV DVR(10)		11/19/2013 1:09:44 PM	✓	
803	CCTV DVR(8)		11/19/2013 1:09:43 PM	✓	
802	CCTV DVR(7)		11/19/2013 1:09:43 PM	✓	
801	CCTV DVR(6)		11/19/2013 1:09:42 PM	✓	
800	CCTV DVR(5)		11/19/2013 1:09:42 PM	✓	
799	CCTV DVR(4)		11/19/2013 1:09:41 PM	✓	

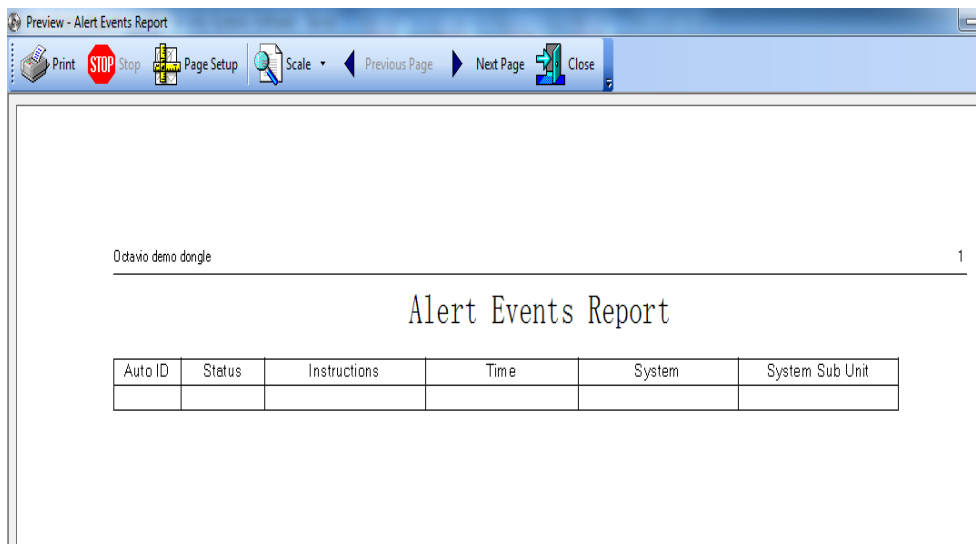
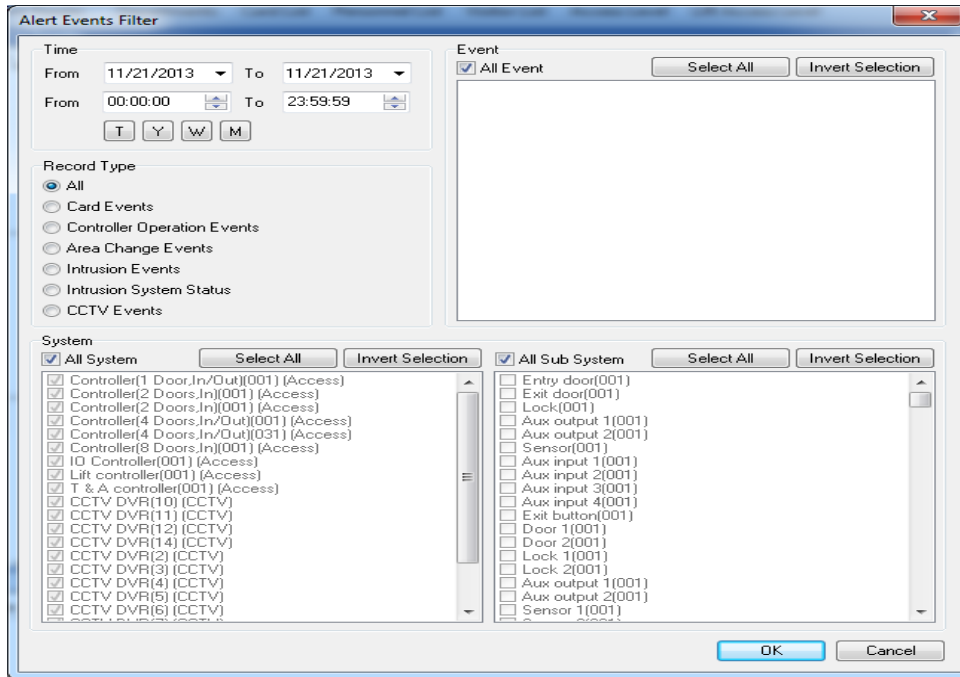
6.18 All Alert Events

The system displays all types of *alert events* such as *card events*, *controller operation events*, *CCTV events*. We can find out problems by checking the events. It has the same features in its *View* menu like the report above (Sections 10.1 – 10.3).

Auto ID	Status	Instructions	Time	System	System Sub Unit

6.19 Alert Events Filter

We can run different queries to get specific alert events records regarding different system, record type, events etc. Similarly to 9.1 the View menu allows us to export the result to an MS-Excel file or previewing it in a printable mode.



6.20 System Log

The System Log displays which WatchNET Access Software user has logged on and when. It shows what kinds of actions were taken by the user. This way we can easily know who was the *Guard* or *Operator* of the system during a certain time. In case we would like to investigate a critical event like intrusion to the office or building the System Log

will allow seeing *In whose shift it happened*. . It has the same features in its View menu like the report above (Sections 10.1 – 10.3).

Preview - System Log

Print Stop Page Setup Scale Previous Page Next Page Close

Ocdavio demo dongle 1

System Log

Auto ID	User	Time	Description	Line ID	Controller	Component
2879	Administrator	11/21/2013 2:50:02 PM	Login successful.	0	0	0
2878	Administrator	11/21/2013 11:44:10 A	Change Controller Component status	7	1	96
2877	Administrator	11/21/2013 11:43:43 A	Change Controller Component status	7	1	96
2876	Administrator	11/21/2013 11:43:11 A	Change Controller Component status	7	1	68
2875	Administrator	11/21/2013 11:43:08 A	Change Controller Component status	7	1	68
2874	Administrator	11/21/2013 11:43:01 A	Change Controller Component status	7	1	96
2873	Administrator	11/21/2013 11:42:54 A	Change Controller Component status	7	1	96
2872	Administrator	11/21/2013 11:36:42 A	Change Controller Component status	7	1	96
2871	Administrator	11/21/2013 11:36:28 A	Change Controller Component status	7	1	96
2870	Administrator	11/21/2013 11:29:43 A	Change Controller Component status	7	1	96
2869	Administrator	11/21/2013 10:50:28 A	Change Controller Component status	7	1	96
2868	Administrator	11/21/2013 10:49:49 A	Change Controller Component status	7	1	68
2867	Administrator	11/21/2013 10:49:46 A	Change Controller Component status	7	1	68
2866	Administrator	11/21/2013 10:49:39 A	Change Controller Component status	7	1	96
2865	Administrator	11/21/2013 10:49:31 A	Change Controller Component status	7	1	96
2864	Administrator	11/21/2013 10:49:11 A	C3 faild 10 times.	2	1	0
2863	Administrator	11/21/2013 10:49:11 A	C4 faild 10 times.	2	1	0
2862	Administrator	11/21/2013 10:48:25 A	To delete a controller, name = Control	9	1	0
2861	Administrator	11/21/2013 10:41:59 A	C3 faild 10 times.	2	1	0
2860	Administrator	11/21/2013 10:41:58 A	C4 faild 10 times.	2	1	0
2859	Administrator	11/21/2013 8:49:40 AM	Change personal access level, for use	1	1	2
2858	Administrator	11/21/2013 8:49:39 AM	Change personal access level, for use	1	1	1
2857	Administrator	11/21/2013 8:49:18 AM	Change personal access level, for use	1	1	2
2856	Administrator	11/21/2013 8:49:17 AM	Change personal access level, for use	1	1	1

Chapter 7 Maintenance

7.1 Delete Records

Delete option can be setup as scheduled or delete all at once, this help saved more storage for database.

