AN1072 - Setting up the Net2 software

The following guide provides an overview of the steps required to configure a Net2 installation listed in the best order in which they should be performed. Detailed application notes are also provided.

Doors

The first section to configure when setting up a new Net2 system is Doors. Readers must be configured before areas, access levels, and other sections can be set up.

AN1046 - Configuring readers and keypads

Areas

'Areas' is a feature of Net2 Professional. If anti-passback or roll call reporting is to be used, areas and area group need to be set up. If not, skip to creating Timezones.

AN1023 - Configuring areas and area groups

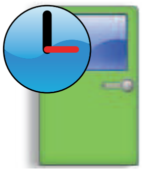
Timezones

Timezones are different times of the day and week when access will be permitted. These should be created/edited before access levels can be fully utilised.

AN1038 - Using Access Levels and Timezones

Access levels

Access levels control where in a building a user is allowed and during what times.



AN1038 - Using Access Levels and Timezones

Departments

Departments allow users to be grouped together enabling quick reporting and viewing of users.

AN1041 - Using Departments

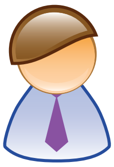
Users

'Users' are people that use the access control system. Users are identified to the system by a card, token or PIN (or a combination of any of these). Once a user has been identified to the system, a decision can be made on whether they are permitted or denied access.

AN1039 - Adding a new user

Operators

'Operators' are users that require access to the Net2 software.



AN1073 - Net2 operators - Adding / Assign privileges

Fire Alarm Integration

Fire alarm integration is a feature of Net2 Professional only.

AN1031 - Integrating Net2 with a fire alarm system

Roll call and muster reporting

Roll call and muster reporting is a feature of Net2 Professional and can be used in conjunction with the fire door unlock feature.

AN1032 - Using roll call and muster reports

Anti-passback

Anti-passback is a feature of Net2 Professional that enhances the security of a site.

AN1063 - Configuring anti-passback

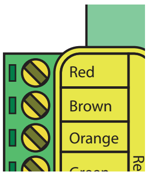
Intruder alarm integration

Net2 can be integrated with an intruder alarm to arm and disarm the system using the access control readers.

AN1035
- Integrating Net2 with an intruder alarm system

I/O Boards

I/O boards can be added to a Net2 system and used for any number of different applications. The boards need to be configured and can then be used is conjunction with Triggers and Actions.



AN1066 - Installing an I/O board

Triggers and Actions

'Triggers and Actions' is a powerful feature, used in conjunction with I/O boards, allowing Net2 to automatically control various systems around a building.

AN1067 - Using Triggers and Actions

AN1079 - Lighting control using Triggers and Actions

AN1080 - Economic control of air conditioning using Triggers and Actions

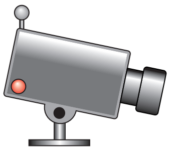
Site Graphics

Site Graphics provide a visual representation of the site, allowing operators to monitor events around the site at a glance.

AN1064 - Using Site Graphics

Cameras

'Cameras' is a feature that allows you to view live images from IP addressable cameras from within Net2.



AN1052 - Integrating IP Cameras with Net2

Camera Images integrated with Net2 Events

Net2 allows integration with camera software to provide digital images to be associated with an event. The camera software needs to be configured before integration with Net2 can take place.

AN1053 - Integrating Net2 with Milestone software
AN1083 - Integrating Net2 with OnSSI software
AN1084 - Integrating Net2 with the JVC NVR
AN1093 - Integrating Net2 with Dedicated Micros software
AN1108 - Integrating Net2 with Pelco software

Timesheet

Net2 can provide basic time and attendance reporting when used with the Net2 Events table. Users, Departments and Operators will automatically appear in the Timesheet programs.

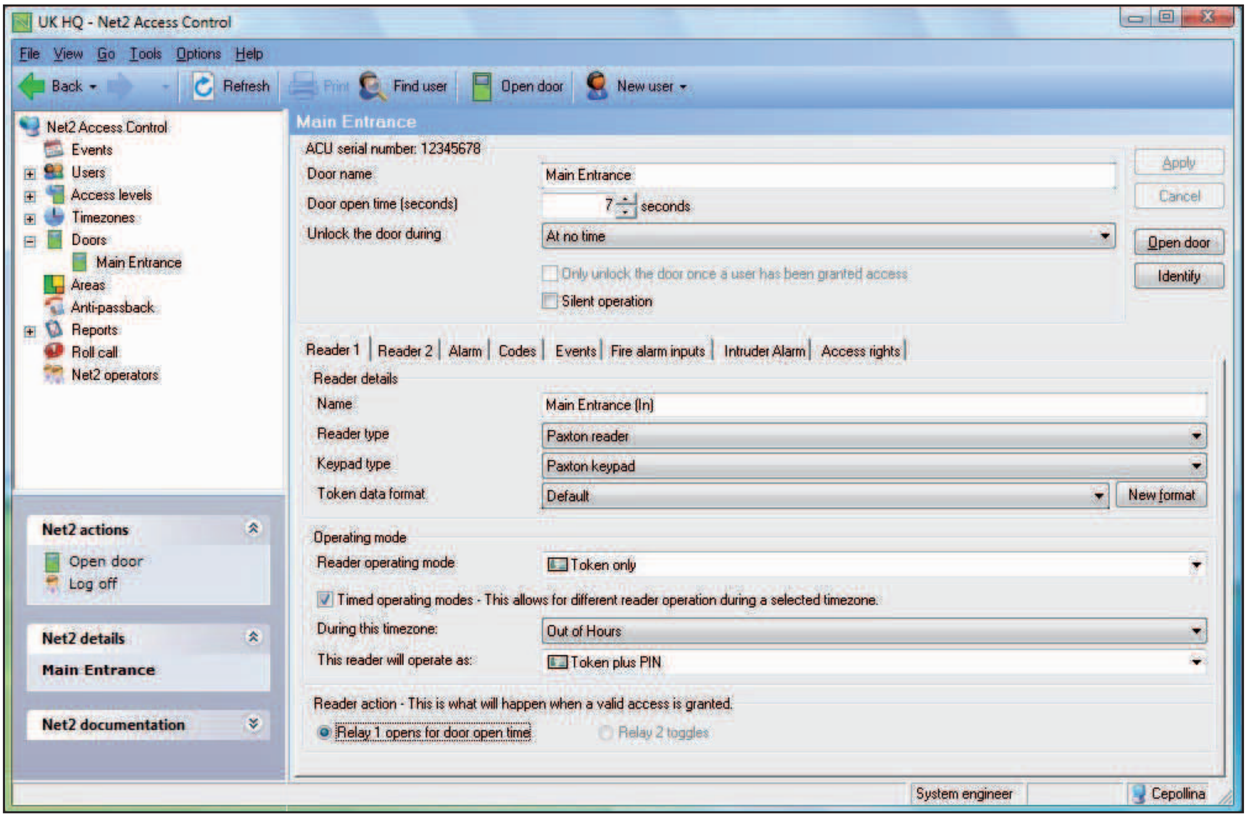
AN1029 - Using Net2 Timesheet
AN1098 - Using Net2 Timeline

AN1046 - Configuring readers and keypads

If the Net2 application is running when a token is presented to a reader or a button pressed on a keypad for the first time, the unit will configure itself in the software automatically.

Some individual settings may need to be set manually. Readers and keypads are configured in the Door settings of each control unit.

The display below shows the settings corresponding to Reader 1 and Keypad 1 connected to that control unit.



UK HQ - Net2 Access Control

Main Entrance

ACU serial number: 12345678

Door name: Main Entrance

Door open time (seconds): 7 seconds

Unlock the door during: At no time

□ Only unlock the door once a user has been granted access

□ Silent operation

Reader 1 | Reader 2 | Alarm | Codes | Events | Fire alarm inputs | Intruder Alarm | Access rights

Reader details

Name: Main Entrance (In)

Reader type: Paxton reader

Keypad type: Paxton keypad

Token data format: Default

Operating mode

Reader operating mode: Token only

☑ Timed operating modes - This allows for different reader operation during a selected timezone.

During this timezone: Out of Hours

This reader will operate as: Token plus PIN

Reader action - This is what will happen when a valid access is granted.

● Relay 1 opens for door open time ○ Relay 2 toggles

Name

The default name for reader 1 is [Door name] (IN). The default name for reader 2 is [Door name] (OUT). The reader names set here will appear in reports and be used to set access levels and areas.

Reader type

This should be set to the relevant type of reader.

Setting	Description
None	If no reader is connected
Paxton reader	If a CARDLOCK or PROXIMITY reader is connected
Clock and data	If a non-Paxton clock and data reader is connected (Paxton readers are clock and data readers)
Wiegand reader	If a Wiegand reader is connected
ANPR - Clock and data reader	If a Paxton ANPR clock and data reader is connected
ANPR - 26 bit Wiegand reader	If a Paxton ANPR Wiegand reader is connected

Keypad

This should be set to the relevant type of keypad. Many third party keypads are compatible with Net2 running v4.18 or later software.
Refer to: *AN1112 - How to configure a Wiegand keypad* < http://paxton.info/1650 >

Setting	Description
None	If no keypad is connected
Paxton keypad	If a keypad is connected

Token data format

Every card enrolled on a Net2 system must have a unique number. The token data format option allows Net2 to read a variety of encoding formats. The default setting is for the Net2 encoded cards and tokens (random 8 digit number). For details on how to set up a new token data format refer to: *AN1045 - Using ABA format 3rd party cards with Net2.* < http://paxton.info/1052 >
AN1125 - Configuring Wiegand 26 bits with a site code. < http://paxton.info/1753 >

Setting	Description
Default	This is for Net2 encoded cards and tokens (random 8 digit number
Paxton token	This is for CARDLOCK and PROXIMITY cards and tokens (encrypted number)
Bank cards	This allows Net2 to use bank cards
First 8 digits	This allows Net2 to use the first 8 digits encoded on the magstripe
26 bit Wiegand	If a Wiegand reader is connected, Net2 is configured to read 26 bit Wiegand tokens
26 bit Wiegand with site code	If a Wiegand reader is connected, Net2 is configured to read 26 bit Wiegand tokens and check the site code.
Custom Wiegand	If a Wiegand reader is connected other than a 26 bit Wiegand reader. A Custom Wiegand format must be first set up in the Net2 Configuration Utility

Reader operating mode

The correct operating mode should be selected from the drop down menu.

Setting	Description
Inactive	There is no reader or keypad connected (or they are inactive for some other reason)
Token only	Access is granted by presenting a valid user token
Token plus PIN	Access is granted by presenting a valid user token AND entering the relevant PIN
Token plus code	Access is granted by presenting a valid user token AND entering a valid code
Desktop reader	A desktop reader is connected. This reader is to be used to add users to the system
PIN only	Access is granted by entering a valid PIN
Code only	Access is granted by entering a valid code
Token or PIN	Access is granted by presenting a valid token OR entering a valid PIN
Token or code	Access is granted by presenting a valid token OR entering a valid code
Token, PIN or code	Access is granted by swiping a valid card OR entering a valid PIN OR entering a valid code
Clocking in reader	For use with Timesheet software. Events from this reader will be sent to the Timesheet software
Clocking out reader	For use with Timesheet software. Events from this reader will be sent to the Timesheet software

The list of operating modes displayed in the drop down menu is dependent on the reader type and keypad type settings.

For example, if a keypad is configured without a reader, the drop down menu will only allow: Inactive, Code only and PIN only.

Difference between Code and PIN

Code

Codes are low security as they are not included in user access levels.

They are set in the individual Door's screen. A control unit can have up to 50 codes between 4 and 8 digits long. When using 'Code Only', Net2 will not be able to track who has entered through that door as no user is specified, only that a valid code has been entered.

Codes are very quick to set up and change. This can be handy for casual visitors entering a non-public area but should be changed on a regular basis as they can easily be disclosed.

PIN

PIN stands for Personal Identification Number. They are 4 digits long and are set up in a user record. PIN's allow the users access rights to be controlled and changed without affecting other users. It also allows them to be identified by the system for reporting purposes.

For added security, both Codes and PIN's can be used in conjunction with a user Token. A user token which has been lost or stolen still requires the specific PIN or Code to be known.

Timed operating modes

This feature allows a different operating mode to be used depending on a timezone. For example, during the day, the door may be set to 'Token only' but out-of-hours this can be upgraded to require 'Token plus PIN'.

To configure this, tick the box, select the required timezone from the drop down menu and the required operating mode from the other drop down menu.

Reader action

This is the action that will happen when access is granted.

Setting	Description
Relay 1 - door open time	Access granted will energise relay 1 for the door open time.
Relay 1 & 2 - door open time	Access granted will energise relays 1 and 2 for the door open time. This is used when fitting two locks on one door.
Relay 1 - toggles	Access granted will toggle relay 1. - The relay will stay energised until a second access granted is made.
Relay 2 - toggles	As above but for Relay 2.

