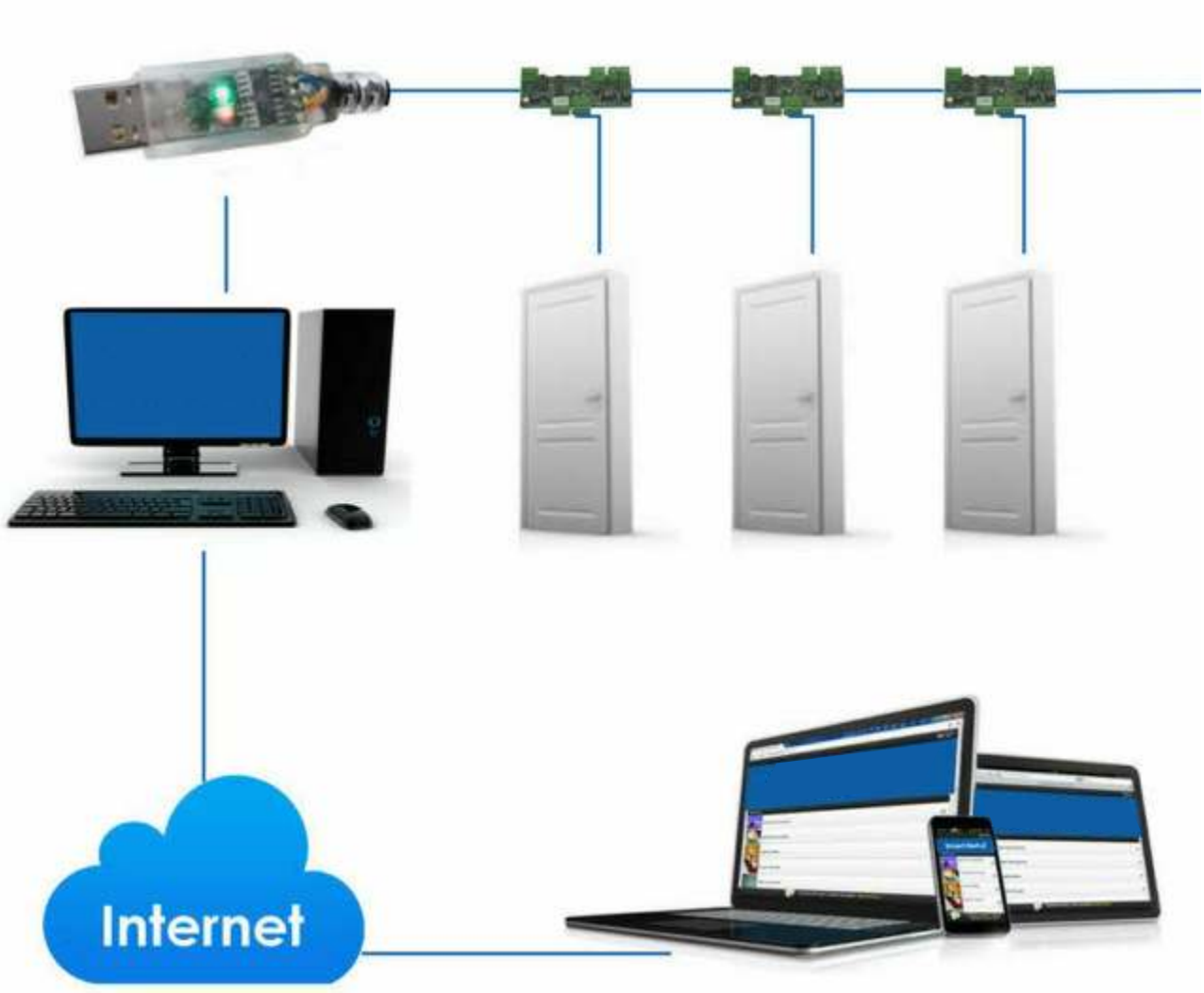
Smart.Net-IP

Door Access Control

DESKTOP – WEB – MOBILE



Operation & Technical Manual v3.03

TABLE OF CONTENTS

Smart.Net-IP Site Manager

Thank you for downloading the Smart.Net-IP Site Manager software. Thisprogram will allow you to control and manage all your electronically secured doors and entrances through easy-to-use desktop and mobile interfaces. Please read and follow these instructions for the successful installation, configuration and day-to-day operation of your access control system.

About

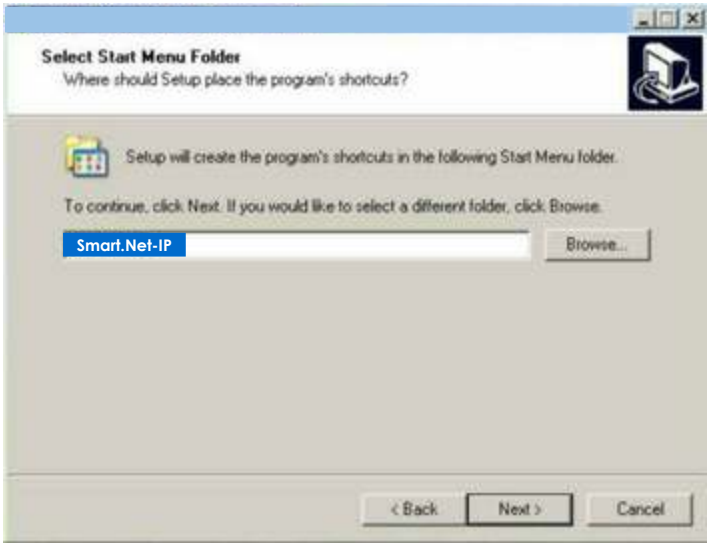
Smart.Net-IP is a computer administrated electronic access control system for up to 128 doors or entrances. Utilising individual compact single door intelligent controllers, installation is simple, modular and economical from 1 to 128 doors. The easy to use application is installed on a spare computer to control and manage the system for on-line or full off-line operation. All features are designed for ease of use with the minimum requirement for training. Smart.Net-IP is a fully distributed intelligence system enabling all changes and system configuration made at the computer to be stored locally at the door or entrance controllers, giving full door access control functionality on or off-line with maximum reliability.

Download & Installing Smar.Net-IP Site Manager

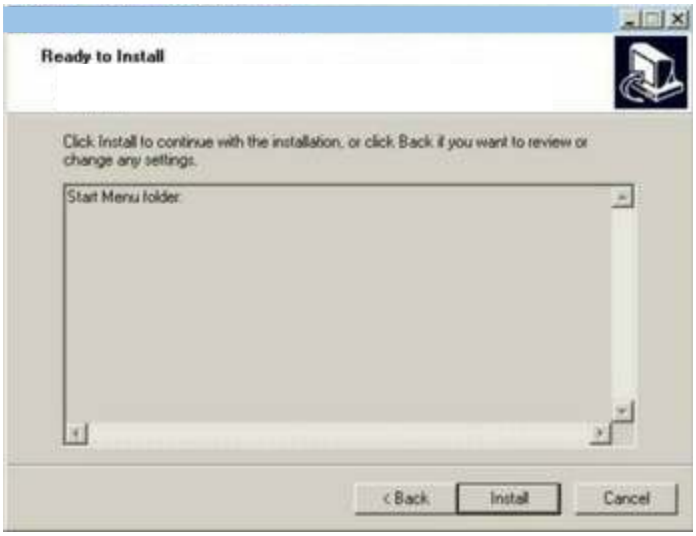
Before you can begin to configure and manage your controlled doors and entrances you must download and install the latest application software for the system. The Smart.Net-IP Site Manager Software Suite can be downloaded directly from our web site at www.doorentrydirect.com Navigate to this page and click on the single link for the latest release of Smart.Net-IP Site Manager. Save this single self-executing installer to the same computer that you intend to install the application on. The stored installer can be downloaded freely without the need for registration.

Once the file has been downloaded to your local hard disk you can then locate the file, run it and start the installation process. The simple installer will guide you through the installation and minimum intervention is required. After the software installation has been completed a desktop shortcut icon will be created for you to run the Site Manager program.

Follow the on-screen prompts and note that it is recommended you do not change the target descriptions within the installation program.



Select the Next button to proceed through the installation process.