Delete Events from Database

Delete Events

- Controller Operation Events
- Card Events
- Area Changed Events
- Access photo / video file capture records
- Intrusion Events
- Intrusion System Status
- Intrusion photo / video file capture records
- CCTV Events
- CCTV photo / video file capture records
- Alert Events
- Canteen Records
- Event send records
- SMS send records
- E-Mail send records
- Event print record
- Keep playback capture /video download records

Delete Mode

Delete all records prior to this date
Date: 2018-05-25

Keep the recent records
Keep the last: 1000

Delete all

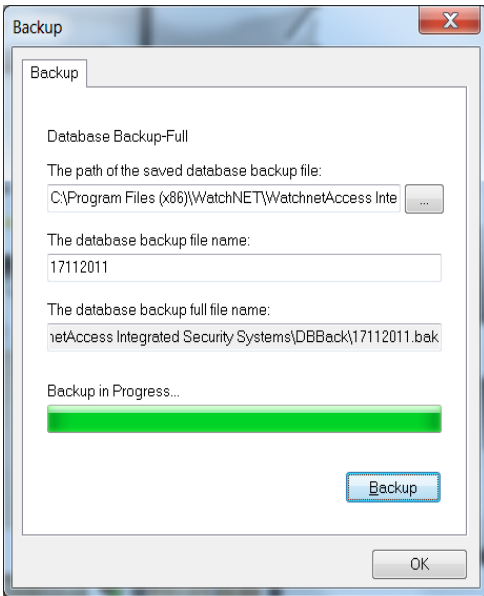
When delete the event records, and delete photo / video file capture records

When delete the photo / video file capture records, and delete the photo / video file

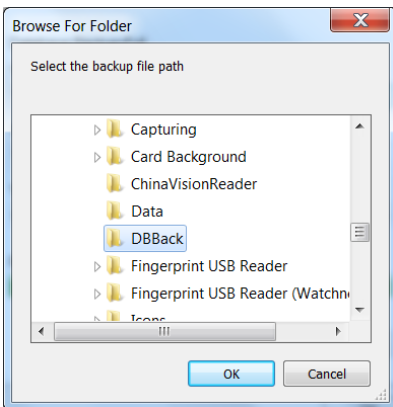
OK Cancel

7.2 Backup Database

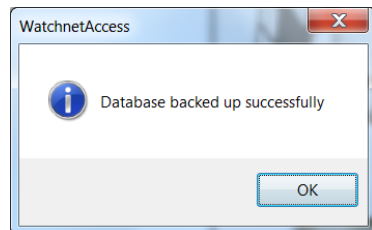
The user should backup the Database after any programming or Personnel changes so that the data can be restored if required. Select *Backup Database* from the *Maintenance*.



Disconnect any clients that may be accessing the database. Select a location to save the Database (Zip format) and then select *OK*.



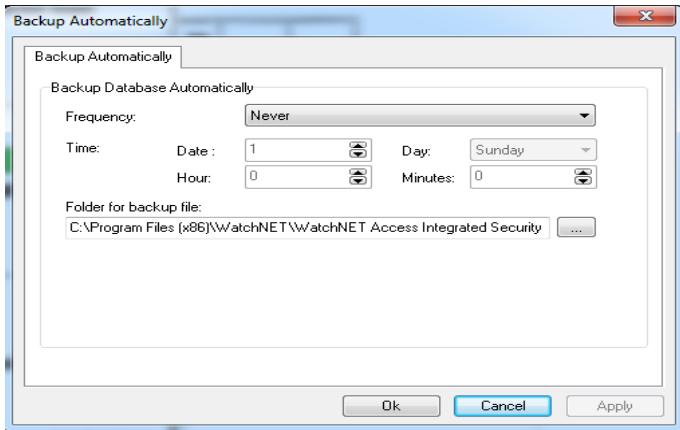
Then click the *Backup* button to continue.



If the Database was backed up successfully the *Database backup successful* message below will display. Click *OK*.

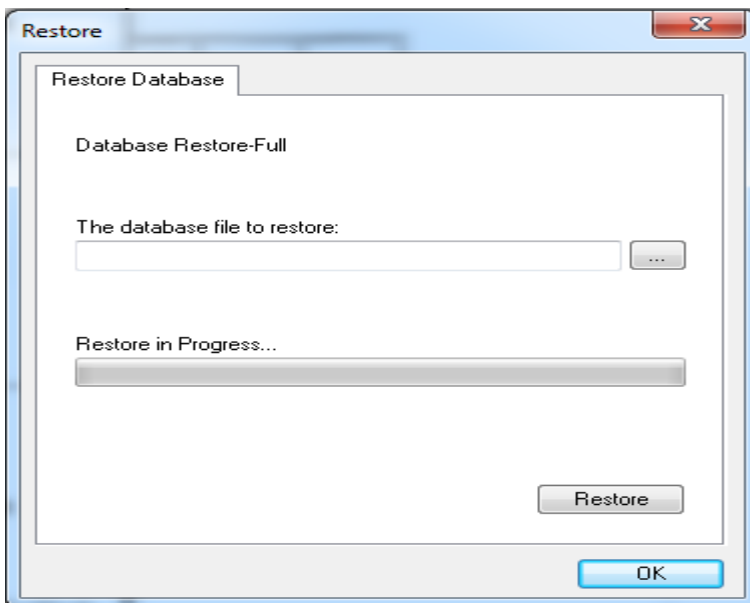
7.3 Auto Backup Database

Similar to 10.3 we perform a scheduled database backup.

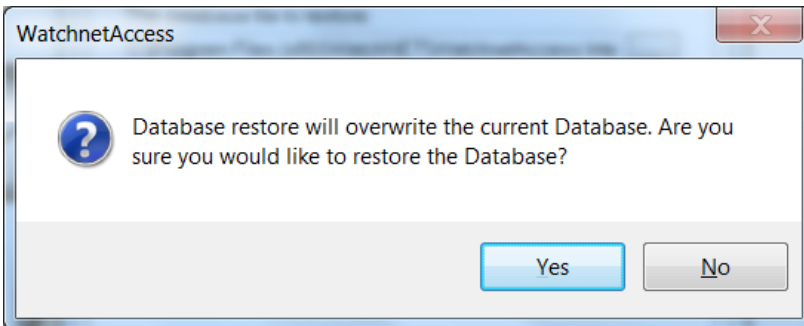


7.4 Restore Database

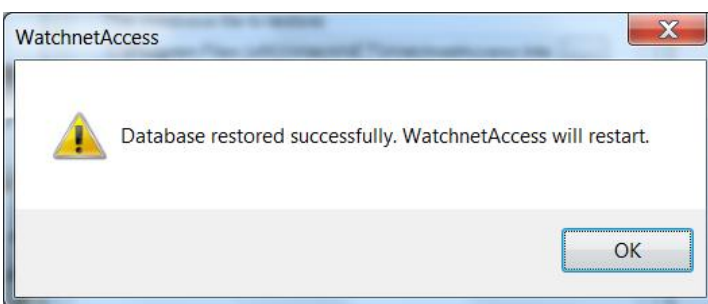
If the Database needs to be restored select *Restore Database* from the Maintenance menu. The restore needs full access to the database and if some other programs are using the database, the *Database Restore* option may not work. Disconnect any clients that may be using the database before restoring. Select the database that you wish to restore and click on *Restore*.



Before restoring a warning message will be displayed warning that the existed database will be overwritten and lost.

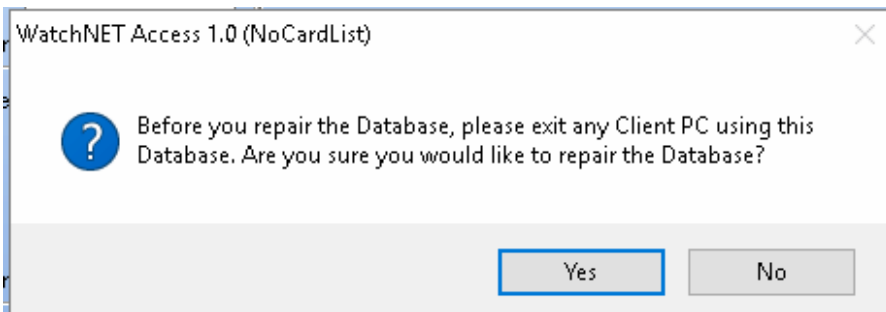


Once the database has been restored the software will need to be restarted. Click *OK* to restart.