Further information: *AN1124 - Two locks on one door* < http://paxton.info/1780 >

Doors\[Door name]\Reader 2

The Reader 2 tab shows the settings corresponding to Reader 2 and Keypad 2 connected to that control unit.

The default name for Reader 2 is [Door name] (OUT). This can be changed.

Readers 1 and 2 are configured separately and can have completely different settings.

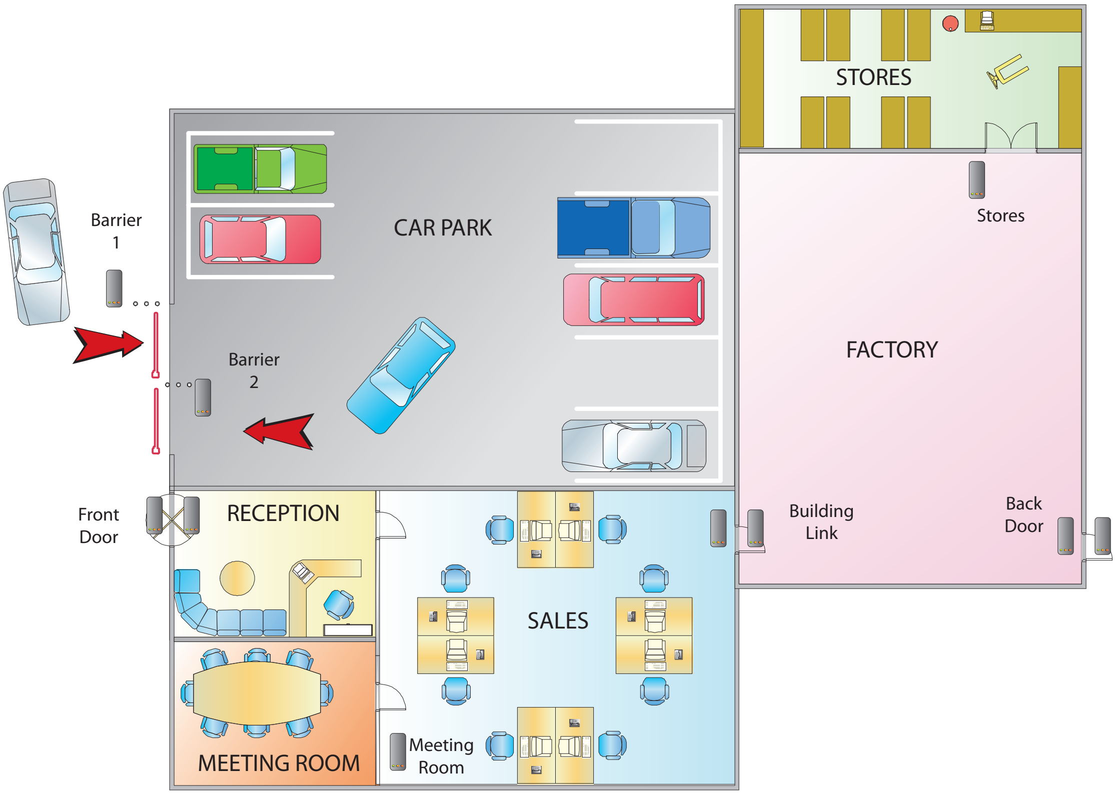
AN1023 - Configuring areas and area groups

A typical site plan

Areas and area groups make it easier to set up access levels on larger sites by grouping readers into a single entry. (e.g. Factory) It also allows you to use advanced features like anti-passback.

The diagram shows a typical site controlled by access control.

The following examples will guide you through the steps you would need to go through to configure this site for Area and Area Groups.

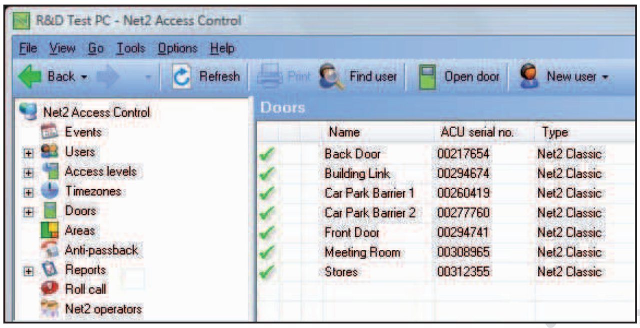


We will set up individual areas such as Car Park, area groups such as Manufacturing which contains areas for Factory and Stores and also a full Building Complex group that we would use to run a single fire alarm roll call for everyone on site.

Name the ACU's and Readers

The first step is to give each control unit a meaningful name.

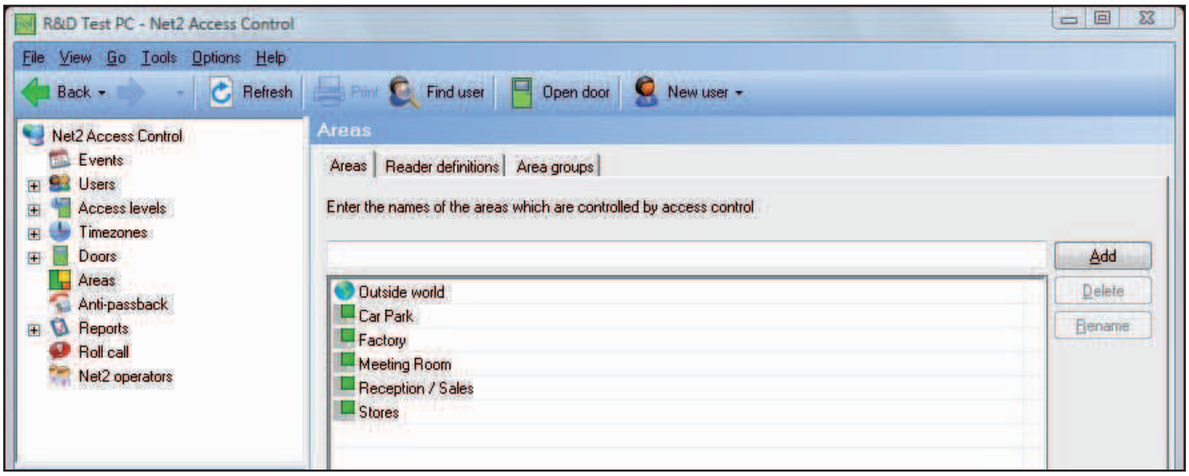
Now select each ACU from the tree view and make sure that the In and Out readers are also configured and named properly.



	Name	ACU serial no.	Type
✓	Back Door	00217654	Net2 Classic
✓	Building Link	00294674	Net2 Classic
✓	Car Park Barrier 1	00260419	Net2 Classic
✓	Car Park Barrier 2	00277760	Net2 Classic
✓	Front Door	00294741	Net2 Classic
✓	Meeting Room	00308965	Net2 Classic
✓	Stores	00312355	Net2 Classic

Areas

Click on the Areas icon to enter the names. You will notice that we have created Reception / Sales as a single area as no ACU controls the door between Reception and Sales. A default area called 'Outside World" has also been created. This can be re-named if required.



Enter the names of the areas which are controlled by access control

- Outside world
- Car Park
- Factory
- Meeting Room
- Reception / Sales
- Stores

Reader definitions

Once the Area names have been entered, click Apply and then move onto Reader definitions.

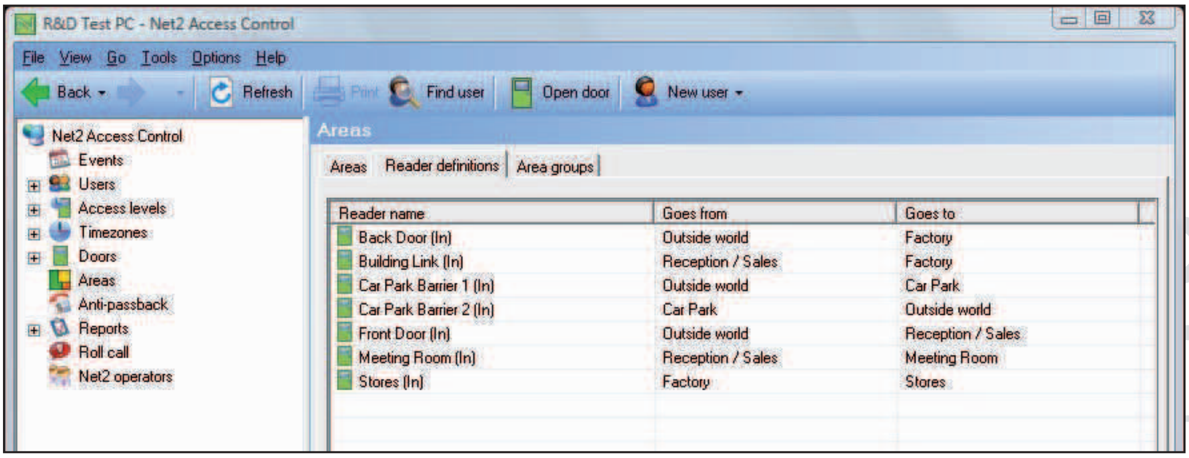
This is where we tell the system which ACU's control the access across Area boundaries. Note that we only define the IN reader, as the ACU is a one door controller and so the OUT reader is assumed as being on Reader 2 (if fitted).

A very simple site can have Exit buttons and even leave some ACU's undefined in the Areas system. These ACU's will be shown as a '-', however, this does impose severe limitations and some Net2 functions will not be reliable (e.g. roll call) as users can change Areas without being tracked.

The screenshot below shows how the reader definitions would be set up for our example site.

Back Door (In) goes from Outside World to Factory.

Make sure that you get the direction (From and To) correct. For example Barrier 1 (In) goes from Outside World to Car Park and Barrier 2 (In) goes from Car Park to Outside World. In this case we define both Reader 1 (In) as Reader 2 (Out) is not being used.



Reader name	Goes from	Goes to
Back Door (In)	Outside world	Factory
Building Link (In)	Reception / Sales	Factory
Car Park Barrier 1 (In)	Outside world	Car Park
Car Park Barrier 2 (In)	Car Park	Outside world
Front Door (In)	Outside world	Reception / Sales
Meeting Room (In)	Reception / Sales	Meeting Room
Stores (In)	Factory	Stores

Area Groups

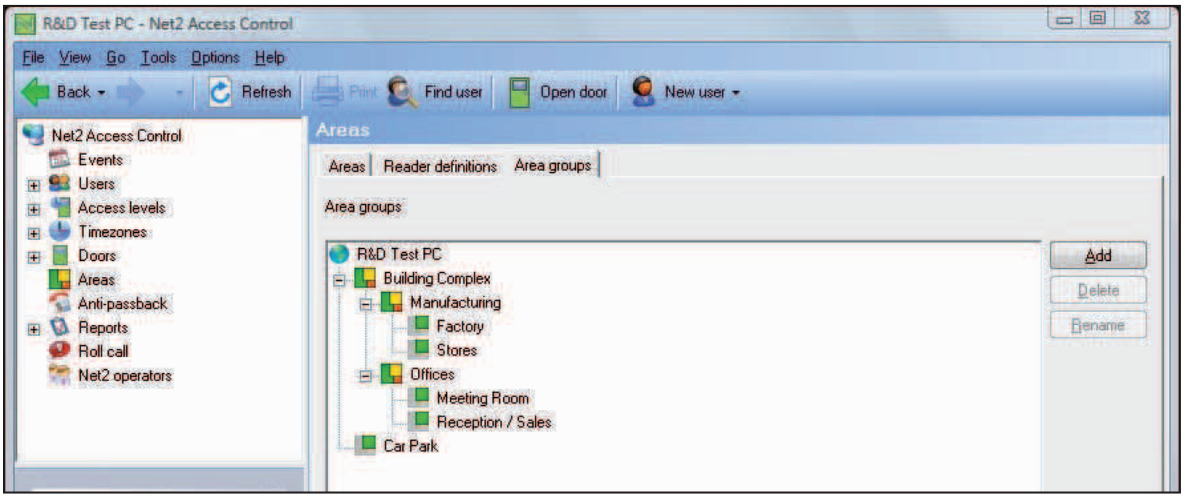
We can further put areas into groups to make roll call and anti-passback easier to configure and understand.

Click on the area groups tab, and you should see a list of your areas. You will note from the site plan, that Reception/Sales and the Meeting Room can be defined as an area group called Offices, and the areas of Factory and Stores are better grouped as Manufacturing.

Add an Area group by clicking the Add button, and entering the name.

You can now drag and drop the areas into their groups to show the correct structure. The screenshot shows that we have also created an area group called Building Complex which we can use for site roll call reports. Drag the Manufacturing and Office icons into this new area group.