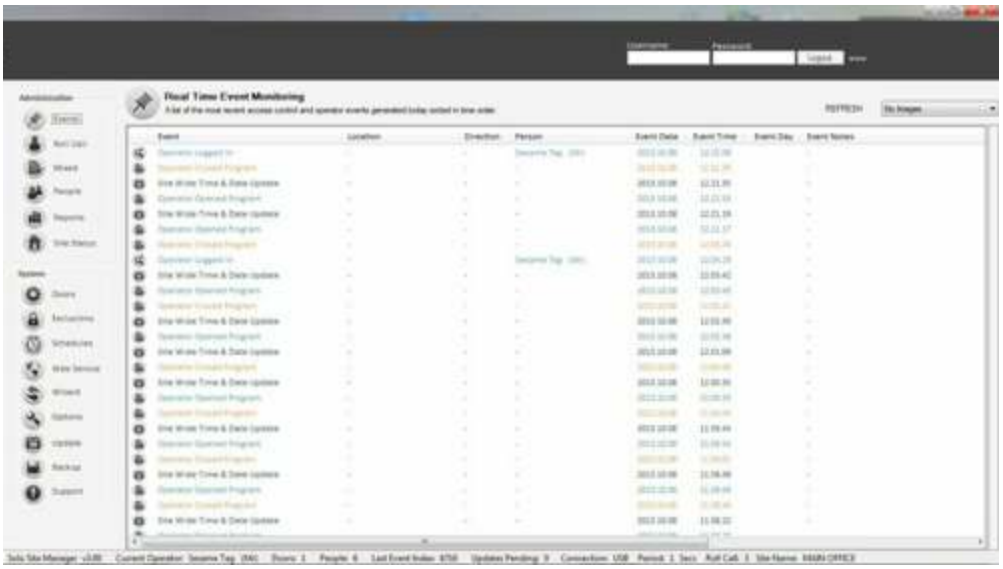
Please click on the Install button when ready.

The main application program will begin to install and may take some time to complete. It is recommended that you do not select the Cancel operation at this stage. If you wish to uninstall the Site Manager program at a later time then do this through the Program Manager function in Windows.

The installer may require you to install further items that are required and contained within the downloaded installer package. If this is the first time you have installed the Site Manger program on the target computer you must accept these additional item installs and click Finish. Please follow the onscreen prompts for the further installing support items. Once all the installations have completed the program should automatically launch, but if not try double- clicking the desktop shortcut icon.

Understanding the User Interface

The Smart.Net-IP Site Manager program has been designed to be quick and efficient to use. The easy to read screen and uncluttered views are prepared to give powerful information quickly and enable the operator to make changes simply with minimum training.



There are two distinct areas to the graphical view, the navigation panel on the left and the larger information panel on the right. The navigation panel is split in to two main groups Administration and System functions. System functions allow you to install and modify doors and entrances and make system wide installation sensitive changes, additions and deletions. The Administration functions are limited to day-to-day use of card holder maintenance, report production and door override control. The information panel contains all live information and information relating to the function and process being performed as selected on the navigation panel. The information panel will change its heading and icon as you select differing functions from the navigation panel.

Whenever you wish to use any functions of the program you are required to authenticate yourself with a username and password entered in the lower area of the navigation panel. When the Site Manager is first run there are know users defined and as such the default username and password are presented so just select the Login button to get full access to all Administration and System functions. You later can, as you define people, create individual usernames and passwords and allow or deny programming permissions for administration and/ or system functions for one or many if you wish.

Default Username & password

The default username and password are ‘admin’ but the default record containing these credentials should be deleted when at least one further record has been created with full administration and system permissions through the People screen option. If you inadvertently lock yourself out or forget any of the

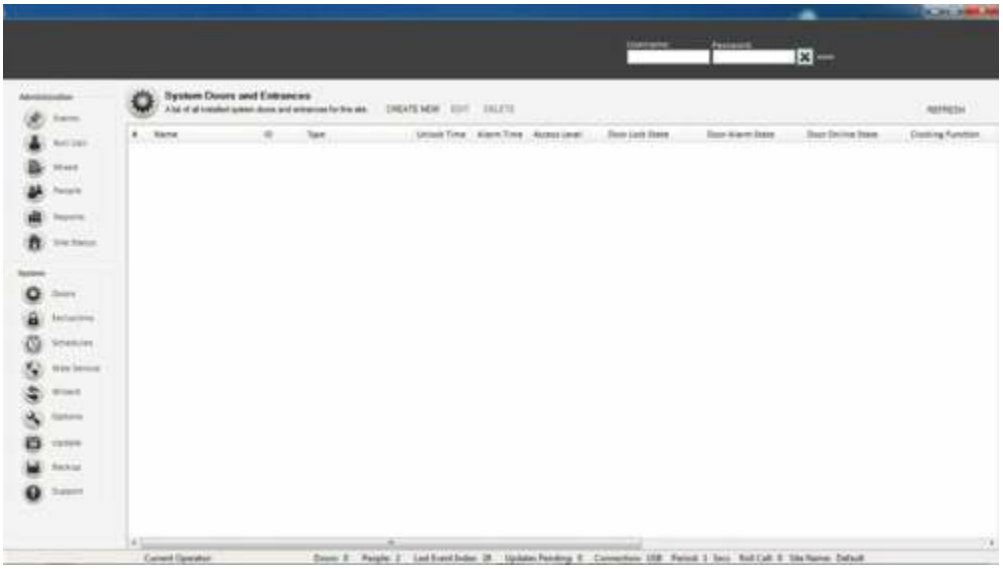
credentials you will need to contact Technical Support. Please also observe that usernames & passwords are case sensitive.

Initial Setup

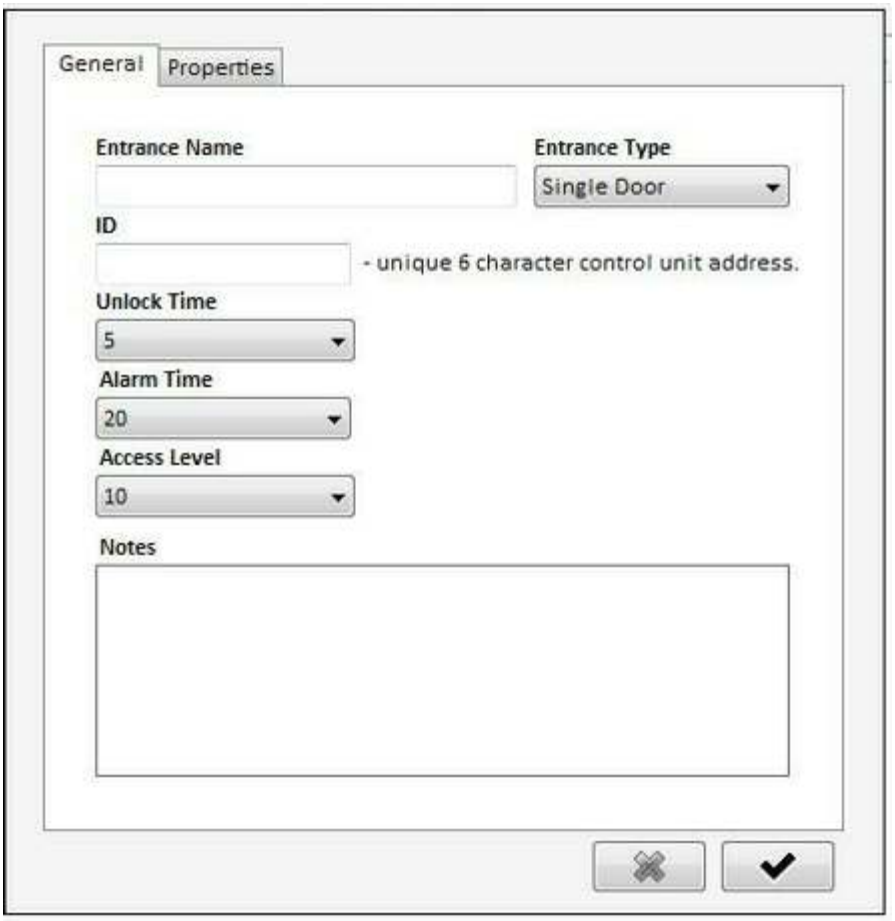
The following section will deal principally with the initial setup and proving of your secured doors and entrances. We will see how to setup a basic configuration to enable full system testing before dealing with the day-to-day functions.