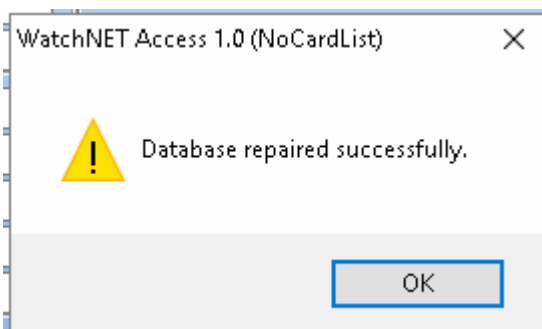


7.5 Compact/Repair Database

The Compact/Repair feature will repair and compact the database.

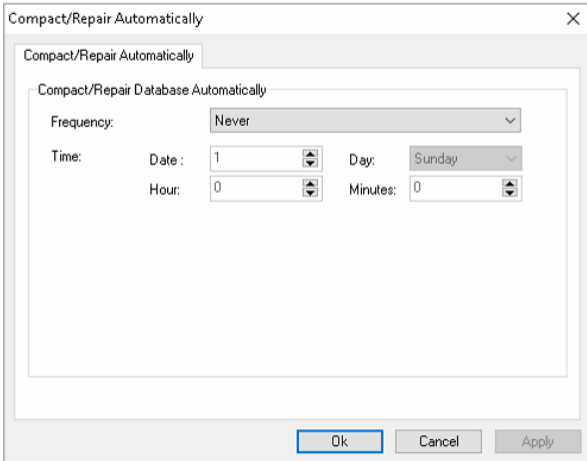


A warning message will be displayed. Click on *YES* to continue.



7.6 Auto Compact/Repair Database

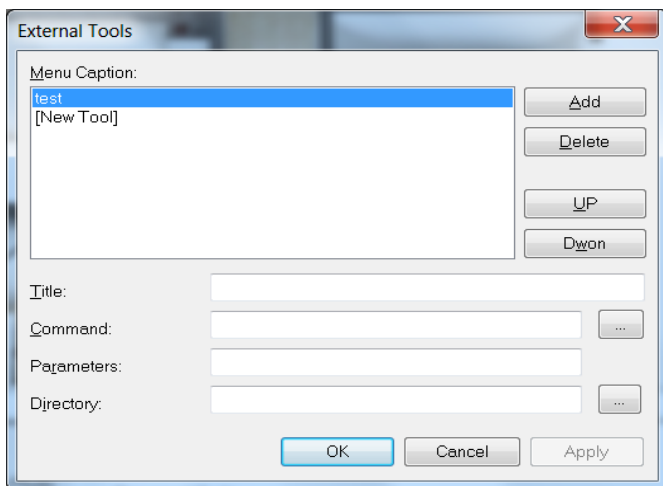
Allows you to set a date or time when the auto repair starts



Chapter 8 Tools

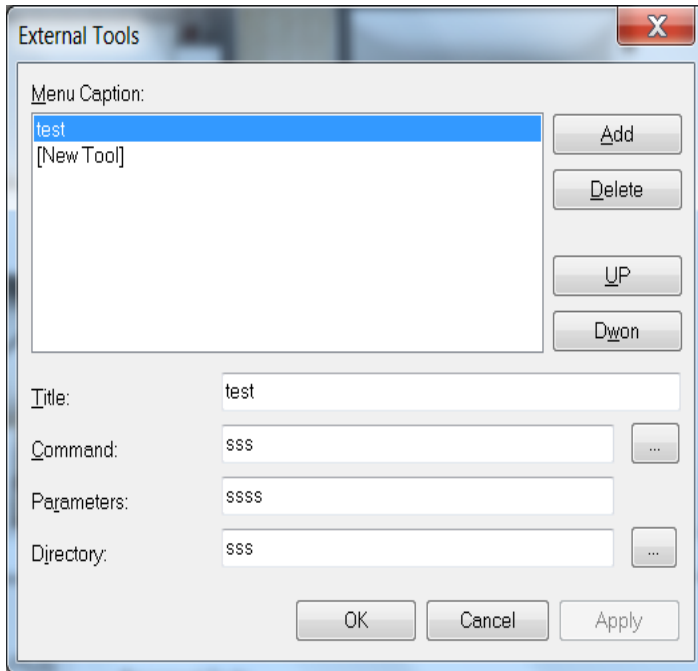
8.1 External Tools


Allows users to have External Icons of third party software to be imported into the WatchNET Access Software and to open the applications conveniently from within the software window.



To add an *External Tool*, follow the steps below:

1. Click *Add* to open the following window.



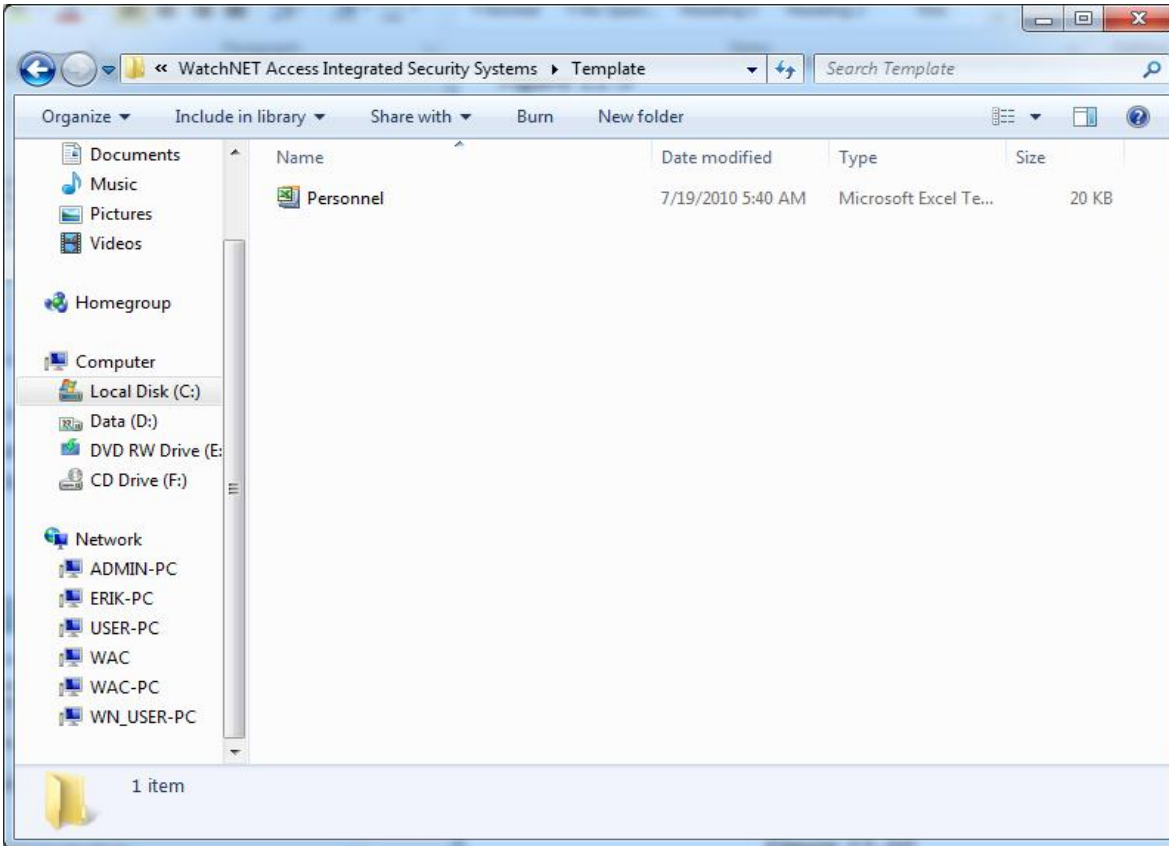
2. Amend the default title.
3. Click the *Command*  button to select a tool.
4. Enter the parameters in the *Parameters* text field.
5. Enter the value of the *Directory*.
6. Click *OK* or *Apply* to finish adding the tool.