The car park is not part of any larger area group.



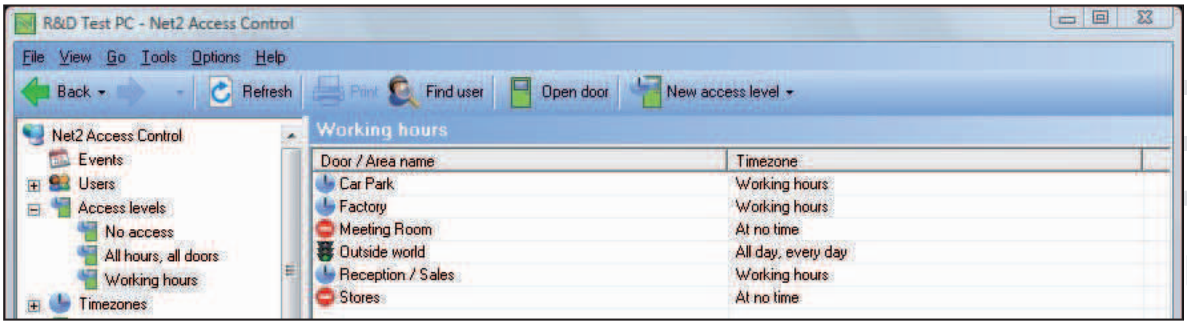
- R&D Test PC
  - Building Complex
    - Manufacturing
      - Factory
      - Stores
    - Offices
      - Meeting Room
      - Reception / Sales
  - Car Park

Using Access Levels with Areas

Access levels are defined using areas instead of individual doors. On large sites this makes the administration of the system easier as some areas, like Factory, have more than one access door but only require one entry in the table.

Note that we have set Outside World to 'All day, Every day' ensuring that wherever you are on the site you can always exit the complex.

Doors not configured in the Reader definition screen as having an area location will still appear in this list as individual ACU's and can be configured as normal. (See following restrictions)



Working hours

Door / Area name	Timezone
Car Park	Working hours
Factory	Working hours
Meeting Room	At no time
Outside world	All day, every day
Reception / Sales	Working hours
Stores	At no time

Areas and Area Group restrictions

Now that areas and area groups are set up additional features of Net2 can be used.

Anti-passback: This feature can be activated to ensure that a user card cannot be used twice in succession to gain access to the same Area.

Please note that the same door may not be used to control two individual anti-passback boundaries - i.e. You cannot have both Manufacturing and Building Complex (Manufacturing + Offices) anti-passback systems as the Back Door is required in both definitions.

See also:- *AN1063 - Configuring Anti-passback* < http://paxton.info/984 >

Roll call and muster: Muster reports are compiled by area or area group. These reports provide a list of users by Area when the report is run. This function can also be linked to an alarm input which will produce the report automatically. Readers can also be designated as Muster Points. When users appearing in the roll call report present their card at a Muster Point their status is moved from 'Missing' to 'Safe'. See also:- *AN1032 - Using roll call and muster reports* < http://paxton.info/060 >

EVERY reader must be within an Area definition to achieve an absolute site roll call. This may mean creating areas for a Stationary store, Cleaners cupboard, etc. so that every use of any reader still tracks a user within the Areas system. Exit buttons are permissible at these locations as we are checking the roll call for people reaching a Muster Point, but their 'Missing' location will not always be accurate as Net2 only records the last reader used.

AN1038 - Using Access Levels and Timezones

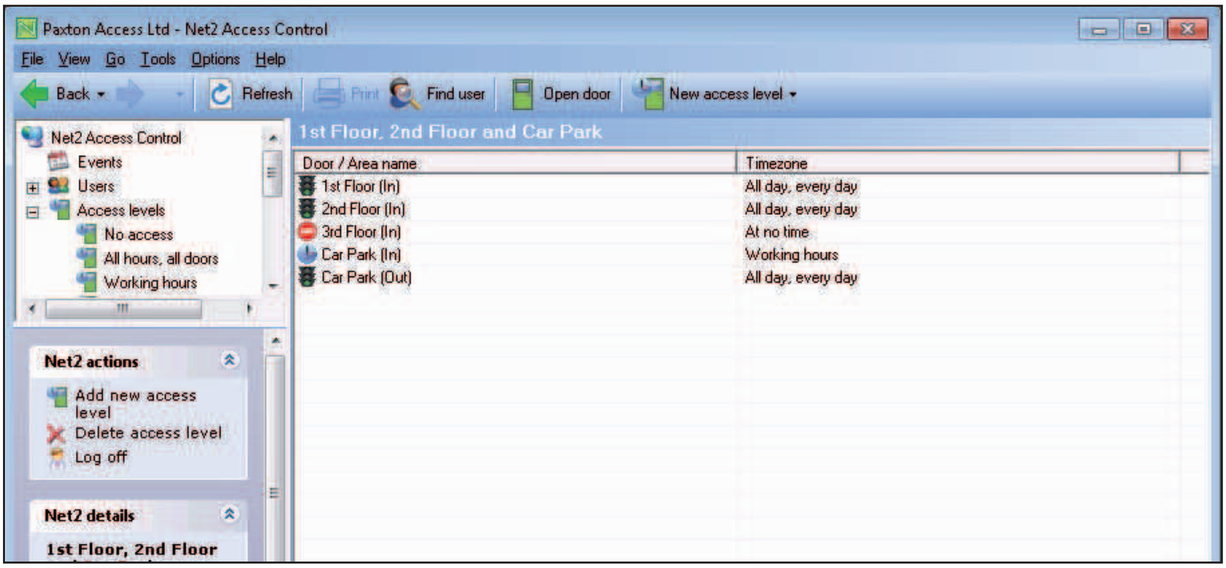
Overview

The Access Level is at the heart of Net2. Each one defines the relationship between the doors and the times when a user has access through them.

When you set up a user's record, you select the access level that is applicable to them. With a possible 250 access levels, all combinations can be catered for.

Timezones are used to define the time periods and are discussed later in this application note.

Access levels



1st Floor, 2nd Floor and Car Park

Door / Area name	Timezone
1st Floor (In)	All day, every day
2nd Floor (In)	All day, every day
3rd Floor (In)	At no time
Car Park (In)	Working hours
Car Park (Out)	All day, every day

In the above example we see an entry in the table for every reader that has been enabled. The Car Park ACU has both In and Out readers installed and so this 4 door system has a total of 5 entries. Alongside each entry is the timezone that defines when this reader is active and users who are assigned this access level will use these reader restrictions.

The three timezones used here (All day, every day / At no time / Working hours) are already set up as defaults in the software. You can modify the Working Hours timezone if required.

We have allowed full access to the 1st & 2nd floors, restricted the access to using the Car Park and denied access to the 3rd floor. By naming the access level with its description, it makes it easy to assign the correct one to a user as its name will display in the user record in a drop down menu for easy selection.

A basic system could be configured with these default timezones in different door combinations.

NOTE: It is usually good practice to set Out readers to All day/every day to avoid locking people on site after work.

Creating an access level

When deciding what access levels are required, you should determine how the system will be used by the customer in the future.

A site manager will easily relate to the physical layout of the building.

Example names: 1st Floor only, 1st Floor, 2nd Floor & Car Park. This makes it easy to upgrade a user from one to the other just be selecting the new level in their user record.

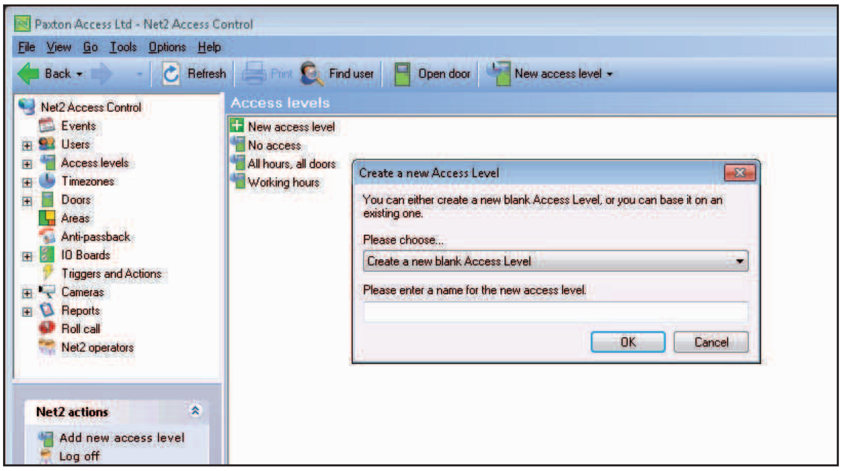
A personnel department may be better suited to defining access levels by user/job type.

Example names: Accounts Dept, IT staff, Cleaners, etc. These will often give access through the same doors but they will have different timezones.

You can use either style or a mix of both as required. Examples of both appear in this document.

To add a new access level, click on Access levels in the tree view and then New access level.

You now have the option to create a new blank access level with all timezones and all readers set to At No Time, or you can use one of the existing access levels as a template. This is helpful if there is a large numbers of doors on a system and this new level only differs slightly from an exisiting one.



Create a new Access Level

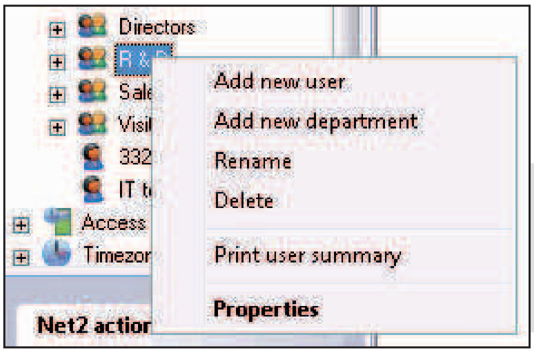
You can either create a new blank Access Level, or you can base it on an existing one.

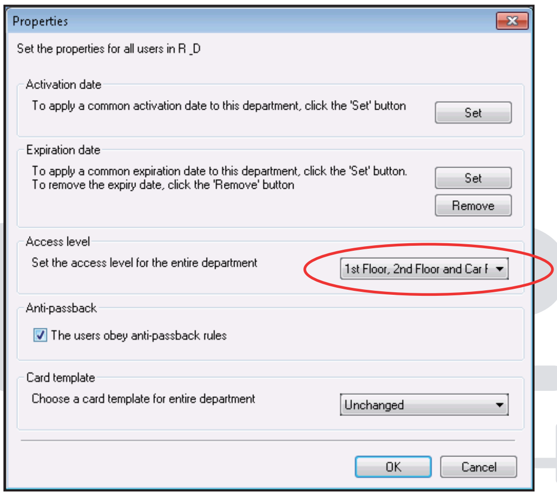
Please choose...

Create a new blank Access Level

Please enter a name for the new access level

You can set the access level for all people in a department by right clicking on the department in the tree view, and selecting Properties.




Properties

Set the properties for all users in R _D

Activation date

To apply a common activation date to this department, click the 'Set' button

Expiration date

To apply a common expiration date to this department, click the 'Set' button.
To remove the expiry date, click the 'Remove' button

Access level

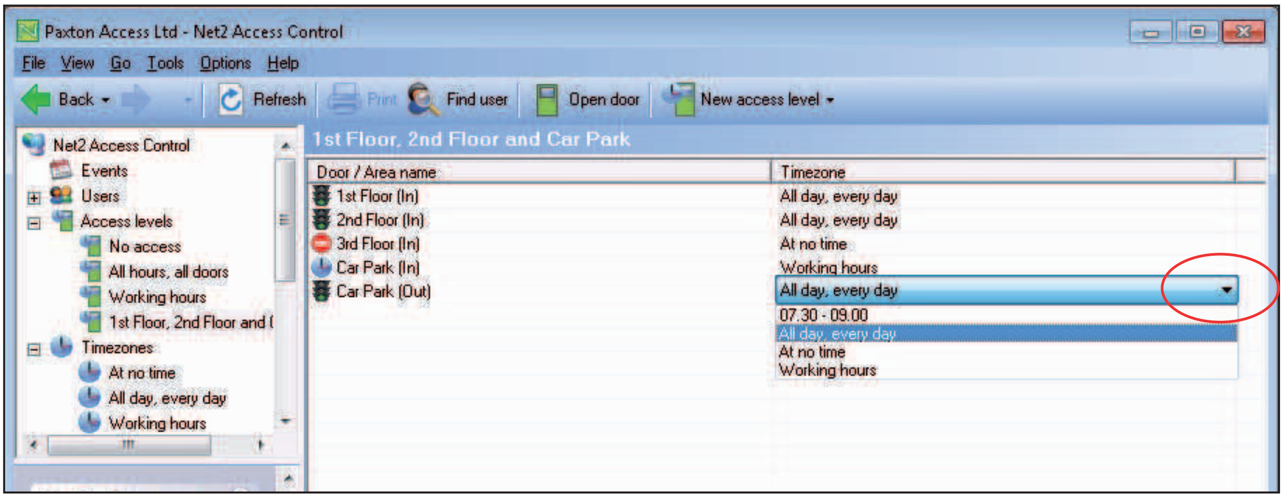
Set the access level for the entire department: 1st Floor, 2nd Floor and Car F

Anti-passback

☑ The users obey anti-passback rules

Card template

Choose a card template for entire department: Unchanged



1st Floor, 2nd Floor and Car Park

Door / Area name	Timezone
1st Floor (In)	All day, every day
2nd Floor (In)	All day, every day
3rd Floor (In)	At no time
Car Park (In)	Working hours
Car Park (Out)	All day, every day

Once the basic level has been created, you can then select the timezone by clicking directly on the timezone entry (right hand column) and activate the drop down menu of available timezones.