Creating Doors & Entrances

All doors and entrances for your system must first be declared and created as records in the Site Manager Database. To do this you must first login with system privileges and select the doors option from the navigation panel.



Displayed in the information panel is a summary of all your current defined door records. In this case the summary list is empty as no doors have been created. Select the CREATE NEW option above the empty list summary.



There are many field options across two property tabs but for initial testing and proof of operation we need only define two key parameters. The first is a fully descriptive name for our door or entrance which will be used by the system as a label for event activity from now on. Enter the text description in the Entrance Name field i.e. Front Entrance Door. The second compulsory field is the ID information which is the unique electronic serial number of the local door electronic controller as printed on a white label on the printed circuit board. This unique electronic ID consists of a 6 digit value i.e. 'BBF4C6' and enables the Site Manager application to identify and communicate with this door or entrance. Enter this information in the ID field. We can optionally modify or specify other parameters at this stage and an explanation of these are as below:

Unlock Time – this setting defines the amount of time in seconds the door or entrance is unlocked after an exit button or valid card activation. The range is 1 to 30 seconds. In the case of automated gates, turnstiles or barriers that have separate control electronics a general setting of 1 second (trigger) isrecommended and for a normal access controlled door about 7-10 seconds is normal.

Alarm Time –if after a door or entrance is held open too long or a door is forced or defeated by malicious means a local alarm can be triggered and a host event message relayed after a certain period of time. This time in seconds can be

defined here. Please note that if this functionality is required please check with your installer that a magnetic door contact sensor has been fitted to all doors requiring this alarm detection function.

Access Level – the security access level value defines the normal level of security for this particular door or entrance. The higher this number then the greater the level of security will be as only people with there personal access level equal to or greater than this setting will gain access. The normal access level setting may be overridden by defined System Schedules which are discussed later.

Notes –the notes field allows free entry of text for your own use relating to the door or entrance and can be altered at will.

Reader Type – your installer will provide information on the type of reader that is installed at the associated door or entrance. This information does not alter the operation of your system so if you are not sure leave this setting in its default state. One exception to this rule is when you have a Card & PIN high security reader connected at any entry point. In this case you must select the MPROX+PIN option to invoke this mode.

Exit Function – your installer will provide this information if required as to the exact functionality required from this door or entrance input. If you are not sure or you are aware that at Exit Request Button is fitted at the associated door or entrance leave this setting in its default state.

Clocking Function – doors and entrances when used generate access control messages that are stored in the historical database for later report analysis. If we only require this standard function then we keep this setting in its default state of 'None'. It is also possible when individuals access through a door to update their personal record displayed on screen with the last door or entrance used with the time and date attached. If this functionality is required for this door or entrance then select the option 'Logging'. Additional to the logging function, we may at strategic doors and entrances want to clock an individual on or off-site for the purposes of Roll Call. If this functionality is required please select the option 'Clocking'.

Adding a Cardholder

The People view provides you with a list of all people (cardholders) for the current site installation. You can add, modify, disable or remove people as you wish. Additionally, if you select an item or entry on the list and click the right mouse button we can see a range of other options available. To add a new person or cardholder, select the link CREAT NEW and the record entry form isdisplayed. There are many fields available for completion including the ability to place a small (150px by 150px) image of the individual in to their record. Essential fields include Forename, Surname and the 8 digit unique card number which is printed on Smart.Net-IP proximity cards and tags. To understand the numbering please observe on the proximity card or tag an eight or ten digit number sequence. To administrate this number correctly in to the card number field, enter the last 8 digits printed on 10 digit tokens and the entire 8 digits on 8
digits based tokens. If you require this person to also have administrative access

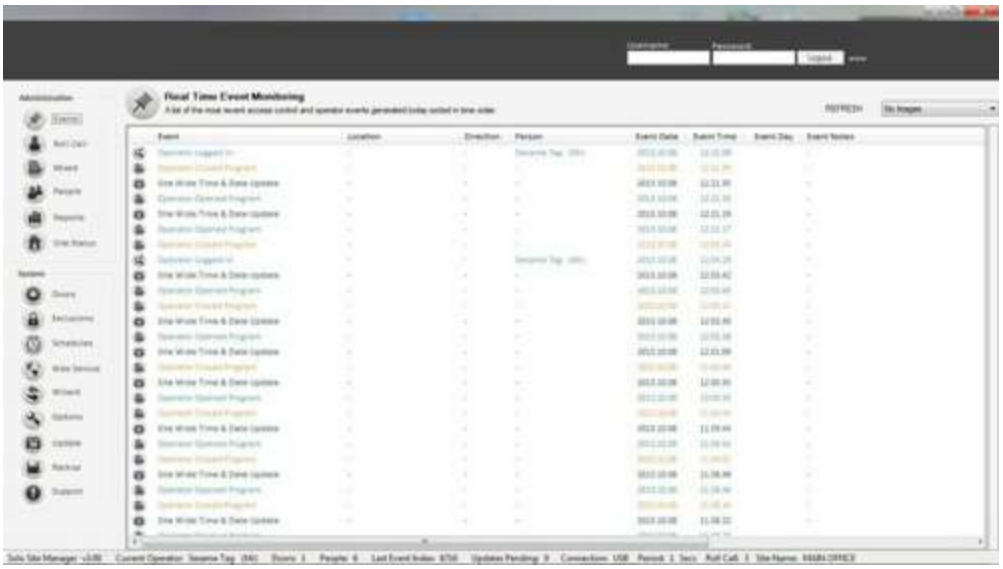
rights to the Site Manager software we can enter a unique username and password and select their programming rights type. Once all essential fields have been entered and any additionally optional fields you may select 'Ok' to commit the record to the site database. The record entry form will always check that your date entry is complete and valid so if the record form does not close please check all fields and data entry validity.

Administration Functions

The administration processes are protected by a username & password that should have been provided by your System Operator. Administrative functions are defined as processes that will be carried out on a regular basis such as people addition, editing, suspension, removal, historical audit report production and manual door override control. The administration processes do not include the addition or modification of the existing site installation definitions or core predefined operating parameters.

Event Views

The Events View which is selected by default initially displays a list of the most recent events that have occurred. The Events View allows you to view real time system & host activity as it happens and provides a snap-shot of the latest audit history. The Event View is visible and updating even when logged out. Additionally you can display images of people that have recently transacted successfully through your doors and entrances. Simply select the appropriate door or entrance name from the drop-down list box to display real time images associated with activity at the chosen door or entrance. The Events View list can be sorted in a pre-defined manner which is defined only by the System Manager.

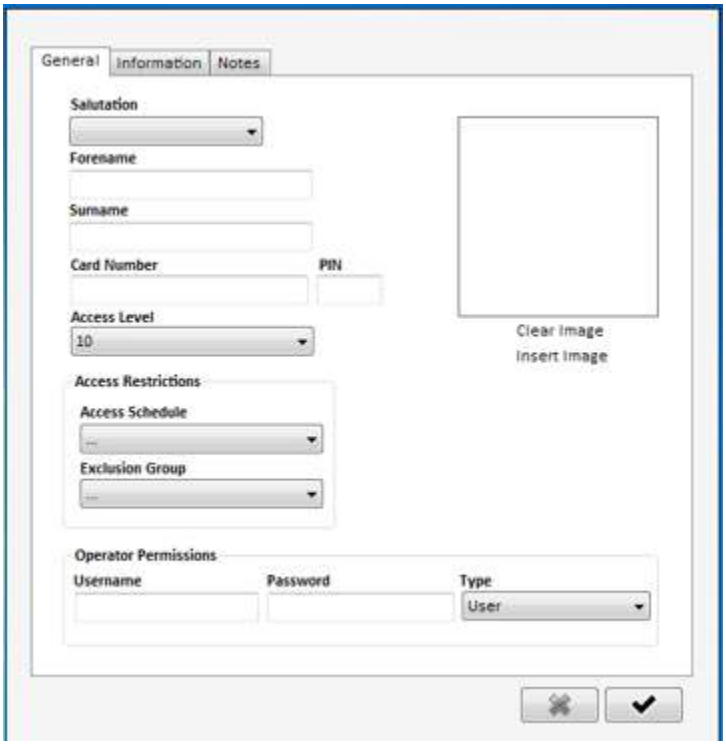


Possible sort criteria are - by the last 500 events with the most recent at the top of the list, all events for the current day and the last 500 events recorded in the history database with the most recent at the top of the list. As with all the list based tables you may size the columns manually by grabbing and moving them with your mouse.