8.2 Imports from Excel

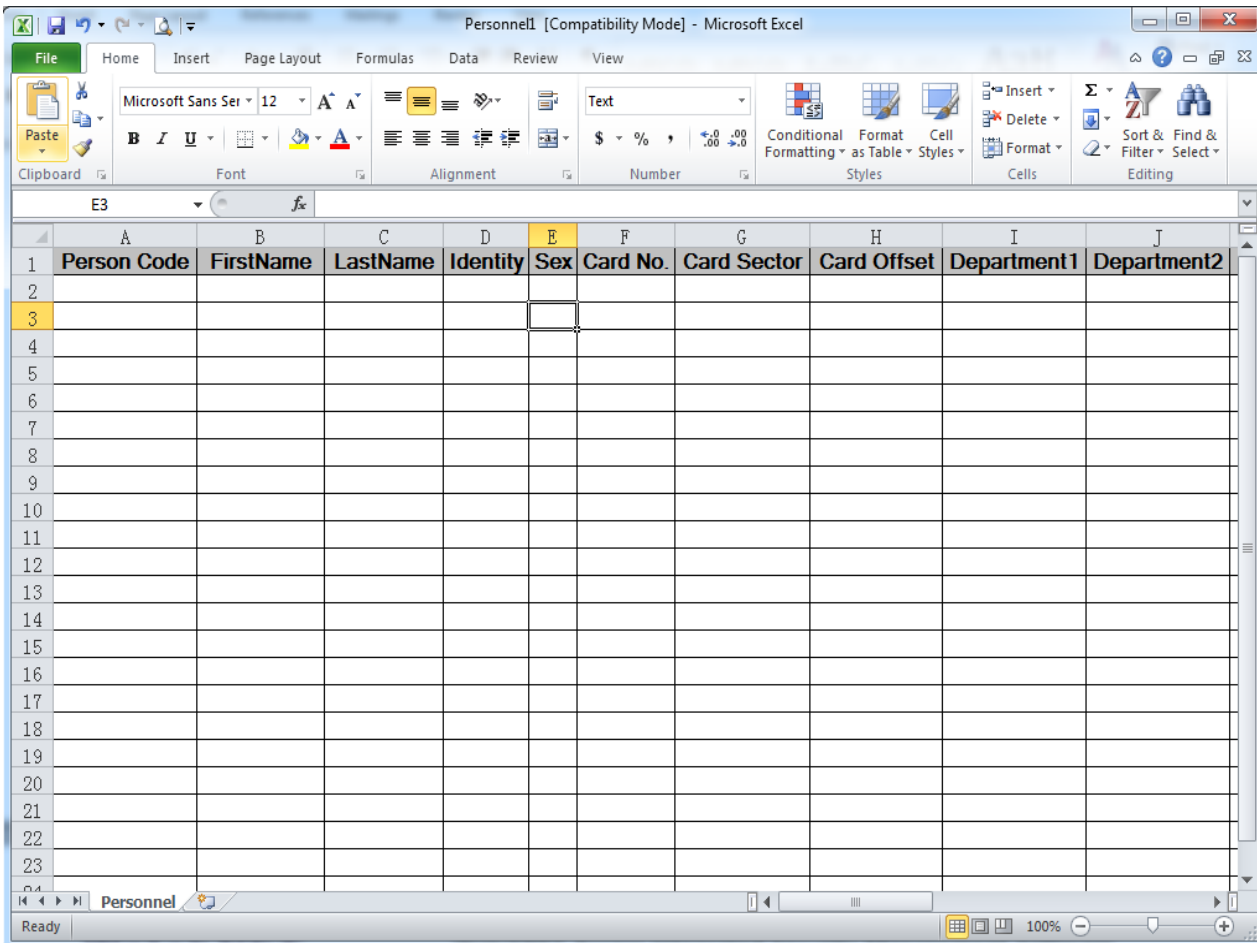
WatchNET Access Software allows the user to import data from an Excel file. The data can be taken from 3rd party software like *TIME AND ATTENDANCE* software, Human Resources software or any list of data.

The data which can be imported are *Personnel ID, First Name, Last Name, Identity, Gender, Card Number and Departments*. Before you proceed with importing, it's highly recommended to back up the current WatchNET Access Software Database. Select *Tools -> Import from Excel* and the window will be opened.

Inside the WatchNET Access Software folder there is a folder named "*Template*" which has a MS-Excel Template file named *Personnel.xlt*.

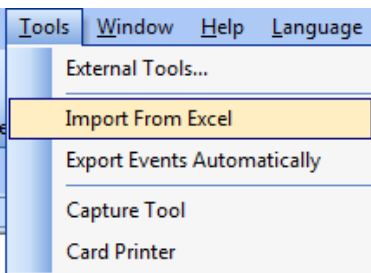


Open the file and enter the information you would like to import to the WatchNET Access Software. Save the file as *Excel 97-2003 Workbook*.

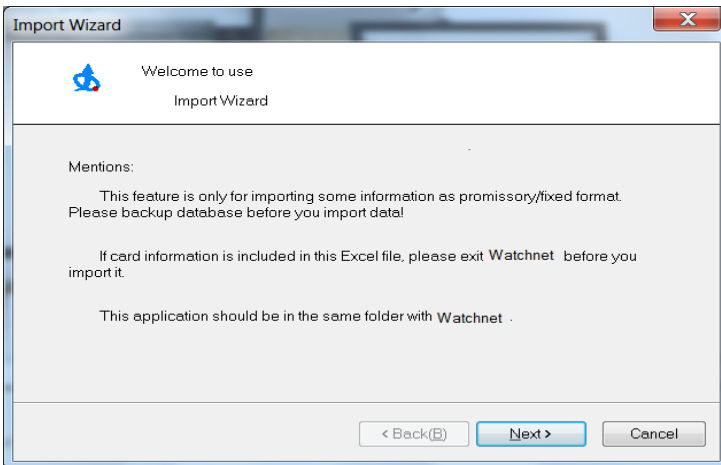


Note: "Card Sector" is the Site Code and "Card Offset" is the card number. For example is the card number is 226 ,03138 then in the "Card Sector" column input 226 and in the "Card Offset" input 03138.

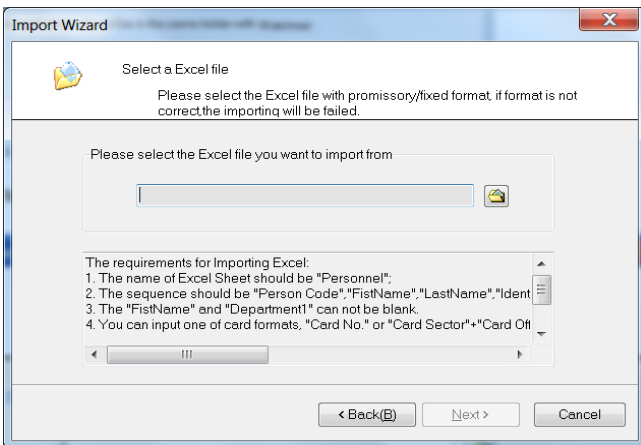
To start importing select *Tools -> Import from Excel.*



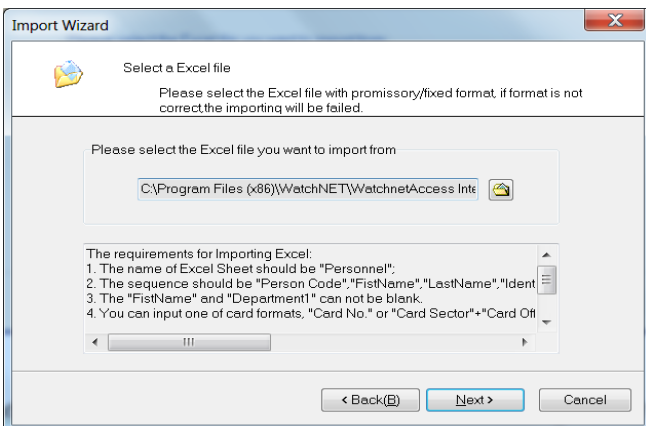
The *Import Wizard* window will be displayed.