Timezones

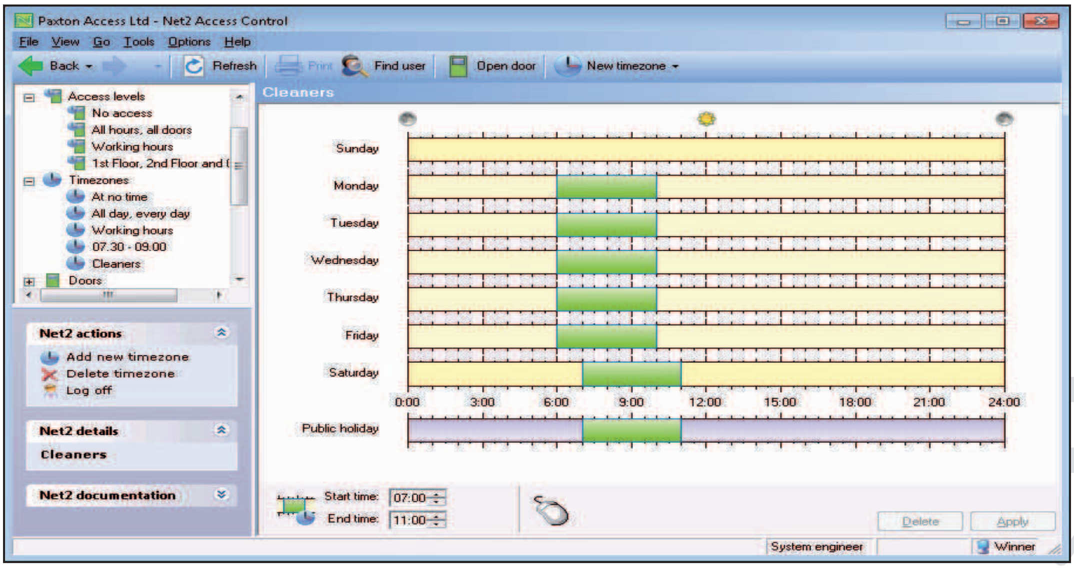
The Net2 system makes use of timezones in functions that depend on the time and day of the week. Once a timezone has been set up, it can be used for any number of features that need to be active during the defined time period. The maximum number of timezones is 64.

Their main use is in Access levels to define active time periods but they can also control system functions, like opening the main gates during working hours.

A timezone is made up of several timeslots. An example is shown below for a Cleaner.

Sunday	No Time
Monday - Friday	6am to 10am
Saturday	7am to 11am
Public Holidays	7am to 11am

Timezones can have several timeslots per day allowing for break times, evening classes, etc. The maximum number of timeslots per timezone is over 2000.



Start time: 07:00
End time: 11:00

New Timezones are created in the same way as Access levels. Click on Timezones in the tree view and New timezone.

- Adding timeslots

New timeslots can be added by putting the mouse pointer on the required day at the start time, click and hold the left mouse button while dragging the pointer to the end time.
Note: The values also display in the time window at the foot of the page.

- Deleting timezones

Timezones can be deleted by clicking the 'Delete' button.

- Deleting timeslots

Timeslots can be deleted by first selecting the timeslot and pressing the 'Delete' button.

- Dragging and dropping

Timeslots can be moved by dragging and dropping. Select the timezone by holding the left mouse button down and moving the pointer whilst the timeslot is selected. The start and end times of a timeslot can be adjusted to the nearest 15 minutes by dragging the end of the timeslot.

- Start time and End time windows

These appear in the bottom left hand corner of the main display window. When a timeslot is selected the start and end times are displayed. The timeslot can be adjusted to the nearest 1 minute using up and down arrows.

- Copying and pasting

Clicking on the right mouse button whilst a timeslot is selected will activate cutting, copying and pasting. An entire sequence of timeslots in one day can be copied using the copy day feature.

- Public holidays

As well as the 7 days of the week, there is an entry for public holidays. This allows specific timeslots to be set up for days that are nominated as public holidays. By default, this is left blank so that any days defined as public holidays will not allow access. (except All day, every day)

In the previous example, the Cleaners timezone has been set up to allow access to the premises between 7am and 11am on public holidays.

- Apply

Changes must be applied for them to be added to the database and become active immediately.

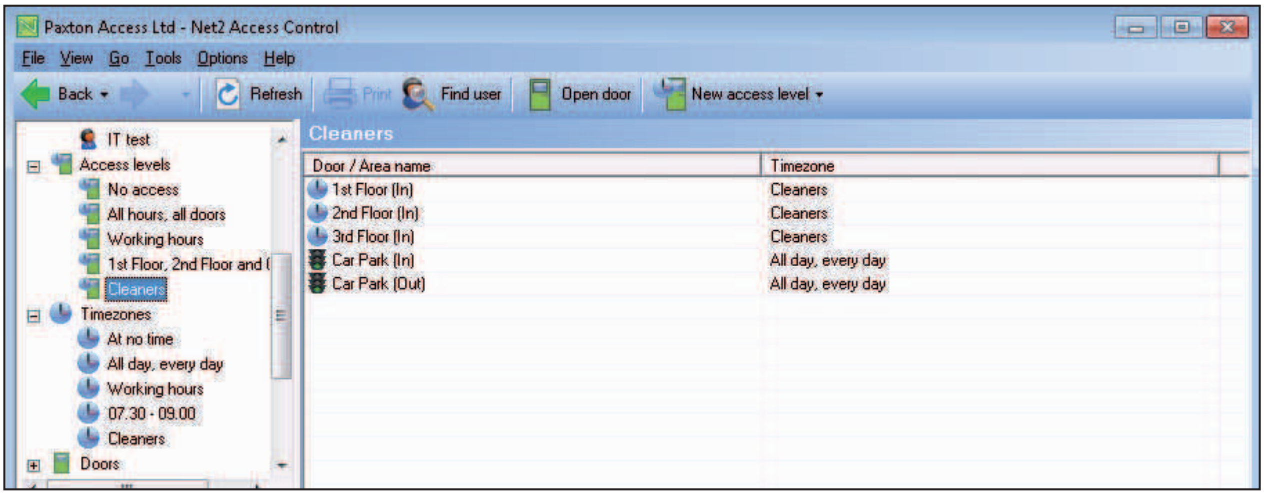
- Naming the Timezone

As with Access levels, choosing the name you give them will make future programming much easier. As the name of each timezone appears in the access level alongside its reader it may be better to use a description (e.g. Mon-Fri : 06:00 - 18:00) rather than the user (Cleaner).

If you use the time of day (07:30 - 21:00) then clearly you should not modify the timezone in future but create new ones (07:30 - 23:00) should the need arise. However if you have created a Cleaners timezone, only users with access levels linked to the Cleaners timezone will be changed.

It is always a balance that you will need to decide during installation, although names can be changed at any time in the future.

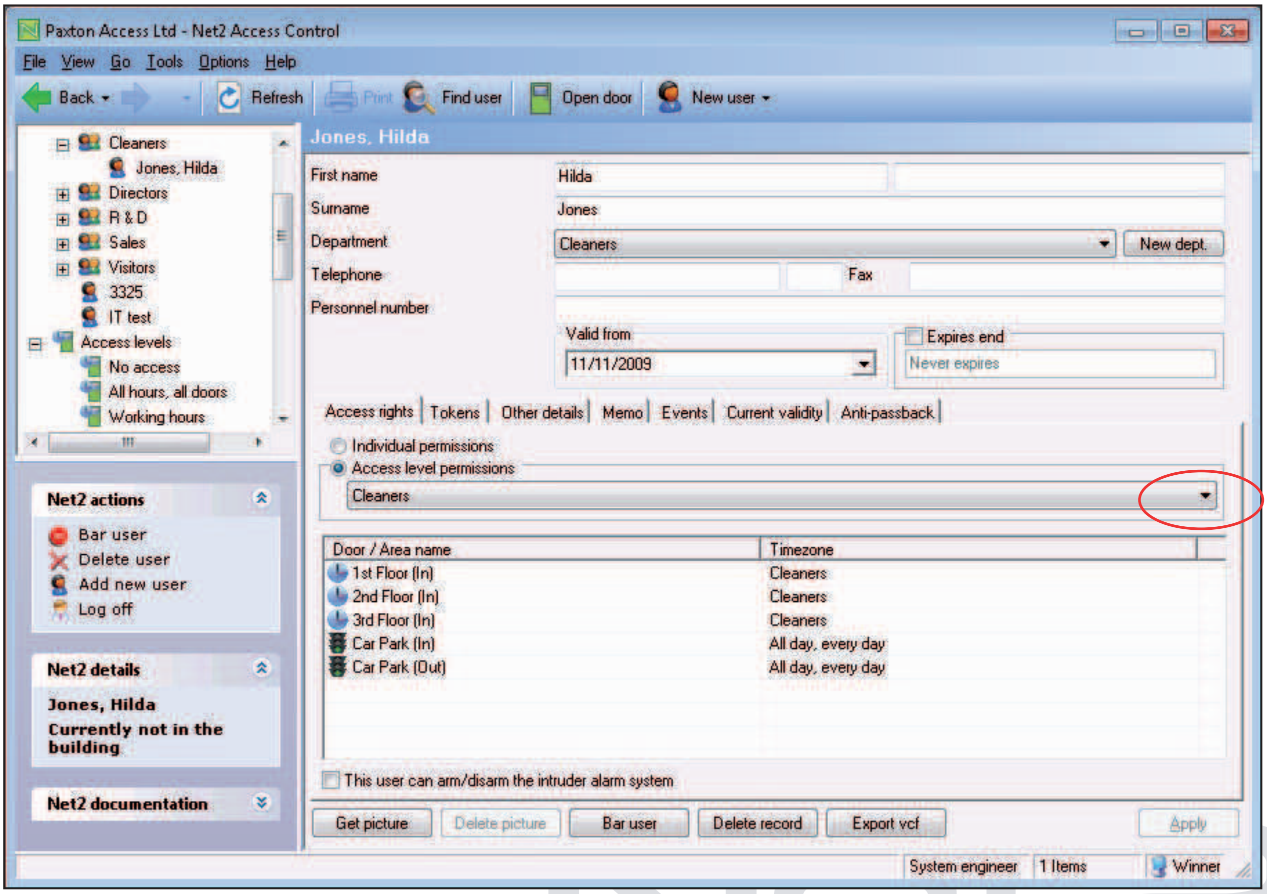
We can now use this Cleaners timezone to define a Cleaners Access level that limits their building access but gives them 24 hour access to the car park to deliver materials etc.



Cleaners

Door / Area name	Timezone
1st Floor (In)	Cleaners
2nd Floor (In)	Cleaners
3rd Floor (In)	Cleaners
Car Park (In)	All day, every day
Car Park (Out)	All day, every day

Below we see the user's record that also displays the access level. The level assigned is set up on this screen.