People

The People view provides you with a list of all people (cardholders) for the current site installation. You can add, modify, suspend or remove them as you wish. To add a new person you must select the 'Add New' link. If you select an item or entry on the list and click the right mouse button we can see a range of other options available. Please not that after a person is created or modified the information is automatically updated to the relevant doors or entrances for full offline operation.

To add a new person or cardholder, select the link 'Add New' and a record entry form is displayed. There are many fields available for completion including the ability to place a small (150px by 150px) image of the individual in to their record. Essential fields include Forename, Surname and the 8 digit unique card number which is printed on all Smart.Net-IP proximity cards or tags. To understand the numbering please observe on the proximity card or tag an eight or ten digit number sequence. To administrate this number correctly in to the card number field, enter the last 8 digits printed on 10 digit tokens and the entire 8 digits on 8 digits based tokens. If you require this person to also have administrative access rights to the Site Manager software you can enter a unique username and password and select their programming rights type. Once all essential fields have been entered and any additionally optional fields you may select 'Ok' to commit the record to the site database. The record entry form will always check that your date entry is complete and valid so if the record form does not close please check all fields for correct data validity.



Access Level – the desired security access level that this individual will have compared with the door security access level. The Access Level logic is as below:

Person Access Level >= Door Access Level = Access Granted

Person Access Level < Door Access level = Access Denied

Access Schedule – the access schedule number defines an additional active time window that only card holders with the corresponding access schedule number gain access when it is activated by a Security Schedule. If the card holder doesnot have an access schedule number applied then they will gain access as normal regardless of the doors Access Schedule status. The Access Schedule logic is as below:

Person Access Schedule = Door Access Schedule + Access Level Valid = Access Granted

Person Access Schedule Not Set + Door Access Schedule Set or Unset = Access Granted

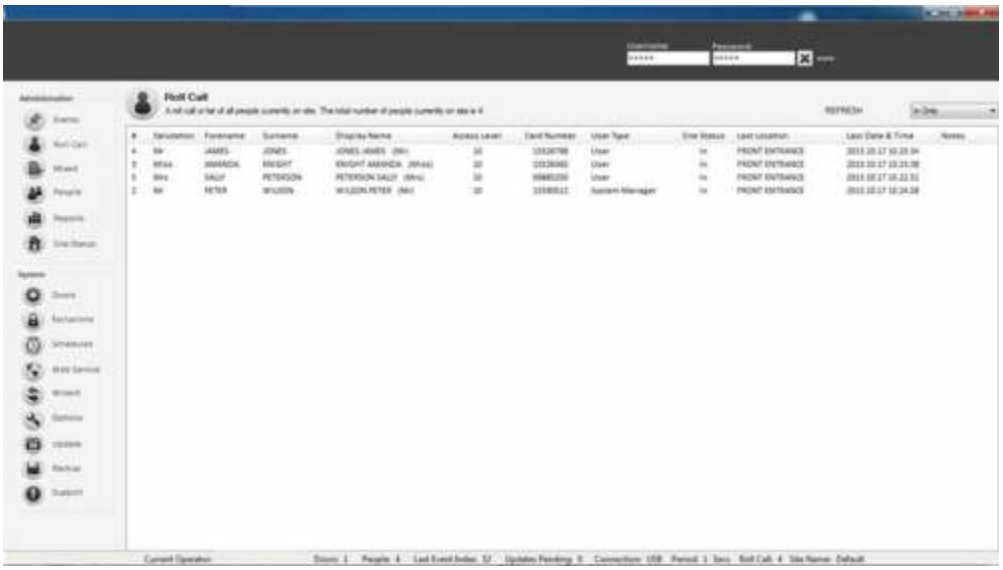
Person Access Schedule Set <> Door Access Schedule = Access Denied

Access Exclusion Group – under normal conditions a persons access control permissions are set by their current access level setting and the current door or entrance access level setting which may be fixed or changed dynamically through the use of Security Schedules. While this method is a fast and efficient way of issuing access control permissions for the site, it may on occasion be desirable to disable a persons access permissions for a given door or collection of doors. For this reason we have the function Exclusions. With Exclusions you can create a small group of doors that can later be applied to a person's record that will supersede their normal access level permission and deny access at these doors or door.

To open or modify an existing person (cardholder) you can either right click on the relevant list record and select 'Open Record' or double mouse click on the list record. After this is done the record form is displayed and you may alter certain fields, change access level rights or add additional information. If you wish to cancel or suspend a persons access control privileges you can simply set their access level value to 0. To restore their access control privileges then you can open the record once again and establish a new appropriate access level value at a later time.

Roll Call

The Roll Call view displays a real-time list of all people currently on-site or on and off-site depending on the optional selection. People are classified on-site when they have accessed through any door or entrance that is designated as a clocking point. In order to be clocked off-site then they must exit by card through similarly classified doors or entrance points.



If a door or entrance is defined as a clocking point then the Roll Call view will automatically update the last known door or entrance used with time and date information attached for all people. Your System Operator should have defined the clocking points for your site installation and can not be modified at administrative level. You can switch the view to display in only or in and out information.

Reports

The Reports view allows you to run a detailed audit report on historical information contained in the current site history database. There is a selection of audit report types available as follows:

All Events – allows the generation of all system and host based event types.

Access Control – allows the generation of only system based access control related event types.

Operator Control – allows the generation of only host operation based event types.

Alarms & Warnings – allows the generation of only door or entrance related high priority alarm & warning based events.

Once the desired audit report type has been selected then the administrator may enter further report criteria to narrow the search results. The report will be viewed on screen and can be printed after completion.

Site Status

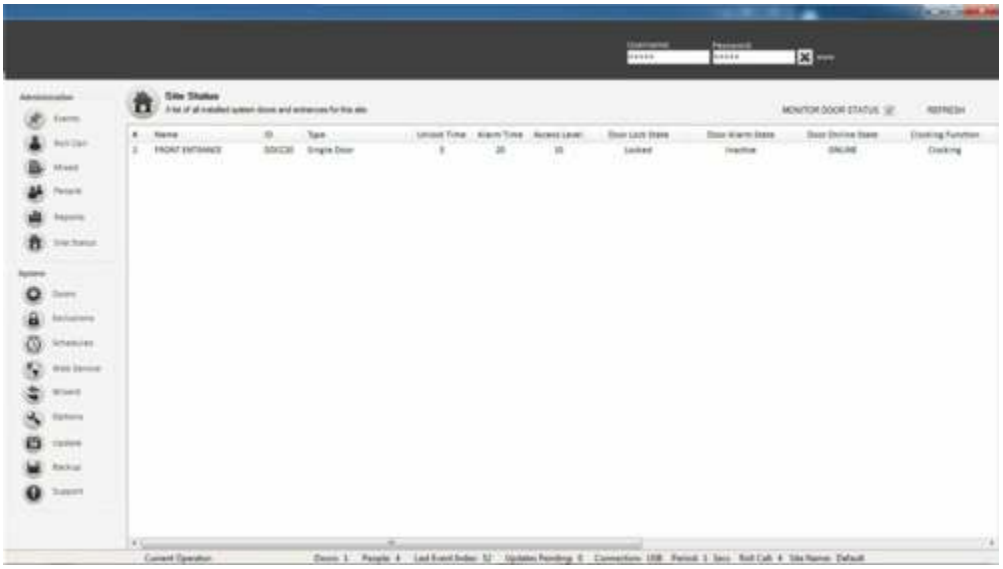
The Site Status view permits a valid administrator to monitor the current door parameters and states. Additionally, if you right click on the doors list you will be offered a range of override control functions for each door or entrance asfollows:

Grant Access – selecting this option for a particular door or entrance opens the door for the predetermined time setting of just a few seconds.