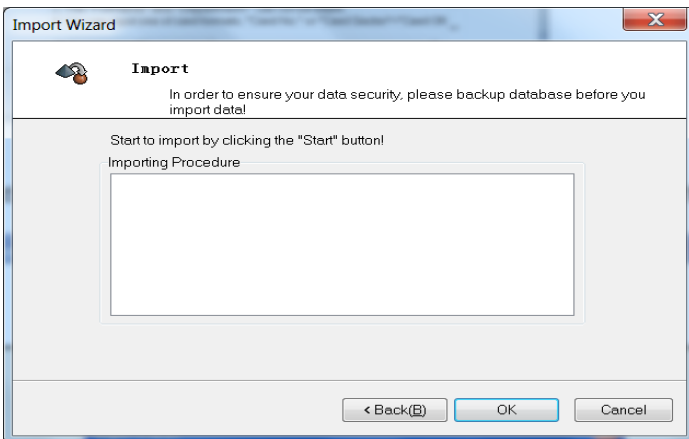
Read the comments carefully and click on *Next*.



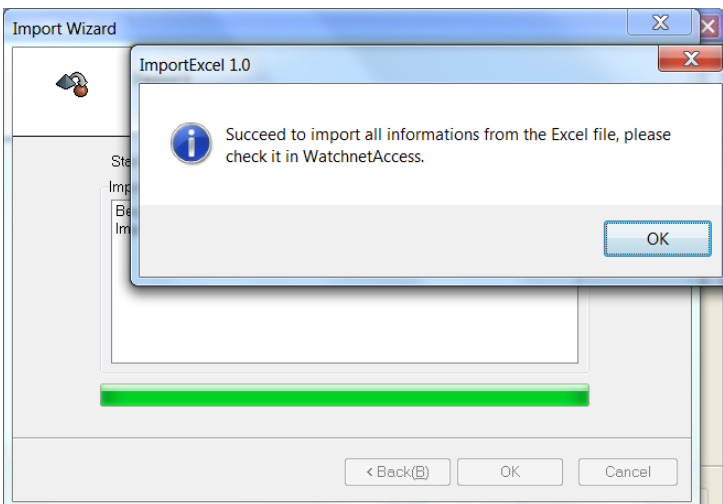
Read the comments carefully. Inside WatchNET Access Software folder there is a folder named *Template* which has an MS-Excel Template file named *Personnel.xls*. Open the file and enter the information you would like to import to WatchNET Access Software. Save the file as an *Excel 97-2003 Workbook*.



Click *Next* to continue.



Click *OK* and the window in will be displayed.

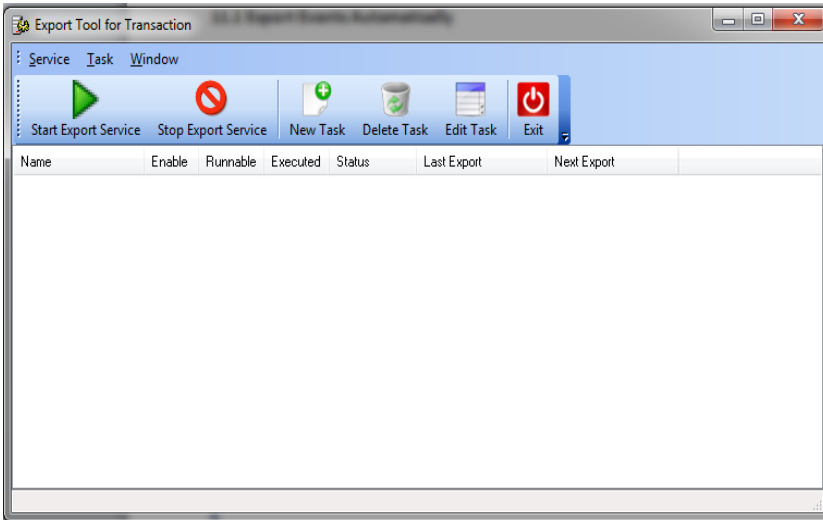


Click *OK* and *Cancel* to exit the *Import Wizard*. Verify that WatchNET Access Software has all of the imported the data.

8.3 Export Events Automatically

WatchNET Access Integrated Security Systems provides a powerful module which can run separately and exports all card events. The exporting is performed by creating *Tasks*.

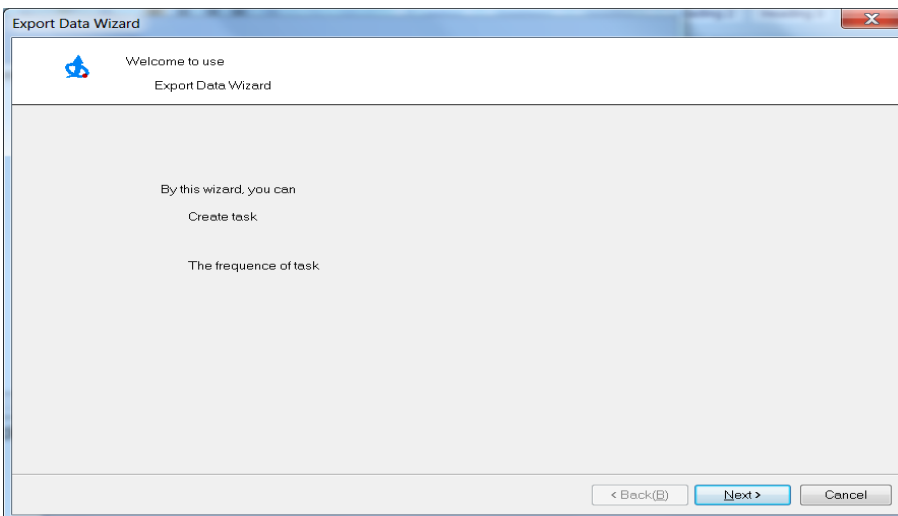
Each task creates a different export file with info that users define. Click on *Tools -> Export Events Automatically* to launch the window.



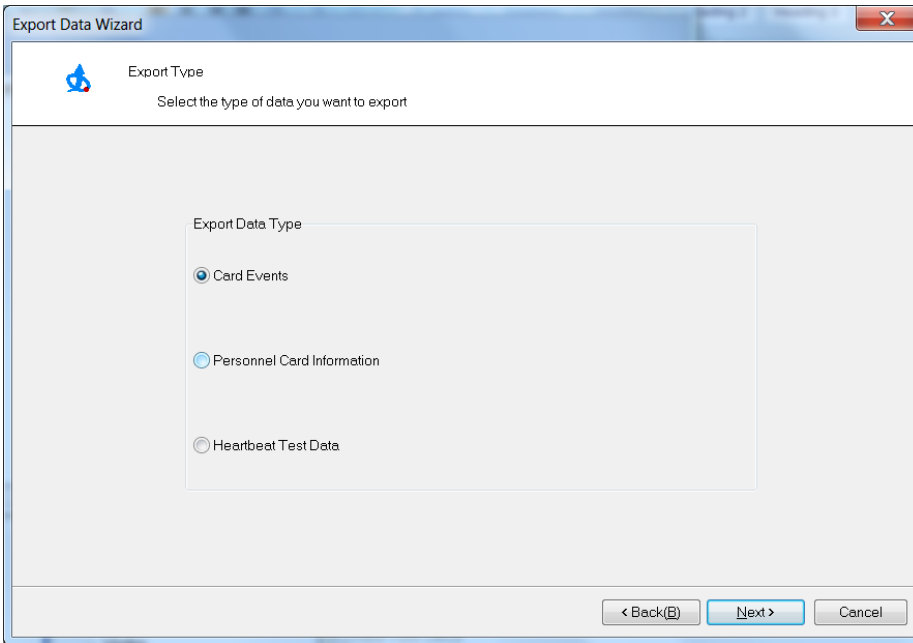
- **Name:** Exporting task name.
- **Enable:** Tasks is saved and enabled, running or scheduled to be running.
- **Runnable:** Task was already executed in the past.
- **Executed:** A task already performed.
- **Status:** Status of the task.
- **Last Export:** When was the last time the task was performing exporting.
- **Next Export:** When is the next time the task will perform exporting.