Jones, Hilda

Currently not in the building

Jones, Hilda

First name: Hilda

Surname: Jones

Department: Cleaners

Telephone:

Fax:

Personnel number:

Valid from: 11/11/2009

□ Expires end: Never expires

○ Individual permissions

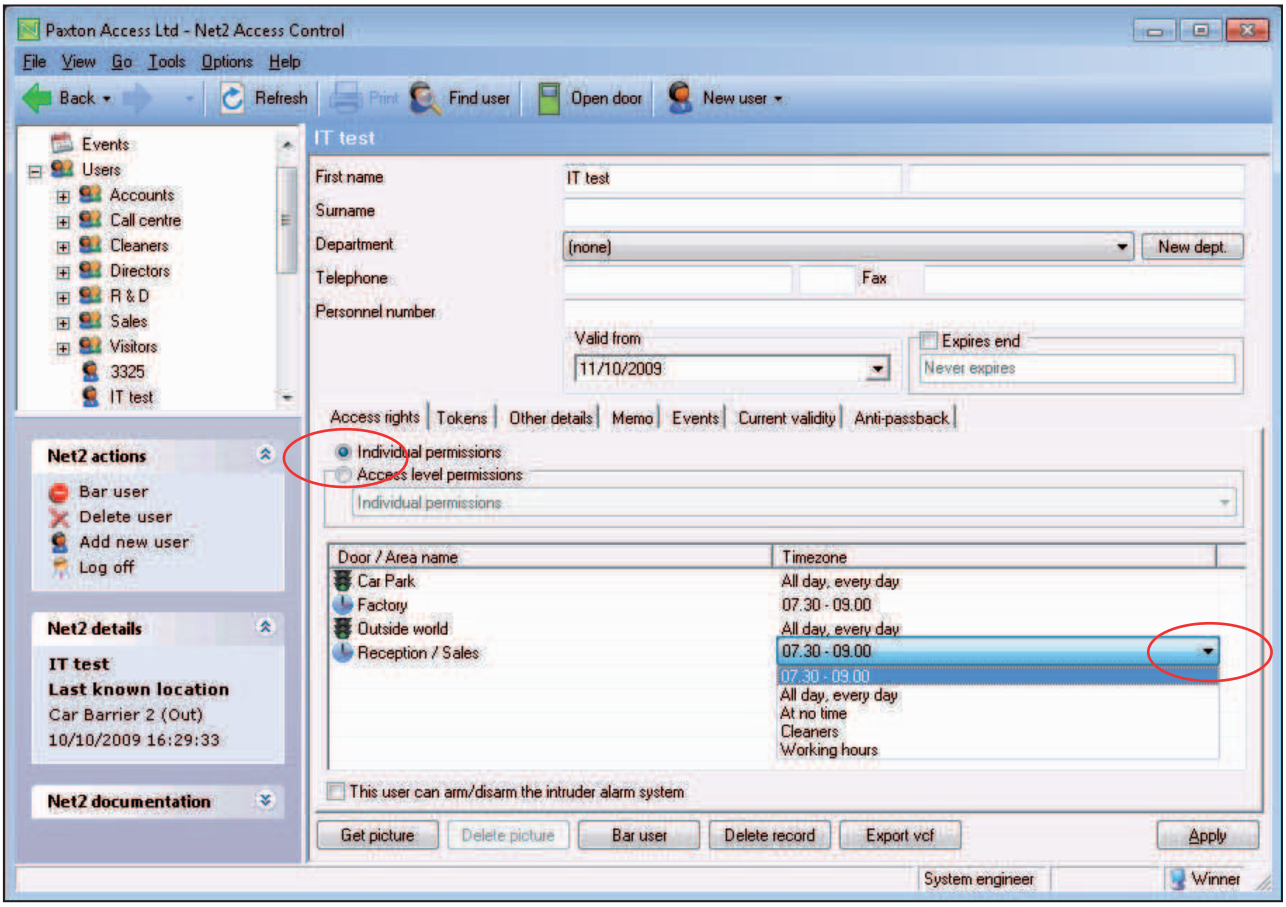
● Access level permissions

Cleaners

Door / Area name	Timezone
1st Floor (In)	Cleaners
2nd Floor (In)	Cleaners
3rd Floor (In)	Cleaners
Car Park (In)	All day, every day
Car Park (Out)	All day, every day

□ This user can arm/disarm the intruder alarm system

It is possible to create a User record with its own Access level by selecting Individual permissions. Assigning a Timezone to each reader is the same as for a normal Access levels.


Paxton Access Ltd - Net2 Access Control
File View Go Tools Options Help
Back Refresh Print Find user Open door New user
Events
Users
Accounts
Call centre
Cleaners
Directors
R & D
Sales
Visitors
3325
IT test
Net2 actions
Bar user
Delete user
Add new user
Log off
Net2 details
Net2 documentation
Access rights Tokens Other details Memo Events Current validity Anti-passback
New dept.
Get picture Delete picture Bar user Delete record Export vcf Apply
System engineer Winner

IT test

First name: IT test

Surname:

Department: (none)

Telephone: Fax:

Personnel number:

Valid from: 11/10/2009

□ Expires end: Never expires

● Individual permissions

○ Access level permissions

Individual permissions

Door / Area name	Timezone
Car Park	All day, every day
Factory	07.30 - 09.00
Outside world	All day, every day
Reception / Sales	07.30 - 09.00

07.30 - 09.00
All day, every day
At no time
Cleaners
Working hours

□ This user can arm/disarm the intruder alarm system

IT test
Last known location
Car Barrier 2 (Out)
10/10/2009 16:29:33

This option should only be used for Emergency/Test situations where a normal access level would take time to create and assign. Their use should be kept to a minimum.

Individual permission levels do NOT show in the Access level tree view and are therefore much more difficult to trace and control.

It is far better to create an Access level for one user (e.g. Directors Assistant) than to create a user record with 'hidden' permissions. These individual records will all need to be updated when doors/readers are added to the site and may get forgotten.

- Using Areas and Area groups

NOTE: In the above example, areas have been used in the software which can combine several doors. Only one entry per area is required, thus reducing the number of things to configure. See *AN1023 : Configuring areas and area groups* < http://paxton.info/978 >

AN1041 - Using Departments

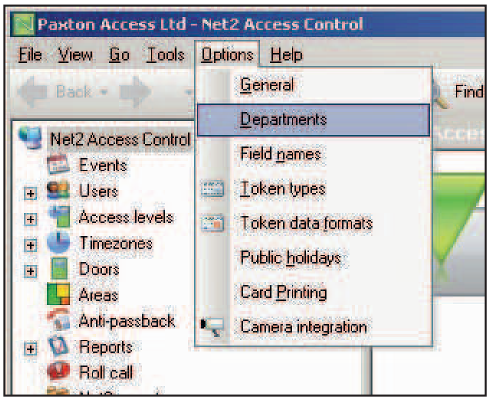
Using Departments

Departments allow users to be grouped together. This is particularly useful when there are a large number of users on the system. Having users grouped together by department enables quick reporting and viewing of users.

Departments can be created and edited by:

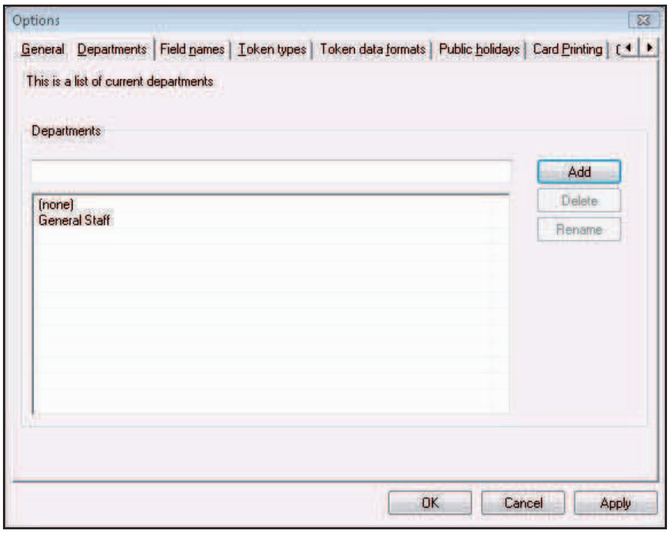
✓ Right clicking on Users in the tree view

✓ Through the Options menu



Go to the Departments tab and add any necessary departments.

Any number of departments can be created. The name of the new department is simply entered into the text box.



This is a list of current departments

Departments

(none)
General Staff

The new department is added to the list by pressing the Add button.

Departments can be deleted and renamed using the relevant buttons.

Departments will be displayed in the tree view window and the main display window.

It is possible to drag and drop users into a department.

Properties can be changed for a whole department by right clicking on the relevant group in the tree view and selecting Properties. This will allow you to set and change the following parameters for all group members:

- Activation date
- Expiry date
- Access Level
- Anti-passback
- Card printing template

AN1039 - Adding a new user

Adding a new user

- General information

'Users' refers to the people that use the access control system. Users are identified to the system by a card, token or PIN (or a combination of any of these). Once a user has been identified to the system, a decision can be made at each door whether they are permitted or denied access.

Every user that has been entered onto the system has a user record. This contains information regarding their access permissions, cards/tokens, PIN's and any other details required.

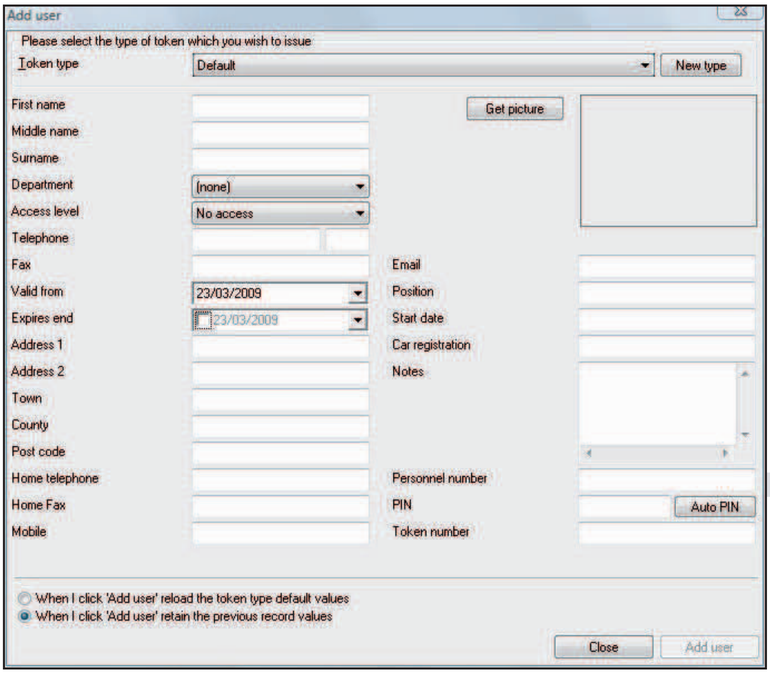
The users on the system are displayed in the main window. If departments have been configured then these will also be displayed.

To set up departments please refer to -: *AN1041 - Using Departments* < http://paxton.info/851 >

- Adding a new user

Adding users can be done in several ways:

- ✓ New User. Click the 'Users' icon on the main Toolbar, click 'Users' in the tree view or click the icon on the Welcome screen.
- ✓ Desktop reader. When a new token is shown to the reader, the Add User form is automatically displayed.
- ✓ Large groups of users can be added by importing user data. Refer to -: *AN1011 - Importing and exporting Net2 user data* < http://paxton.info/55 >



Add user

Please select the type of token which you wish to issue

Token type: Default

Department: (none)

Access level: No access

Valid from: 23/03/2009

Expires end: □ 23/03/2009

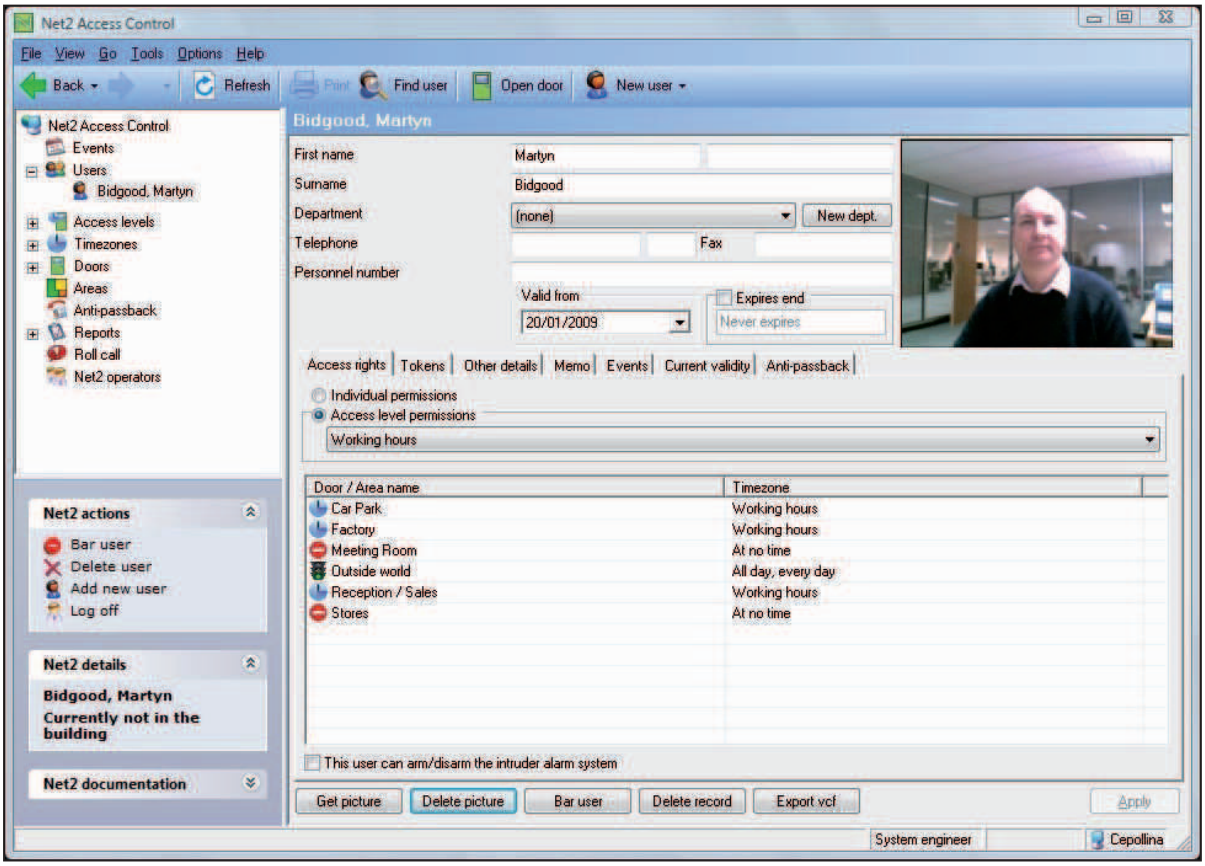
○ When I click 'Add user' reload the token type default values

● When I click 'Add user' retain the previous record values

You can enter as much information as you like through this form. The users name must always be entered. When completed, click 'Add user.' This will save the record and clear the fields for the next user's details to be entered. Clicking 'Close' will close the form and go to the last user record entered.