Unlock – overrides all normal access control rules and operation and unlocks the door by manual administrator intervention until manually restored later.

Restore – restores the normal access control rules and operations after an unlock function has been actioned.

Reset Alarm Status – after a door or entrance has entered the alarm state, usually as a result of a door or entrance being forced or held open too long then the physical condition of the door must be inspected and remedied. After thisthe administrator can reset the alarm flag state of the door by selecting thisfunction. If the door alarm state condition is not physically inspected and restored then the door alarm state will immediately fall back in to the alarm condition requiring some possible repair or remedial action.



If you wish to continually monitor all your door and entrance states you can have the view automatically update by selecting the 'Refresh' option once or periodically by selecting the 'Monitor Door States' option check box.

System Functions

The system functions are grouped for those that are changed infrequently. These functions should be used by skilled operators as their use are often system wide and can make significant operational differences to global system operation. The system functions are protected by a username & password that should have been provided by your installer.

Doors & Entrances

Selecting the Doors menu items displays a list of all defined doors or entrances for your Smart.Net-IP installation. Also displayed is a summary for each door or entrance of the associated settings. It is possible as a System Operator to add, edit, override or remove system door or entrance definitions. If this is a new

installation then there will be no doors or entrances defined and thus no information in the list. To create a new door or entrance definition select 'Add New' where you will see the Door form displayed. Select a suitable description for the door or entrance and select the door or entrance type from the dropdown list. Other fields and selections are defined below.

ID – this field is populated with the unique 6 digit hexadecimal door identification code. This ID code is found on a label of the door control electronics installed locally at the relevant door or entrance. Your installer should have provided you with this information but if not careful inspection inside the door controller will reveal this code. This 6 digit ID code is unique to that door or entrance control electronics and must be interpreted and entered into the ID field correctly. An example of a valid ID code is FFBB34. The unique ID code recognises that door or entrance on the access control network rather like a house number in a street of houses.

Unlock Time – this setting defines the amount of time in seconds the door or entrance is unlocked after an exit button or valid card activation. The range is 1 to 30 seconds. In the case of automated gates, turnstiles or barriers that have separate control electronics a general setting of 1 second (trigger) isrecommended and for a normal access controlled door about 7-10 seconds is normal.

Alarm Time – if after a door or entrance is held open too long or a door is forced or defeated by malicious means a local alarm can be triggered and a host event message relayed after a certain period of time. This time in seconds can be defined here. Please note that if this functionality is required please check with your installer that a magnetic door contact sensor has been fitted to all doorsrequiring this alarm detection function.

Access Level – the security access level value defines the normal level of security for this particular door or entrance. The higher this number then the greater the level of security will be as only people with there personal access level equal to or greater than this setting will gain access. The normal access level setting may be overridden by defined System Schedules which are discussed later.

Notes – the notes field allows free entry of text for your own use relating to the door or entrance and can be changed at will.

Reader Type – your installer will provide information on the type of reader that is installed at the associated door or entrance. This information does not alter the operation of your system so if you are not sure leave this setting in its default state. . One exception to this rule is when you have a Card & PIN high security reader connected at any entry point. In this case you must select the MPROX+PIN option to invoke this mode.

Exit Function – your installer will provide this information if required as to the exact functionality required from this door or entrance input. If you are not sure or you are aware that at Exit Request Button is fitted at the associated door or entrance leave this setting it its default state of exit button.

Clocking Function – doors and entrances when used generate access control messages that are stored in the historical database for later report analysis. If we only require this standard function then we keep this setting in its default state of 'None'. It is also possible when individuals access through a door to update their personal record displayed on screen with the last door or entrance used and direction with the time and date attached. If this functionality is required for this door or entrance then select the option 'Logging'. Additional to the logging function, we may at strategic doors and entrances want to clock an individual on or off-site for the purposes of Roll Call. If this functionality is required please select the option 'Clocking'.

Security Schedules

Security schedules are automated tasks that are performed on or off line by the system doors and entrances at predefined times on a specific day of the week. For example, we may want to define a schedule to unlock the Front Entrance Door at 08:00 on a Monday to give free-access to all people and then secure it again to at 10:00. Another use for schedules is when we wish to automatically raise or lower the security access level of a door or entrance throughout the day and week. You can define up to 40 schedules per door or entrance but it is recommended to keep to as few as possible to avoid over complicating the security structure. When we select the Schedules option a list of all current schedules is displayed with their use and properties attached. To define a new one, select the 'New Schedule' option. Enter a descriptive name for the schedule of your own choice and then complete the remaining fields as explained below:

Description – select a descriptive name for this schedule.

Door or Entrance – select the door or entrance where this schedule applies.

Entry Security – select the type of security access method at the entry reader.

Start Time - the time that the schedule will be active on the selected day. The time range is 00:00 to 23:59.

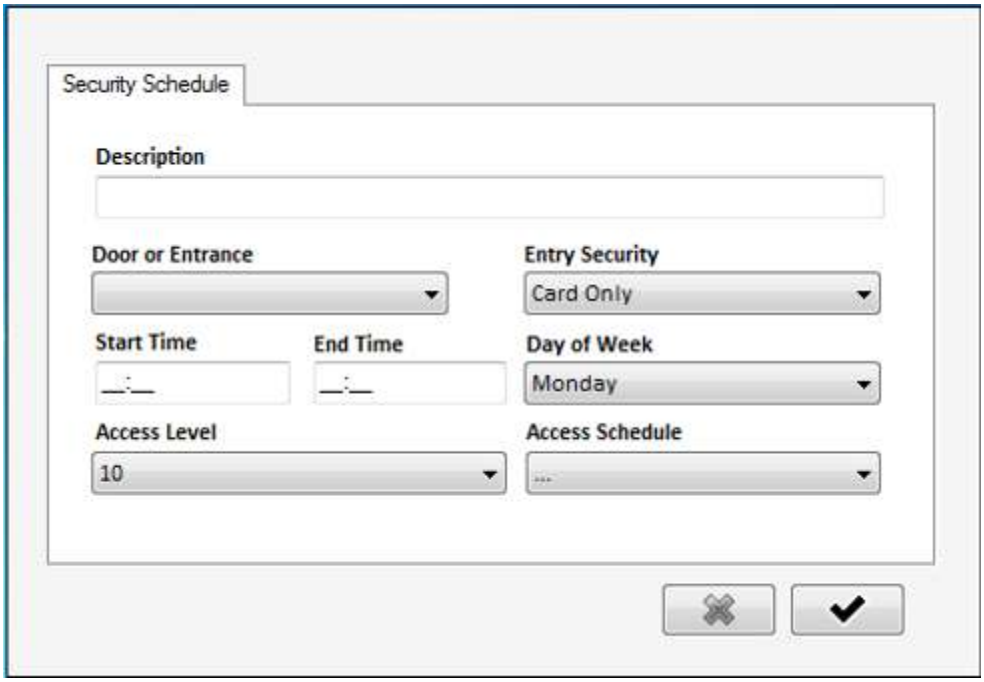
End Time – the time the schedule will expire on the selected date. Please not that the schedule end time is to the end of the minute so an end time of 11:59 will in actually fact expire at 12:00 midday. The time range is 00:00 to 23:59.

Day of Week – select the day of the week that the schedule will be activate within the boundary times. You can also select all Week, Weekend and Weekday to create multiple schedules and save time.

Access Level – the desired security access level that will be set for the door or entrance within the active time range and day of the week. If we wish the door or entrance to be in free access or unlock automatically then select the access level of 0 (unlocked).

Access Schedule – the access schedule number defines an additional active time window that only card holders with the corresponding access schedule number

gain access. If the card holder does not have an access schedule number applied then they will gain access under this condition as normal.



The System Operator can define new and delete existing schedules. If you also right click on the schedules list a small menu appears that allows you to delete or refresh any individual schedule. Please note, when a new schedule has been defined it is normally automatically issued to the appropriate door or entrance directly and is stored there for full on or off-line operation. Please define your schedules carefully and always try to avoid overlapping schedule times and creating contradictions in access level state.