New Task

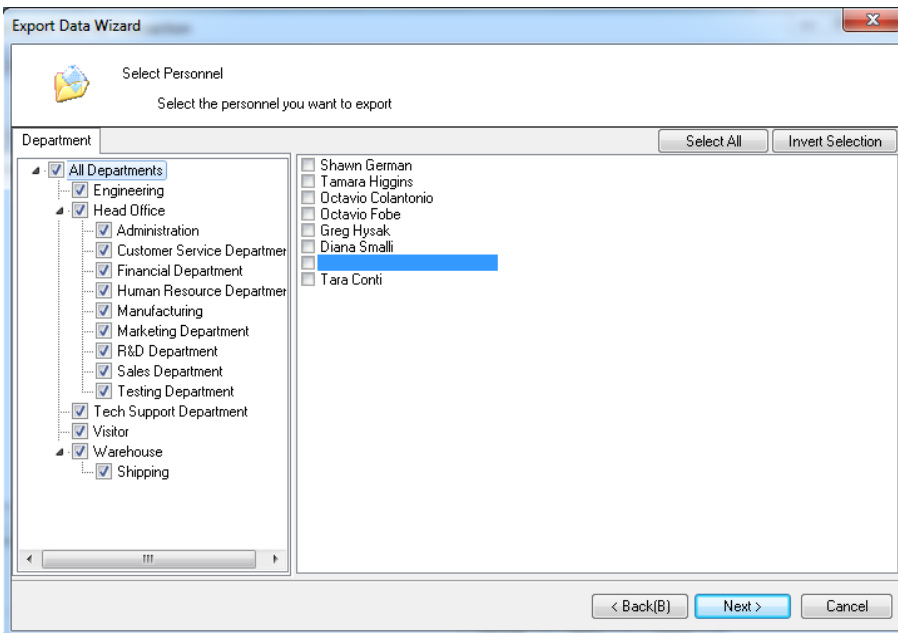
When clicking the New Task button, the window will be displayed.



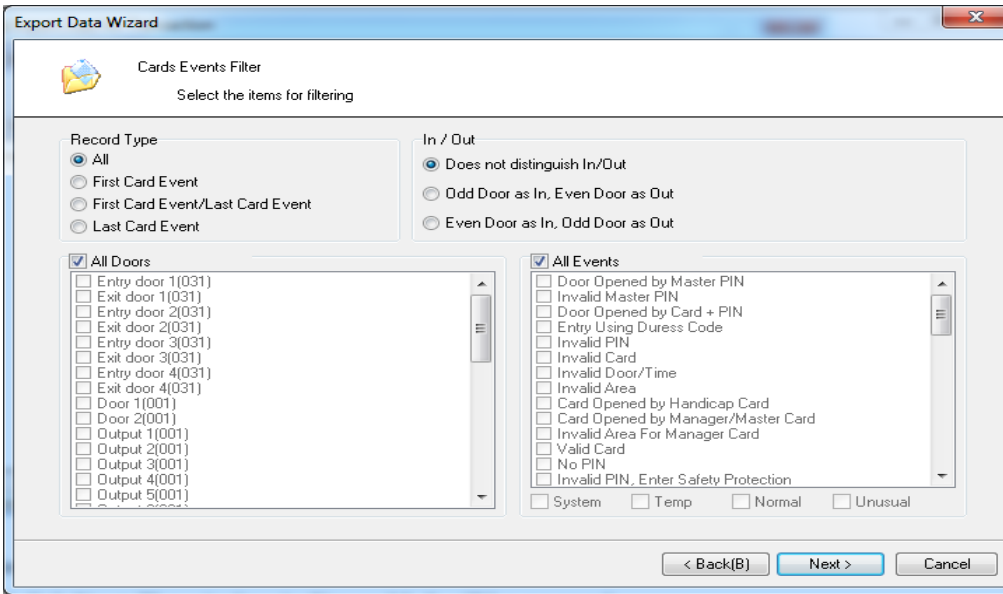
Click *Next*. The window will be displayed.



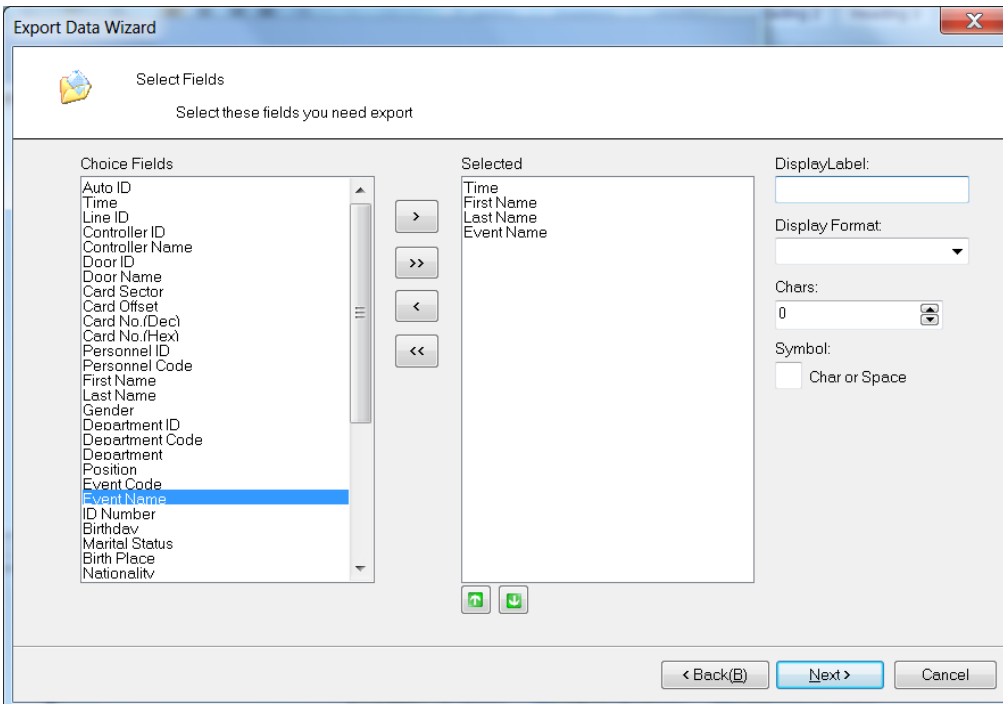
Select the data type you wish to export and click *Next*. Select the *Personnel* you wish to export and click *Next*.

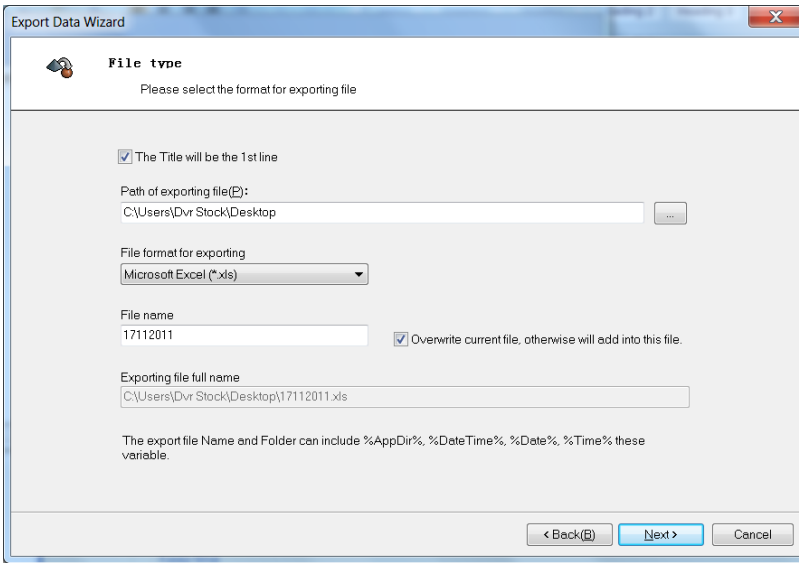


Select the *Departments, Sub Departments, Time Period, Doors, Record Type* to export all relevant records and click *Next*. The window will be displayed.