By setting up a token type, fields can be automatically completed for different groups. (e.g. Visitors) For further details on how to set up Token Types refer to -: *AN1042 - Using Token Types* < http://paxton.info/859 >

User records



Bidgood, Martyn

First name	Martyn
Surname	Bidgood
Department	(none)
Telephone	
Fax	
Personnel number	
Valid from	20/01/2009
□ Expires end	Never expires

○ Individual permissions
● Access level permissions
Working hours

Door / Area name	Timezone
Car Park	Working hours
Factory	Working hours
Meeting Room	At no time
Outside world	All day, every day
Reception / Sales	Working hours
Stores	At no time

□ This user can arm/disarm the intruder alarm system

Net2 details: Bidgood, Martyn Currently not in the building

- General information
Name, telephone number, department and personnel number can be recorded if required.

- Valid from and Expires end
Indicate the dates between which the user is valid. Visitors for example can be configured so that their card automatically expires after one day. Contractors or temporary staff can be configured to be valid between certain dates.

The 'Expires end' date is inactive as default. If required it can be marked as active and a date can be selected from the drop down calendar.

The user can be barred from all doors by pressing the 'Bar user' button.

A user's complete record can be deleted by pressing the 'Delete record' button. This will completely remove the user record from the database. **- WARNING. This action cannot be undone.**

- Pictures

* Get Picture.

A picture can be imported by pressing the 'Get picture' button. Bmp, jpg, gif, wmf and emf formats are supported. Pictures can be deleted by pressing the 'Delete picture' button.

* Capture Picture.

If a webcam has been installed on the PC a 'Capture Picture' button is displayed on the user records screen. This can be used to import a live user picture into the database. To set up the web cam refer to -: *AN1092 - Integrating a web cam for use with Net2 user records* < http://paxton.info/855 >

- Print card

Clicking on 'Print card' will print the card for the user being displayed. To set up card printing refer to -: *AN1034 - Net2 Card Printing* < http://paxton.info/56 >

- Access rights

The user can be assigned an access level from the drop down list. Refer to -: *AN1038 - Using Access Levels and Timezones* < http://paxton.info/847 >

Individual permissions. This option should only be used for Emergency/Test situations where a normal access level would take time to create and assign. Their use should be kept to a minimum. Individual permission levels do NOT show in the 'Access levels' tree view and are therefore much more difficult to trace and control.

- Alarm users

When Net2 has been set up with 'Intruder alarm integration' enabled, a tick box labelled "This user can arm/disarm the intruder alarm" appears in each user record. Tick this box to give the user the authority to control the alarm system.

- Users » [User name] » Tokens

The main display shows the tokens that are assigned to the user. Users can be assigned more than one token as required. Tokens can be added by either entering the card number manually OR by presenting or swiping the card at a desktop reader. Right clicking on the key icon allows this to be changed to the style of token issued.

Tokens can be deleted completely by pressing the 'Delete token' button.

- Lost token

If a token is marked as lost, it will be automatically invalid on all doors. If it is presented at any reader on the system, an alarm event will be generated. If a token that is marked as lost is then found, the token can be reinstated with the 'Found' button or can be deleted and the token issued to another user.

- Users » [User name] » Other details and Memo

Details can be entered for every user on the system. Default user detail fields are:

Address 1
Address 2
Town
County
Post code
Home telephone
Home fax
Mobile
email
Position
Start date
Car registration
Memo

The 16 user detail fields can be modified as required.
Note: Field names can be edited by double clicking on them (unless disabled in Options).

- Users » [User name] » Events

This tab displays the events for that user. This can be useful if trying to locate a user in a large building, simply go to the user record and see where they presented their card last. The events in this screen can be sorted by any of the columns by clicking the left mouse button over the column header.

- Users » [User name] » Current validity

This tab shows where the user is currently valid. The readers on which the user is currently valid will be highlighted; readers where the user is currently invalid will be greyed out.

- Users » Anti-passback

Reset allows the users anti-passback status to be reset and their next valid access sets their location in the system.

By default, users must obey anti-passback rules; this can be deselected. This means that security staff, for instance, can always gain access through doors, which might otherwise have been barred. For example, when in pursuit of an unauthorised intruder, they might end up tailgating users through doors, and it would not be appropriate for them to then be barred from going through other doors. It is possible to right click on a department, go to properties, and then select or deselect all users in that department to obey anti-passback rules.

AN1073 - Net2 operators - Adding / Assign privileges

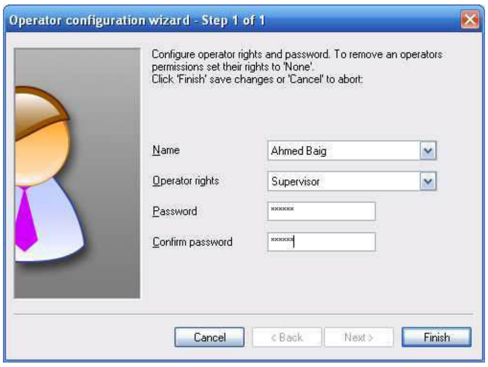
Overview

The term 'Net2 operator' relates to a person that has access to and uses the Net2 software. There is no limit to the number of Net2 operators allowed.

Net2 operators can be assigned different privileges allowing them various levels of access to the features of the system. Operator privileges are split up into 7 levels:

	System Engineer	Supervisor	Card Administrator	Standard (Read only)	Events only	Timesheet Administrator	Timesheet only
Events	✓	✓	✓	✓	✓	✓	✗
Users	✓	✓	✓	Read only	✗	✓	✗
Access levels	✓	✓	Read only	Read only	✗	Read existing and create new	✗
Timezones	✓	✓	Read only	Read only	✗	Read only	✗
Doors	✓	Cannot replace or delete ACU's or refresh ACU firmware. Otherwise full access	✗	✗	✗	✗	✗
Areas	✓	Read only	✗	✗	✗	✗	✗
Anti-passback	✓	Read only	✗	✗	✗	✗	✗
I/O Boards	✓	✓	✗	✗	✗	✗	✗
Triggers and Actions	✓	✓	✗	✗	✗	✗	✗
Cameras	✓	✓	Read only	Read only	✗	Read only	✗
Site Graphics	✓	✓	Read only	Read only	✗	Read only	✗
Reports	✓	✓	Read existing and create new	Read only	✗	Read existing and create new	✗
Roll call	✓	✓	Read existing and create new	Read existing and create new	✗	Read existing and create new	✗
Net2 Operators	✓	Can create new operators at the level of Supervisor and below	Read only	Read only	✗	Read existing and create new	✗
Timesheet	✓	✓	Read only	Read only	Read only	✓	View own info.
Server Config. Utility	✓	✗	✗	✗	✗	✗	✗

Important
Only System engineers and Supervisors can create operators.
Supervisors cannot create System engineer operators.



Configure operator rights and password. To remove an operators permissions set their rights to 'None'.
Click 'Finish' save changes or 'Cancel' to abort:

Name: Ahmed Baig
Operator rights: Supervisor
Password: ******
Confirm password: ******

The new operator wizard is launched by double clicking on the 'New operator' icon.

Before an operator can be added, they must first be a 'User' on the system.

Select the required privilege from the drop down menu. Get the new operator to type in their password and confirm it.

Operators are removed by changing their privilege to 'None'.

AN1049 - Holding a door unlocked with Net2 software

Net2 allows the user to create and select a timezone to hold the door unlocked automatically.

1. Select the door from the Doors menu
2. Select the Timezone that you require in the 'Unlock the door during' menu.

Under normal operation, this should be set to 'At no time' so that a valid user card must be presented each time to gain access.

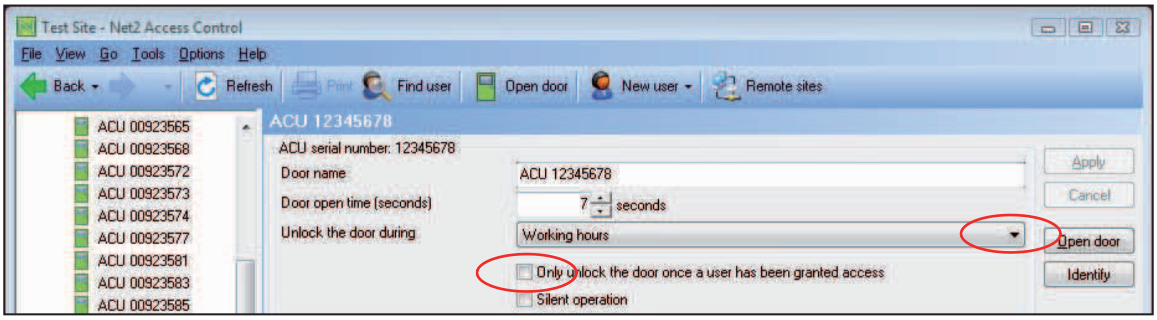
In the example below, we have selected the working hours timezone. The door will therefore be unlocked during the period defined in the 'Working hours' timezone.

You could create a specific timezone (e.g. door unlock 08.30 - 17.30) to only be used for this function.

This is useful where a receptionist is present to supervise visitors during office hours but overnight the main door will be locked and require a valid user card to gain access.

This feature can be further defined by checking the 'Only unlock the door once a user has been granted access' box. This ensures that the door will not unlock if staff have been delayed and the building is still unoccupied when the timezone becomes active.

To create a timezone, refer to:-
AN1038 - Using Access Levels and Timezones. < http://paxton.info/847 >



ACU 12345678

ACU serial number: 12345678

Door name: ACU 12345678

Door open time (seconds): 7 seconds

Unlock the door during: Working hours

□ Only unlock the door once a user has been granted access

□ Silent operation

AN1063 - Configuring anti-passback

Anti-passback principles

The main purpose of an anti-passback system is to prevent a card holder from passing their card back to a second person to gain entry into the same controlled area; for example a Car Park.

It also improves the accuracy of roll call, 'Last known position' reports and deters tailgating.
If a user follows a colleague OUT of an area without presenting their own card, their error is discovered when they try to return to the area. As this user is still shown as being IN the area, the use of their card for the IN direction is barred.

To use anti-passback, areas must be set up first. For further details on how to set up areas and area groups refer to:- *AN1023 - Configuring areas and area groups* < http://paxton.info/978 >

If the system is Reset, the next valid access for a user sets their current location in the system.

Door contacts should be fitted to doors included in the anti-passback system to confirm that the door has actually been opened. If not, the users 'last known position' will not be changed.

Logical Anti-passback

Logical anti-passback is used on sites where strict access control is important. It requires both IN and OUT readers at each area boundary. The system must see a user card leave an area before allowing access in the opposite direction.

This is particularly suited to deter users from tailgating each other. If they do not read out of an area, they will not be allowed back in, no matter which door they try.

An Administrator must Reset the users anti-passback permissions to allow access into the area.

Timed-Logical Anti-passback

This system is suited for a general office environment. As long as a user obeys the logical anti-passback rules, they may re-gain access to an area immediately. If, however, the user tailgates another user out of the area they will be allowed to re-enter after the specified time period from their previous valid access. This waiting period should inconvenience the user but will avoid them being trapped in an area.