Security Schedules – Card & PIN Operation

Please note, to use CARD & PIN operation then your door controller must be of Firmware Version 7 or above. Please check with support by providing you 6 digit serial number or numbers if you are unsure.

Access Exclusions

Under normal conditions a person's access control permissions are set by their current access level setting and the current door or entrance access level setting which may be fixed or changed dynamically through the use of Security Schedules. While this method is a fast and efficient way of issuing access control permissions for the site, it may on occasion be desirable to disable a persons access permissions for a given door or collection of doors. For this reason we have the function Exclusions. With Exclusions you can create a small group of doors that can later be applied to a person's record that will supersede their normal access level permission and deny access at these doors or door. To establish an exclusion group select the Exclusions function from the navigation panel and CREAT EXCLUSION GROUP.

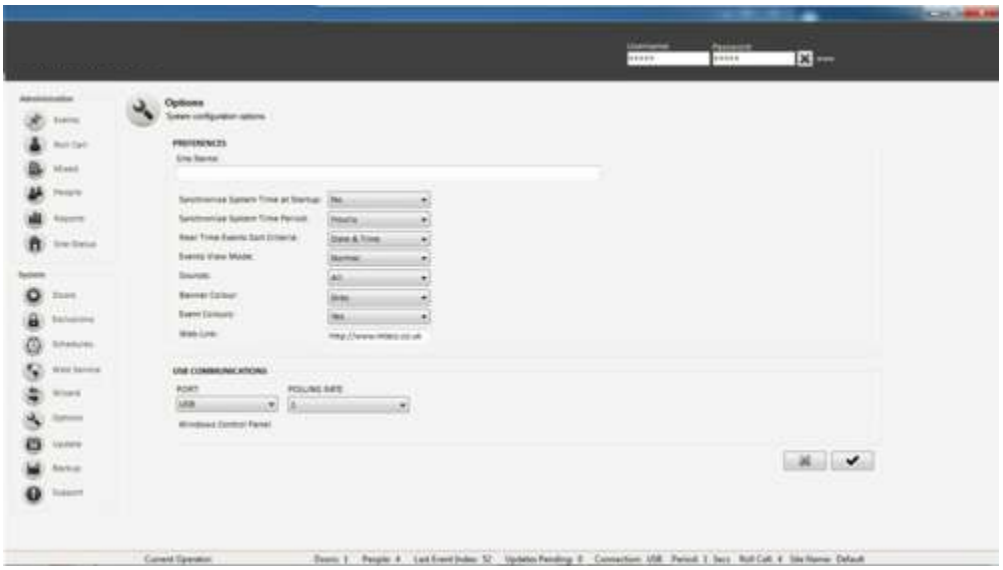
You must enter a descriptive name for the group and you may assign up to 5 doors per group. You can create 128 exclusion groups but only one can be applied to a person's record at any one time. In order to do this you must create a new record or edit the person's record from the People function. The system will automatically update any changes made to your doors and entrances if you are currently connected and online.

Wizard

The Wizard is a utility that allows a system level operator to correct any host and system disparities caused by extensive off-line operation and administration. The wizard prompts you for each function available, but please take care to read the information and understand the task before selecting its operation. Most functions within the wizard may take a few moments or even minutes to complete so you may need to wait for these updates to fully take effect at the doors or entrances.

Configuration Options

The Options screen allows you to adjust certain settings that may be relevant to your installation. In most cases the default options set at software installation are adequate but below are an explanation for all the settings that you may change.



Preferences

Caption – it is possible to display a single line message on the main software application in the header bar that is specific to you as the end user, such as the site installation name or the security installer's name and contact details.

Synchronise System Time at Startup – if you require the computers time & date to be updated to all the doors and entrances when the Access Solo application is launched then select the option 'Yes'. If you use the system extensively in off- line mode then it is recommended that this option is set to 'No'.

Synchronise System Time Period – if you require the computers time & date to be updated in all the doors and entrances on an hourly basis then select the option 'Yes' (recommended). If you use the system extensively in off-line mode then it is recommended that this option is set to 'Never'.

Real Time Events Sort Criteria – select your preferred list sorting criteria for the main events window.

Events View Mode – if you wish to have the Roll Call view displayed on the same screen as the Real Time Events then choose the 'Mixed' option.

Sounds – a selection of options that allow sounds to be played through you computer speakers to indicate process events and punctuate menu navigation.

Banner Colour – a choice of top banner colours for your personal preference.

Event Colours – on the real time events screen differing events are shown by default in separate colours. This option allows you to turn this off to a fully black grid.

Web Link – as standard the WWW link on the top banner acts as a hyperlink to Smart.Net-IP, but this can be changed here. The link can be of the http:// to

jump to a website of your choice or a mailto: link to allow the customer to email anywhere of your choice.

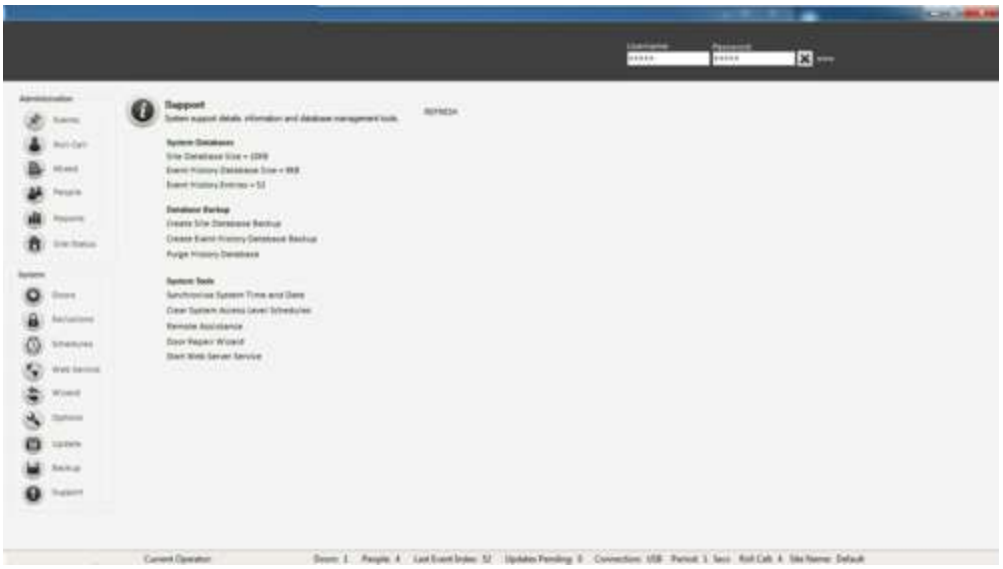
USB Communications

Port - under normal conditions the USB adapter that connects your doors and entrances back to your computer is detected by the Site Manager program automatically and the channel set to USB. In most circumstances you will never need to change this setting as this is the most efficient and fast communication method. If you wish to use a legacy virtual communication port number (COM) instead, then you can select it here. To ascertain the correct communications port number, select the 'Show Control Panel' option and choose System –Hardware – Device Manager. In the list of devices displayed look for an entry described as Ports (Com & LPT) and there should be an entry for 'USB Serial Port'. Next to this entry you will see the communications port number associated with the USB interface. Please transpose this setting in to the Port options selection. Once the setting is made correctly then select 'Save Options' to start communications through this new communications port number.

Polling Rate – this option defines the period the system software and its databases are updated with new information generated at the doors and entrances. An appropriate general setting is between 3 to 10 seconds.

Data Management

The data management functions are available through the Support function from the system function of the navigation panel. Select this option and the resulting view will be available in the information panel:



In this view we can see lots of information about your databases, their size and number. There are also a number of useful links to the World-Wide-Web as well as information on any support license agreements you may have purchased.