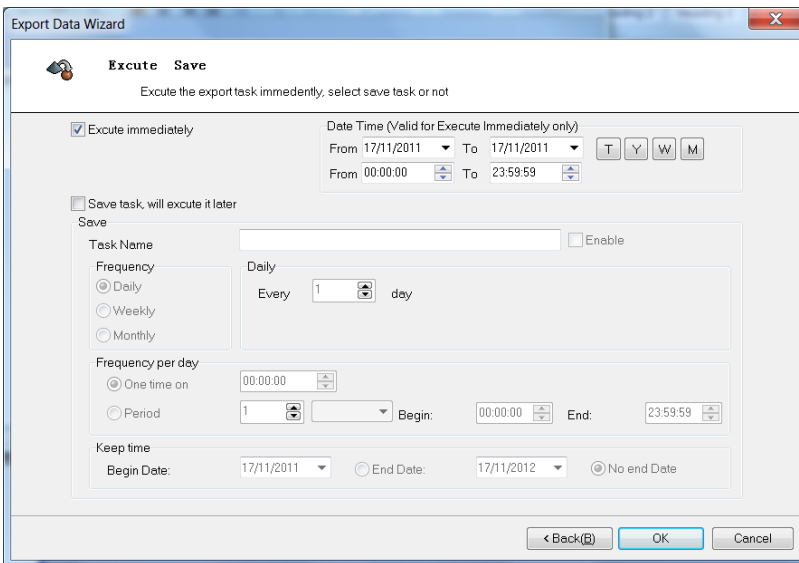


Select the *Fields* to be exported (or all fields). For each selected Field the format can be set according to user's needs.

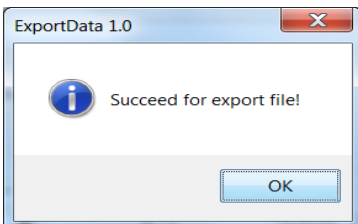




Check the *Title will be the 1st line* if you would like the fields name to be the first line in the file before the events. Enter the folder path and select the file format (MS-Excel, TXT, RTF, HTML etc.). Select the separator to separate between the different fields which were selected in Figure 11-5. Enter the File name and click *Next*. The window in Figure 11-6 will be opened.

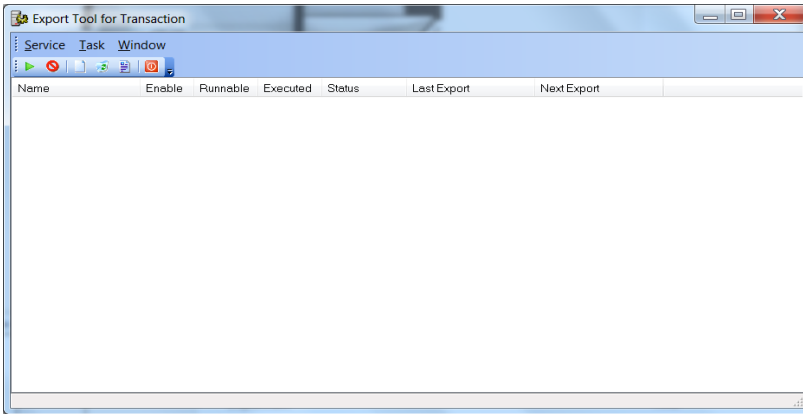


When you click on *OK* the following window for task successfully created will be displayed.



User can decide if the task should run immediately or be scheduled for later. Set the *Task Name* and *Enable* it. Set

the *Frequency* to be Daily/Weekly/Monthly. Set the *Daily Frequency* to be one time or periodically (as frequent as every minute). *Keep Time* will set if we limit the period of exporting to certain dates or infinite. Click *OK* and the window will be displayed.



Delete Task

Delete the selected task.

Edit Task

Allows the user to edit the task details, as in Section 11.3.1.

8.4 Capture Tool

WatchNET Access Software allows taking pictures of Personnel or Visitors using a web camera or Digital camera. Click on *Tools-> Capture Tool* to launch the window in Figure 11-34. User can take photos which will be stored in the *Photo* folder inside the folder of WATCHNET ACCESS INTEGRATED SECURITY SYSTEMS. User can also setup the camera and adjust its parameters.

Before you can use this feature, make sure that the camera is connected to the PC and camera driver is already installed and operating.

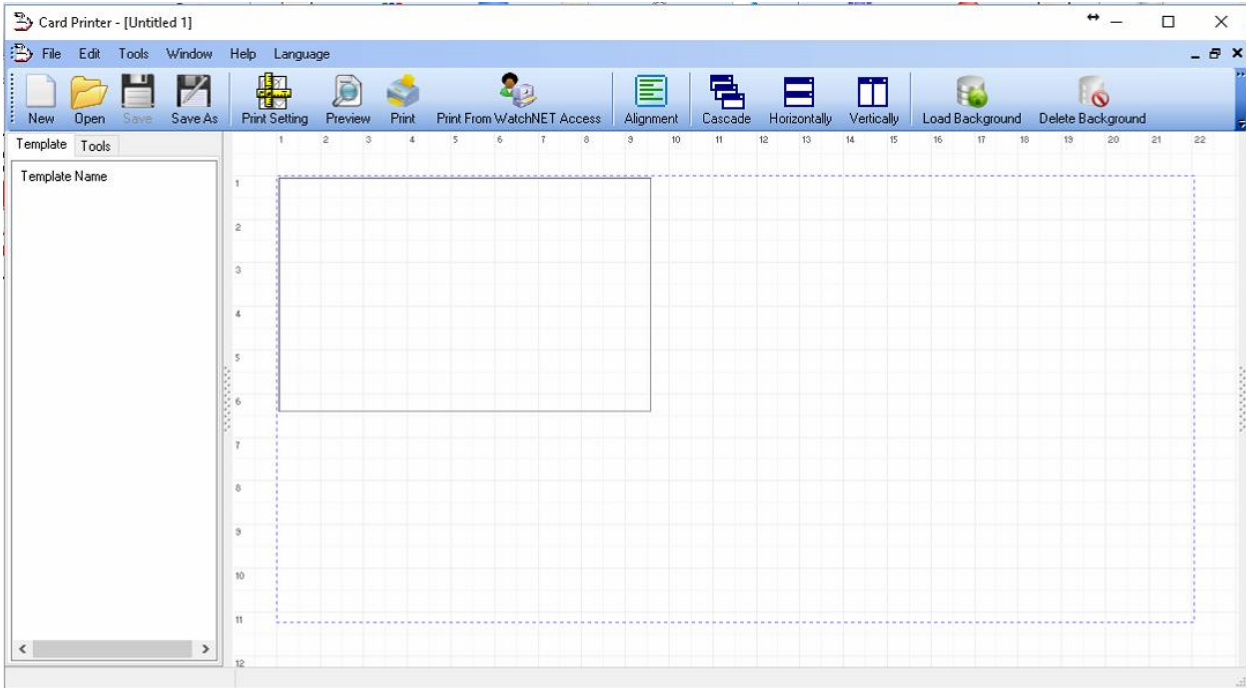


Click the Capture button to capturing the image and click Close.