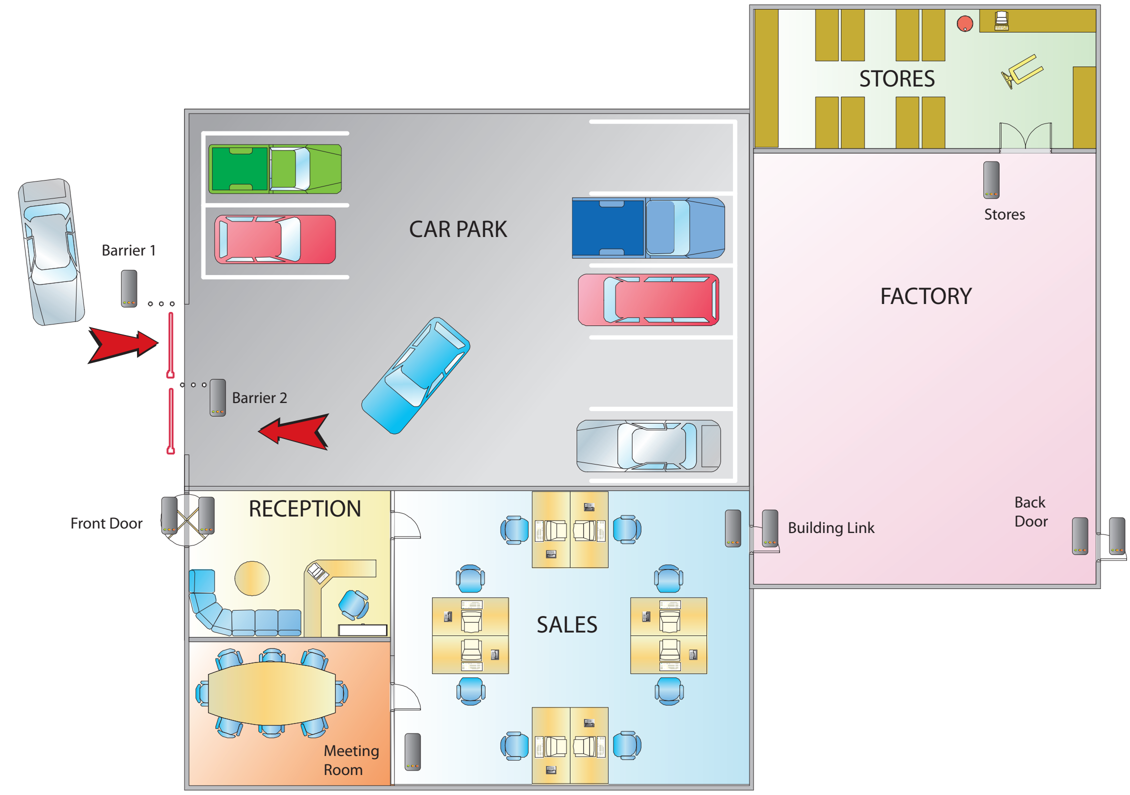
This removes the need to reset the user's permissions but the Access Denied event is still recorded.

Timed Anti-passback

Timed anti-passback prevents a user card from entering the same area twice during a set time duration. This is useful where there is an exit button or free access turnstile and no OUT reader.

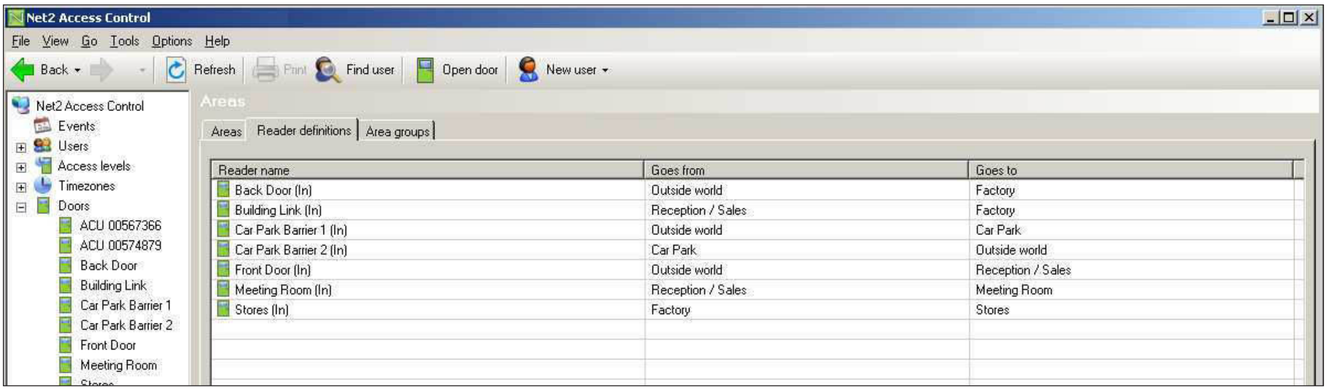
A swimming pool may only have access control into the area but no control on the exit. Setting up timed anti-passback with a duration of 15 minutes, would prevent a user being able to enter the area and hand their card immediately to a friend or colleague to also gain entry.

Configuring Anti-passback



Anti-passback requires areas and area groups to track user cards around the site. In the above diagram, we see that several areas have more than one entry/exit door. (e.g. Factory) Anti-passback must be aware of this to ensure that it controls all the doors surrounding each area.

See also:- *AN1023 - Configuring areas and area groups* < http://paxton.info/978 >

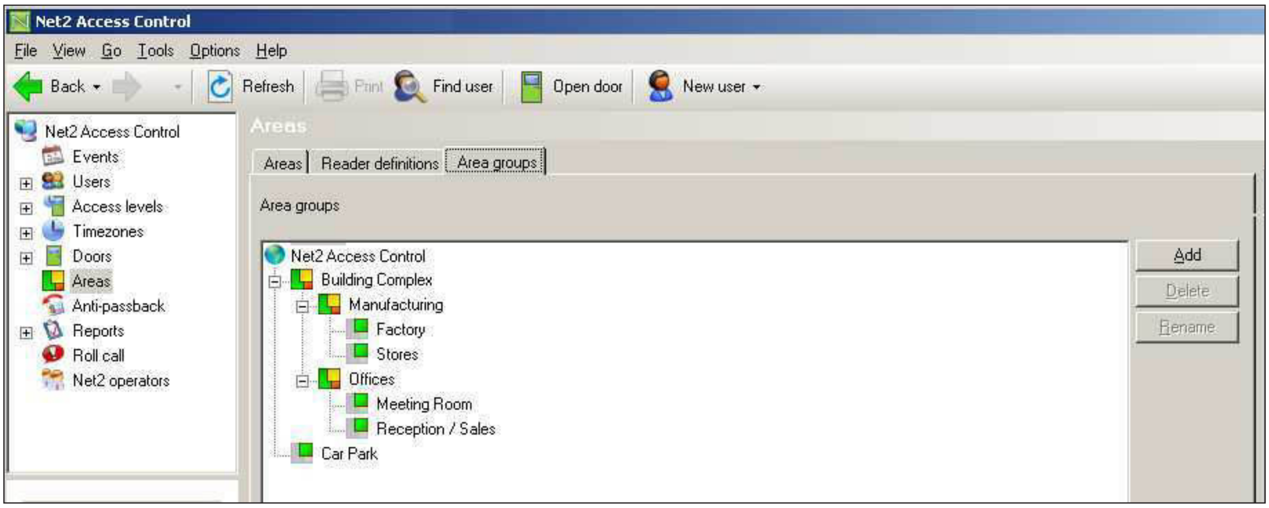


Reader name	Goes from	Goes to
Back Door (In)	Outside world	Factory
Building Link (In)	Reception / Sales	Factory
Car Park Barrier 1 (In)	Outside world	Car Park
Car Park Barrier 2 (In)	Car Park	Outside world
Front Door (In)	Outside world	Reception / Sales
Meeting Room (In)	Reception / Sales	Meeting Room
Stores (In)	Factory	Stores

We will look at some examples of anti-passback.

Car Park - We can set up anti-passback to ensure that once a card has been used at the IN barrier, it must then be read at the OUT barrier before being valid for entry again. This will deter users from handing their card to a friend after they have gained access to the car park.

In the above screenshot, we have a Car Park area with the two barrier ACU's controlling access to and from the Outside World. Ensure that the To and From direction for Reader 1 (In) is correct.



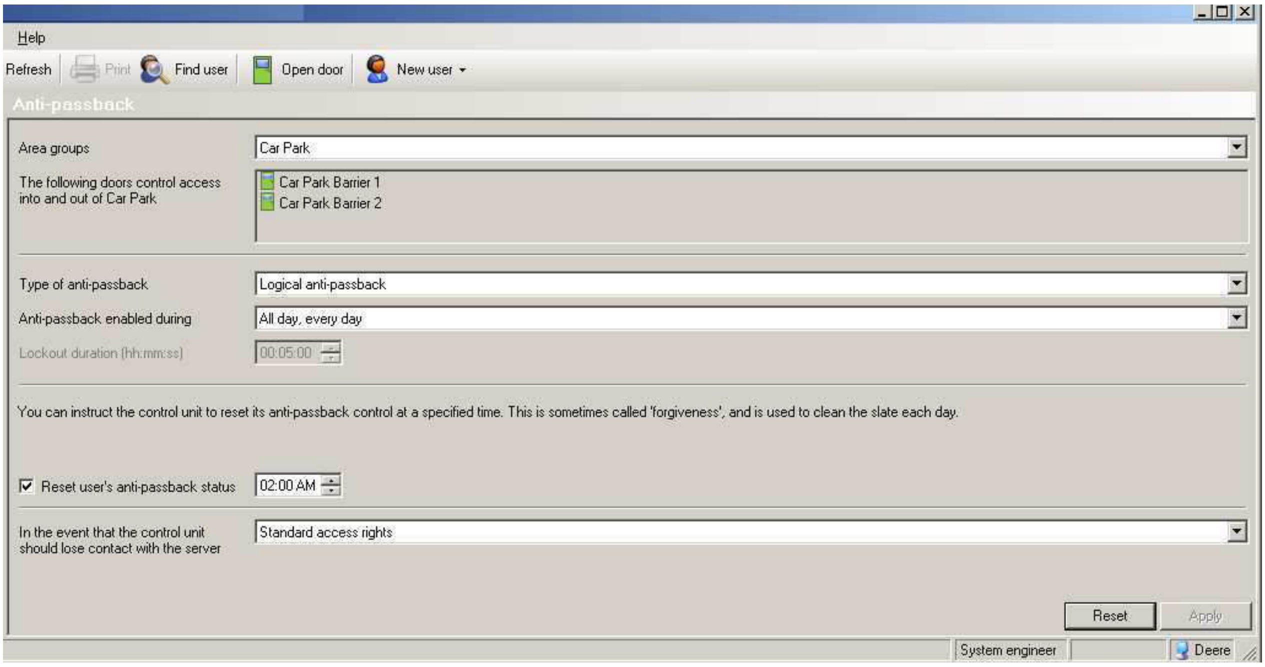
Area groups

- Net2 Access Control
  - Building Complex
    - Manufacturing
      - Factory
      - Stores
    - Offices
      - Meeting Room
      - Reception / Sales
  - Car Park

The area groups have been configured with the Car Park as a standalone area.

Click on the anti-passback icon. Select Car Park from the areas list and we can see the two readers that control this zone.

Selecting **Logical anti-passback** will ensure that this restriction is applied.



Area groups: Car Park

The following doors control access into and out of Car Park:
Car Park Barrier 1
Car Park Barrier 2

Type of anti-passback: Logical anti-passback

Anti-passback enabled during: All day, every day

Lockout duration (hh:mm:ss): 00:05:00

You can instruct the control unit to reset its anti-passback control at a specified time. This is sometimes called 'forgiveness', and is used to clean the slate each day.

☑ Reset user's anti-passback status: 02:00 AM

In the event that the control unit should lose contact with the server: Standard access rights

Anti-passback can be controlled by a time zone. This allows the system to be turned off when tight control is not required or desirable (e.g. out of hours).

The system can be configured to reset the anti-passback status at a specified time. This means that every user can start the next day with a clean slate.

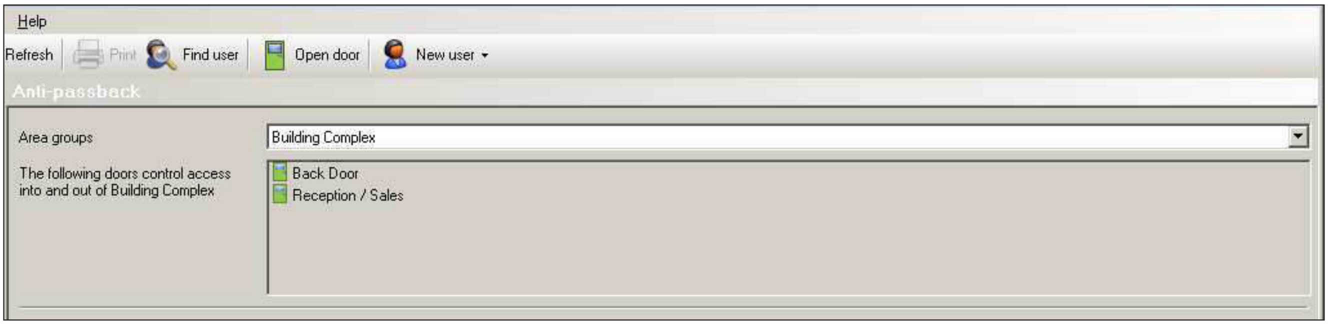
There is also a manual Reset button that gives all the users a fresh start.