Databases

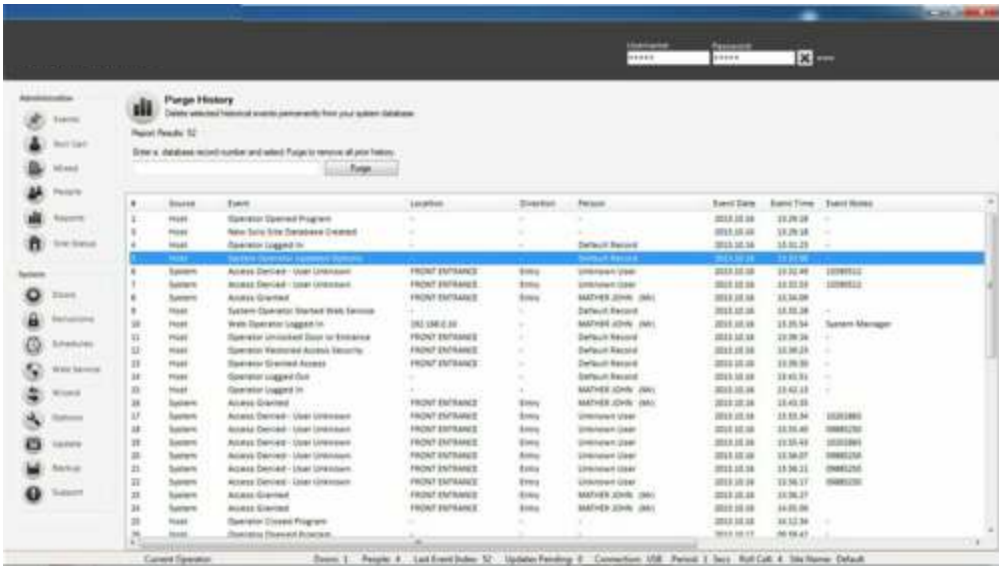
The Smart.Net-IP Site Manager program creates two independent SQL database files in the SOLO directory that can be found in the root of your hard disk drive. The two files are mySoloISite.db and mySoloHistory.db. The first of these files contains all the unique setup information for your site installation including all people information, door parameters, access permissions, usernames and passwords. The second database file contains all of the historical events generated by access control activity and host programming detail. It is important to make regular backup copies of these database files and store them on another computer as this information if lost, can not be recovered. When you attempt to copy these files it is recommended that you close the Solo Site Manager program and reboot your PC prior to the file copy.

Database Backup

An alternative or in addition to a manual database copy described in the previous section is to use the system backup and replication solution from the support menu. Also you can purge your events database mySoloHistory.db of records from a selectable entry back in time to shrink its size and make it more manageable.

To create a copy of either the Site or History databases please select this option from the support menu. A file dialog box will be visible asking you for a location and name for the file. You can accept the default name and location or change them as you wish. This function creates an exact copy of the database file.

In the case of the mySoloHistory.db this can get quite large over time as it contains all events that have occurred. The exact size and growth rate depends on your system size and the number of door and entrance activations. When this database becomes very large then it may be prudent to create a backup of this database file prior to performing the purge function. Once the backup has been created select the Purge History Database function.



Please note, if the history database is particularly large then this view could take some time to build so please be patient. The view will display all events in the current history database sorted with the most recent at the top travelling back in time as you scroll down the list. In the first column is a unique number for each historical event.

Historical Events Purge

To perform the events purge scroll down the list until you come to the date and time where you wish to purge from. Enter the event number in the top data entry field or double mouse click on the event row and then select the Purge button. The system will prompt you for confirmation so please confirm if you wish to indeed perform the purge. Once the purge is complete then the view will be updated. If you have done a backup prior to the purge then the process is completely reversible.

Web Workstations & Remote Management

Your single installation of Smart.Net-IP Site Manager includes built-in capability for operating and managing your site installation remotely. You can manage your site from any PC in your building through its web browser or on portable devices such as Tablets and Smart Phones.

Activating the Web Service

In order to enable remote web workstations and the built-in web service you must turn this on from the Site Manager Software. From the System menu select the option Web Service. After a moment a browser window will appear from your default web browser that allows you to administrate your system through this interface.

Intranet Web Workstation

After activating the Web Service the address bar in your favored browser displays the local intranet address that can be used on any workstation or connected device to your LAN or local network. You must enter the full address including port number as http://theipaddress:4001. This view can be used for all large screened devices such as Desktop PC, MAC, Android and Tablets. All facilities

are available through your operator credentials apart from functions that relate to the hardware installation.

Mobile Optimised Working

For small screened devices such as some smart phones and smart appliances the above service may be hard to use because of its graphical nature. For this end there is a further WAP enabled service that is optimized for the small screen. In order to access this service you mast add / mobile to the IP address as detailed above to give http://the ipaddress:4001/mobile.

Working Across The Internet

The above methods are relevant when remote working inside a building or as part of a local network. It is also possible with the correct infrastructure, to open up the ability to access the web services of Access Solo from any external Internet enabled device from anywhere in the world.

In order to achieve this, the host computer that is actively running the Smart.Net-IP Site Manager application must be connected to the Internet and be able to accept incoming remote connections through the port 4001. In reality this is done by your router switch device that is connected to your ISP and setting up a port-forward for port 4001 to the Smart.Net-IP site manager machine IPaddress. Remote users would then navigate remotely using your ISP generated IPaddress (external IP address) and the port number 4001.

This can be a complicated topic and it is recommended that you contact Technical Support if you are unsure in anyway.

Troubleshooting Guide

The following table details possible reasons & remedies to common problems that may be encountered with the Smart.Net-IP software and associated doors and entrances:

Symptom	Cause	Remedy
I do not appear to be USB communicating with all my doors or entrances	USB interface unplugged	Plug in the USB interface in to a spare USB2 port on your computer
	The communication port for USB interface is not defined or incorrectly defined on the OPTIONS screen	Check in the Control Panel - System - Hardware - Device Manager that the correct communication port has been defined on the OPTIONS screen or is set to USB in the Site Manager Options menu
I have checked in the Control Panel and there is no specification for my system USB interface under COM/ LPT	Missing Solo USB Device Driver	Close down the software application, contact technical support to download and install the latest USB interface driver.
I do not appear to be communicating with one or some of my doors and entrances	Door not defined	At System Operator level define the doors that are missing
	Incorrect electronic ID	Check on the electronic door control unit that the correct unique ID has been entered in the door definition record correctly
	Power missing at door	Check that the access control reader LED's are on and power is connected to the door control unit. Call installation engineer
	Installation error	Call installation engineer
My system events are slow to update on the Events screen	Long polling period set on the OPTIONS screen	At System Operator level change the polling rate to a lower setting (seconds)
My system generated times are inaccurate against my computers core time	Time & Date has not been synchronised	At System Operator level select SUPPORT and Synchronise System Time and Date. Additionally you could select the update hourly setting in the OPTIONS screen to

		maintain closer core and system times
People are entering through a door or entrance and not appearing on the Roll Call as on-site	Door definition error	At System Operator level ensure the door definition has the Clocking function set to 'Clocking'
People are exiting through a door or entrance and not removed from the Roll Call as off-site	Door definition error	At System Operator level ensure the door definition has the Clocking function set to 'Clocking'
A defined Security Schedule is not firing correctly	Door or entrance time & date maybe incorrect or inaccurate	At System Operator level select SUPPORT and Synchronise System Time and Date. Additionally you could select the update hourly setting in the OPTIONS screen to maintain closer door and system control times
	The schedule has been defined incorrectly	Delete schedule and recreate it with the correct parameters
	The schedule is contradicted by another	Check the full schedules list and delete the contradicting entry
	The schedule is corrupt at the door or entrance	Use the Synchronise feature and then refresh all schedules from the scheduleslist.
	DCU2 Firmware Version	Check firmware version is V7 or greater for software release V3.02 or greater
My door or entrance parameters do not perform as stated on the doors menu	System door parameters not synchronised to host	At System Operator level open the door record and select OK to refresh all door parameters for the specific door or entrance
A door or entrance is unlocked and the green LED displayed	Free access schedule active	Remove the free access schedule
	The host has unlocked the door or entrance (override)	At Administrator level check the manual override status on the Door Control screen and restore (right mouse click)
	Exit button or installation fault	Call engineer

Appendix A

The following sections detail information relating to the access control system hardware installation. They replicate instructions that are also provided with the appropriate additional electronic components or sub-systems.

Smart.Net-IP Door Controller Installation

Best results will be achieved when following these instructions as they describe the planning and installation of a single door or entrance. A wiring diagram with notes is shown below that states clearly all the common associated devices that may be required for each single door installation. The main circuit board can be removed during enclosure installation but must be stored and handled with care.