8.5 Card Printer

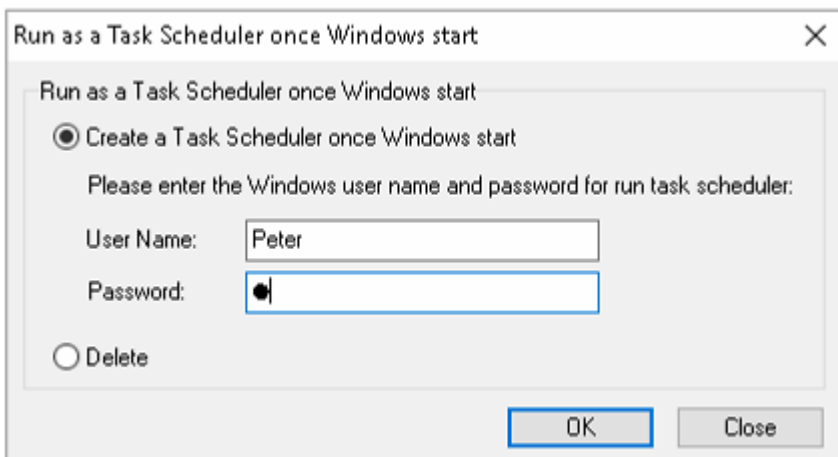
Card Printer option allows you to print badges for the card; user can create their own template to print.

Note: Printer must be installed first before running this feature



8.6 Run as Task Scheduler once Windows start

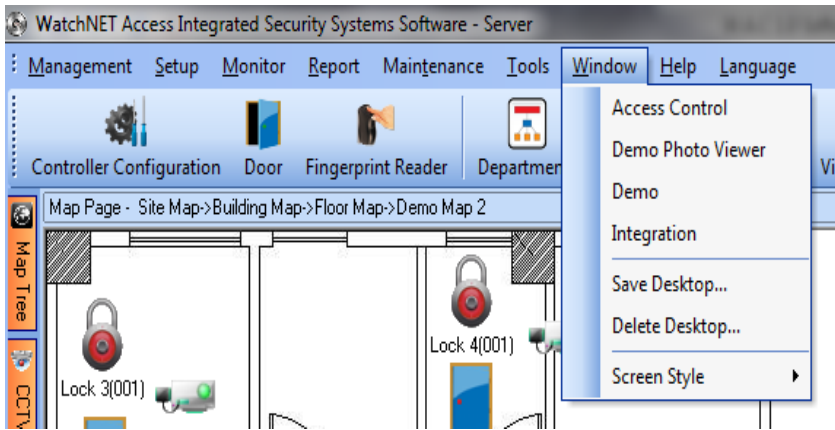
Input username and password for the windows so that software will start when the computer reboots.



Chapter 9 Window

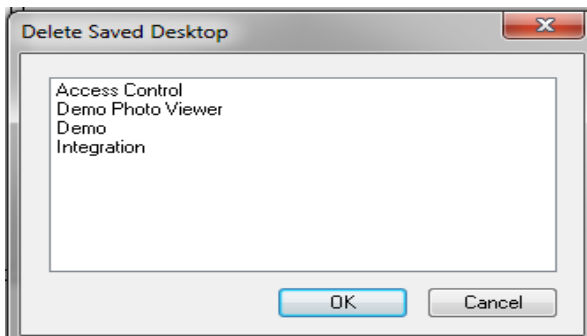
9.1 Save Desktop

You can save your desktop layout as a template through this command.



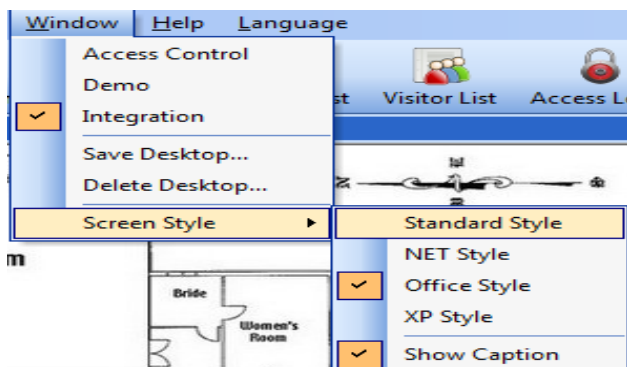
9.2 Delete Desktop

You can also delete unwanted desktop layout by clicking on the appropriate one and clicking on OK.



9.3 Screen Style

WatchNET Access Software provides you with an option to view the Window in the following styles: *Standard Style*, *NET Style*, *Office Style*, and *XP Style*.



If you need to see captions on all the Icons then you can check the *Show Caption* option.

Chapter 10 Help

10.1 Help

Clicking on *Help* will launch the WatchNET Access Control Software Manual.

10.2 Home Page

Launches the WatchNET Access Control Website.

10.3 On-line Update

Coming soon

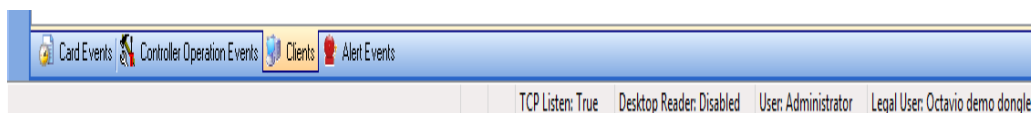
10.4 License Information

Will display the information of the *Registration Information* of this WatchNET Access Software.



10.5 Upgrade License

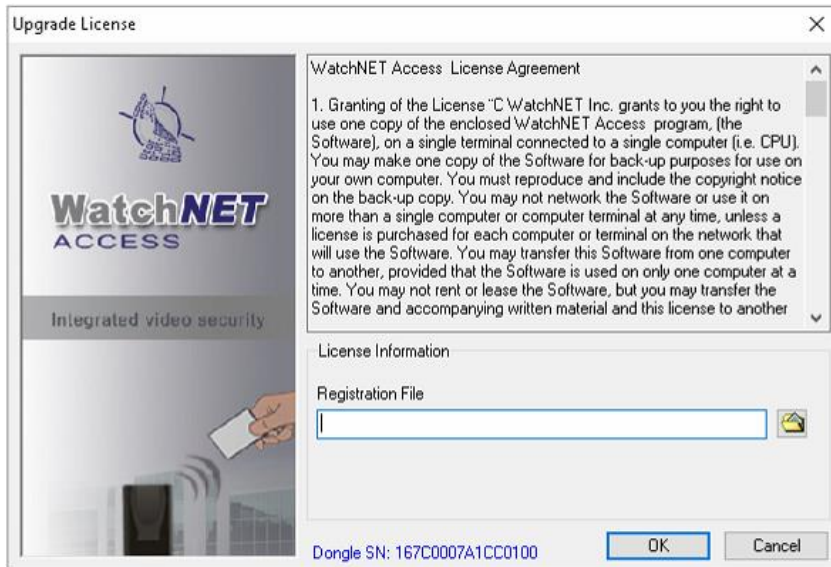
It is important to Re-Register the end user so the *Legal User* will display at the bottom of the main window. Accurate and updated *Legal User* is needed for verifying that the WATCHNET ACCESS INTEGRATED SECURITY SYSTEMS is genuine and a legal copy.



It is also needed for upgrading the WatchNET Access Software license. The user can upgrade the software license to control more doors, more clients PCs, have additional modules like CCTV, Intrusion etc. For upgrading the WatchNET Access Software license the user needs to provide WatchNET Access information such as the *USB dongle serial*

number and the *Legal User* name as seen in *Help -> Registration Information*.

In the case above *Serial Number* is 00000005 and the *Legal User* is WATCHNET ACCESS. WatchNET Access will provide a *Registration Code* in a TXT format. Click *Help -> Re-Register* and search for the file *client.txt* that's provided by WatchNET Access (Figure 13-3). Clicking *OK* will upgrade the WatchNET Access Software license to the needed license while keeping the existing USB Dongle.



10.6 About

About window lists the software details such as the *Version number* and the *last build* time plus WATCHNET ACCESS contact details.