Planning

The Smart.Net-IP single door control unit is designed to be installed locally to the door or entrance it will serve in a dry internal location. This allows all cable connections to be short and efficiently run. All connections are made by removable side-entry polarised screw terminals designed for multi-stranded cable types. For all connections, apart from the networking cable and readers you may use low cost intruder alarm cable. All cables entering the door control unit housing must not be coiled up inside but routed efficiently through the various edge and rear cable entry knockouts and drill points of the enclosure.
Cable tidy anchor points are provided with suitable cable ties. Please ensure that the rear enclosure mounting screws do not foul the PCB or terminals.

Power Supply

The control unit can be powered from a single low voltage DC regulated supply only. The voltage input range must be between 8 to 16 Volts DC, ratings outside of this may cause damage to the control unit and / or its associated devices. The Smart.Net-IP single door control unit has been designed for low power operation. Its quiescent current is only 80mAmp rising to 200mAmp with both proximity readers connected and the lock and alarm relays energised.

Always use an individual power supply to power each door and its associated local components in isolation. Never share the power supply between adjacent door controllers as ground loops may be created that can cause communication bus faults. Choose linear power supplies and not switch mode types. The current capacity of the PSU should be greater than the locking peak current consumption by at least 200mAmp (0.2A).

Networking Cable

The communication or networking cable type may be a Belden type or equivalent #8132 or #9842. These cables are of a multi-stranded construction and have good resistance to mechanical stress. The use of CAT5/ 6 or similar cable is not

recommended as its solid core construction breaks easily under mild mechanical stress. The total networking length must not exceed 1.2KM (1200M) and contain any spurs or star points. You can connect up to 128 door control units on one continuous network cable installation.

End of Line Termination

In the last door control unit which is the one furthest away from the PC interface connection you must employ end-of-line resistor termination. Connect the two 120 Ohm resistors provided with the USB-485 Adapter, one across the last controller terminals T+ & T- and the other across R+ & R-. To check that the termination is correct, disconnect the USB interface from the computer and measure with a multi-meter set on the resistance range that you can read between 60 to 70 ohms across the T pair and again across the R pair. The exact readings will depend on the total networking cable length and its resistance.

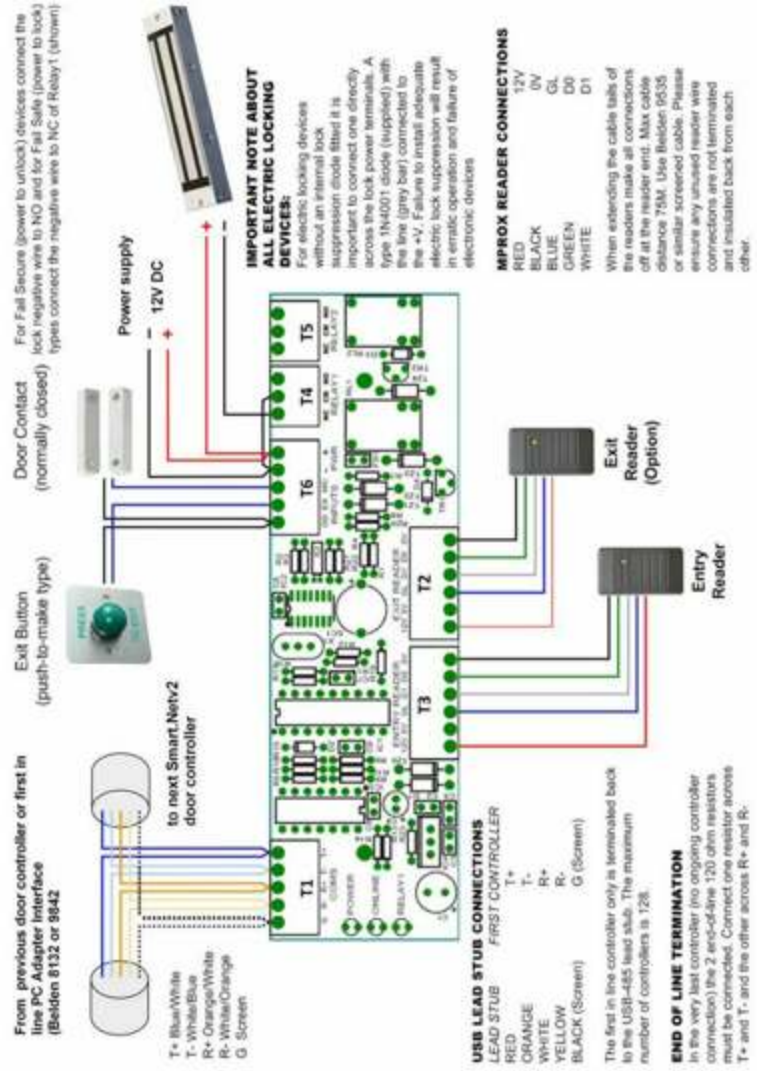
Relay 2 Output

The relay 2 output can be used to indicate if the door or entrance is in the alarm state locally to the door or entrance. An alarm state condition is generated when the door magnetic contact is fitted and the door is forced ajar or left open too long. Any general purpose sounder or other device may be switched with a rating not greater that 24VDC at 2 Amperes. The relay 2 has normally open and closed volt free contacts (Form C). If the magnetic door contact is not fitted to any door controller then this condition is automatically detected by the controller and disabled.

Exit Request Input

The exit input is normally used if an exit button is required to gain exit through the controlled door or entrance. It can be reassigned on the software to be used as a general purpose input for other purposes if required. Configurable options available are intruder alarm set detect, power supply fault detect, general tamper input detect and release (free access) all system doors on a single closing contact. By default (factory) the operation is as an Exit Request Button utilised with a push-to-make momentary switch. If the exit button function input is later reassigned by the software application all functions are normally open with a closing circuit for an active state. If the release (free access) all system doors function is required only a single connection at one door control unit is required as the host computer will manage the command for the rest of the system. Never apply a voltage of any kind to this input as damage to the control electronics will occur.

Door controller connections



POWER SUPPLIES:
Always use an individual power supply to power each door and its associated local components in isolation. Choose linear power supplies and not switch mode types. The current capacity of the PSU should be greater than the locking peak current consumption by at least 200mAmp (0.2A).

USB-RS485 Adapter Network Interface Connection

Best results will be achieved when following these instructions as they describe the installation and best practice for this adapter product. The USB-RS485 lead has been designed to simplify the connection of a multi-drop network of door controllers. You can use this product to connect a PC(Personal Computer) to up to 128 door controllers by virtue of a single USB2/3 connection.

Power Source

The USB-RS485 adapter derives its power source from the standard USB2/ 3 port it is connected too. It does not require any additional power sources.

Connections

The connections on the output stub of the USB-RS485 lead will allow the network connection of up to 128 door controllers with single continuous multi-drop door network installation. The connections from the adapter to the first control unit and on to the next etc. are shown below:

LEAD	First Controller	Next Controller…..
RED	T+	T+
ORANGE	T-	T-
WHITE	R+	R+
YELLOW	R-	R-
BLACK (Screen)	G (Screen)	G (Screen)

Two LED's are embedded in the USB connector body. When at least one door is defined and the system software is actively communication with the door(s) then the Red LED indicates a transmission to the door network and the Green LED a reply. With these LED's and the Green LED in each controller any network cabling errors can be remedied easily.

Interface Commissioning

The application software driver must be installed prior to the connection of the device to your PC. The application driver software is installed automatically when you fully install the Smart.Net-IP Site Manager application which isavailable exclusively on download from our website at www.doorentrydirect.com You can also download a separate stand alone installer of the driver if you wish, but thisis not necessary if you are or have installed the Smart.Net-IP Site Manager application.

Once all the network connections have been terminated and the software or device driver has been installed you are ready to plug in the adapter to a spare USB port on your PC. Once the device is recognised messages on your screen will prompt you on the progress of the automatic configuration of this adapter. If the software or driver has been installed correctly prior to the physical connection then this will result in your PC informing you that "The device has been installed correctly" or similar. In the case of Smart.Net-IP Site Manager software application, the adapter should be detected automatically and no further configuration is needed.