For anti-passback to work, the Net2 server must constantly update all ACU's. In the event of the server losing contact with the control units you can choose to either have the ACU's deny users access or allow them standard access rights.

Tailgating

We can use anti-passback to deter users from tailgating. If they do not use their own card when entering or leaving the building, anti-passback rules will bar them from returning to that area. Anti-passback will therefore increase the accuracy of any roll call or 'Last known position' data.

By using Area Groups we can create a large group (e.g. Building Complex) that includes all the individual areas (or other area groups) that make up the whole building.



Area groups: Building Complex

The following doors control access into and out of Building Complex

- Back Door
- Reception / Sales

In the configuration that we have created, we show that access between the Outside World and the Building Complex is controlled by the Back Door and the Reception/Sales doors. Combining doors in the software is known as Global anti-passback, but it does have limitations.

See later restrictions on Global anti-passback.

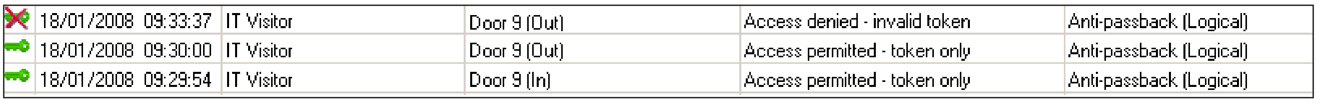
If you set up **Timed Logical anti-passback,** this will allow users to pass freely unless they fail to use their card every time. Anti-passback rules will then delay their return to an area until the time period has expired. This inconvenience should deter tailgating. The 'Access Denied' event will also be recorded.

Lockout duration is timed from the users previous 'access permitted' event into that area.

Event data

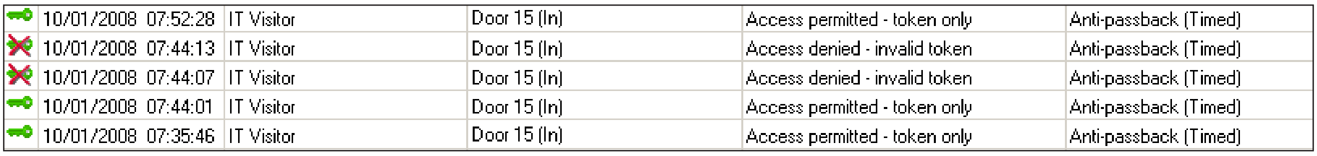
Every anti-passback event will have the type of anti-passback used (Logical, Timed or Timed+Logical) included in the event record. If this is information is missing, that door or user has not been included in the anti-passback system.

The first example (events are displayed from the bottom up) shows a user attempting to pass through a door twice in the same direction, possibly having tailgated a previous user, that has Logical control.



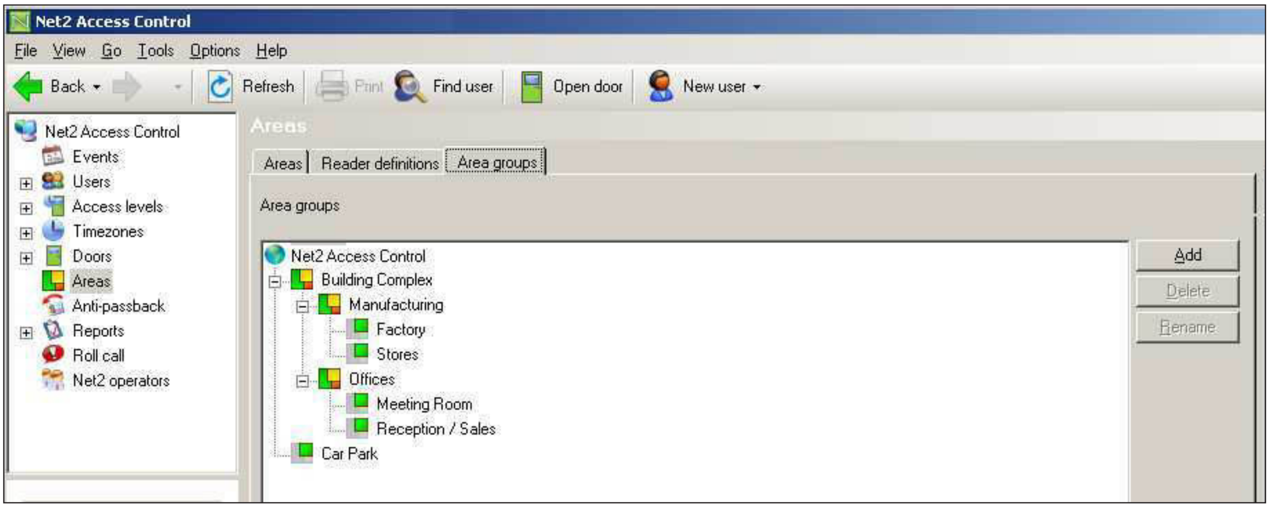
✗	18/01/2008 09:33:37	IT Visitor	Door 9 (Out)	Access denied - invalid token	Anti-passback (Logical)
🔑	18/01/2008 09:30:00	IT Visitor	Door 9 (Out)	Access permitted - token only	Anti-passback (Logical)
🔑	18/01/2008 09:29:54	IT Visitor	Door 9 (In)	Access permitted - token only	Anti-passback (Logical)

The second example shows a user card being denied access through a timed door with a 5 minute timeout. The repeated use of the card within the 5 minute period has been denied.



🔑	10/01/2008 07:52:28	IT Visitor	Door 15 (In)	Access permitted - token only	Anti-passback (Timed)
✗	10/01/2008 07:44:13	IT Visitor	Door 15 (In)	Access denied - invalid token	Anti-passback (Timed)
✗	10/01/2008 07:44:07	IT Visitor	Door 15 (In)	Access denied - invalid token	Anti-passback (Timed)
🔑	10/01/2008 07:44:01	IT Visitor	Door 15 (In)	Access permitted - token only	Anti-passback (Timed)
🔑	10/01/2008 07:35:46	IT Visitor	Door 15 (In)	Access permitted - token only	Anti-passback (Timed)

Global anti-passback restrictions



Area groups

- Net2 Access Control
  - Building Complex
    - Manufacturing
      - Factory
      - Stores
    - Offices
      - Meeting Room
      - Reception / Sales
  - Car Park

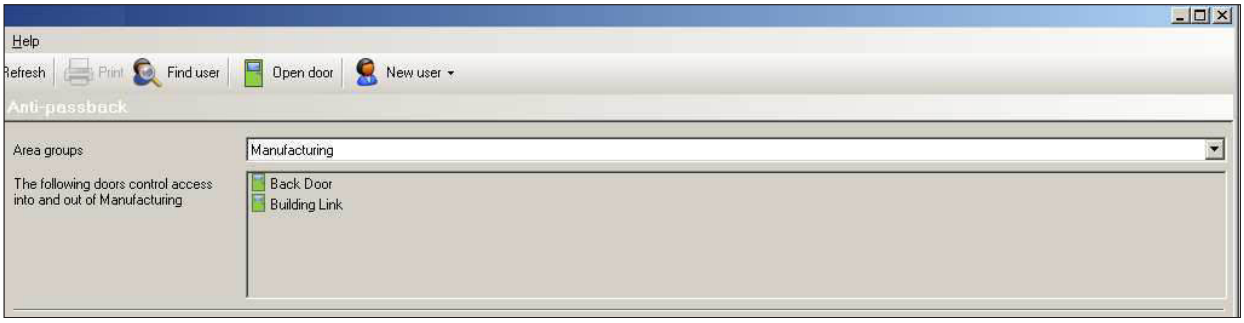
The same door must NOT be used to control two individual anti-passback boundaries.

The system will display all the possible door combinations that relate to the area or area group. This does not mean that it is valid to use them all at the same time.

In our example, we have set up anti-passback on the Building Complex. We cannot activate any of the other possible anti-passback zones that will use the same door as a boundary. One access event cannot update multiple anti-passback calculations.

- i.e. You cannot use anti-passback on both the Manufacturing and Building Complex (Manufacturing + Offices) areas as the Back Door is required in both definitions. Leaving the Manufacturing area does not always mean that you are leaving the Building and so the Back Door operation would be unreliable.

The Car Park and Building Complex can each use anti-passback as no door is used in both definitions.



Area groups: Manufacturing

The following doors control access into and out of Manufacturing

- Back Door
- Building Link

You may NOT create a group that contains individual Timed and Logical anti-passback areas.
You may NOT set up a Logical area with only a single reader and an EXIT button. (e.g. Stores)

In both cases, the user can return to an area without being tracked and will eventually produce a conflict within the anti-passback rules.

Try to determine the users exact requirements and only set up those zones that are necessary. Combining internal areas to produce sequential locking may be configurable (A to B then B to C) but may conflict with other anti-passback rules.

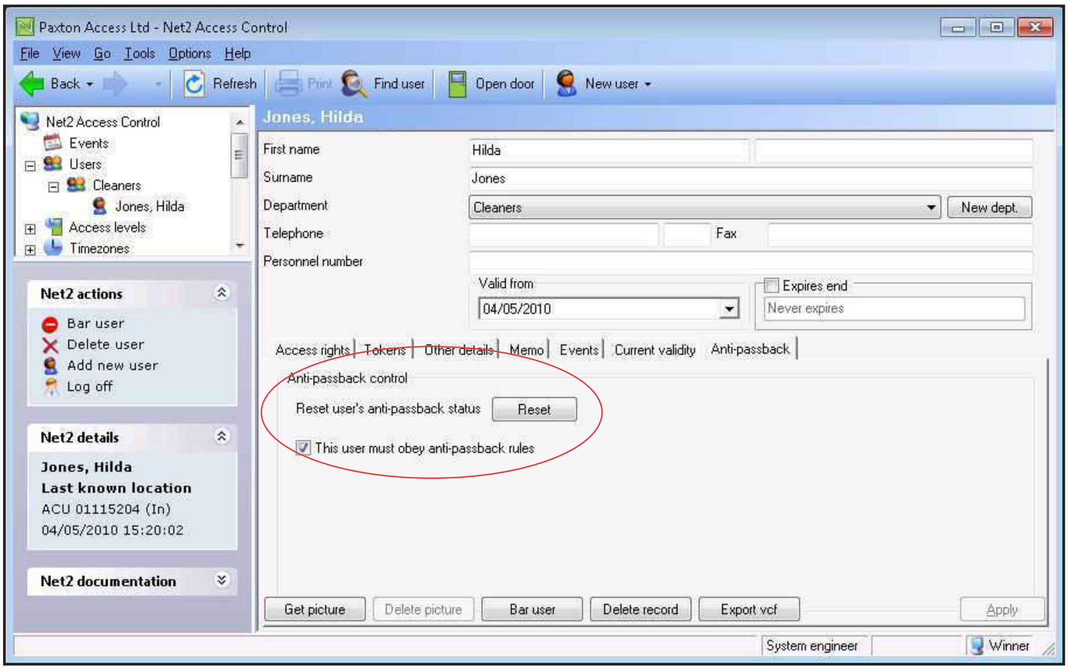
WARNING - These conflicts are difficult to predict and should not be offered as a reliable solution.

User permissions

By default, users must obey anti-passback rules. The Administrator has access to an anti-passback tab on the user record that allows the user to be deselected from the system. (e.g. Security Staff).

This allows them to tailgate an unauthorised intruder and not then become barred from other areas.

The users record also contains a Reset button. This clears their status should they become denied access by the anti-passback system. Their next valid access sets their location in the system.



Jones, Hilda

First name: Hilda

Surname: Jones

Department: Cleaners

Telephone:

Fax:

Personnel number:

Valid from: 04/05/2010

□ Expires end: Never expires

Anti-passback control

Reset user's anti-passback status [Reset]

☑ This user must obey anti-passback rules

Jones, Hilda
Last known location
ACU 01115204 (In)
04/05/2010 15:20:02

Important

Anti-passback requires the Net2 Server to be running. If you want to use anti-passback, it is recommended that the Net2 Server be installed on a dedicated machine.

If Net2 Fire Alarm integration is also configured, the Anti-passback system is reset when the Fire Alarm event is cleared and the doors relock. This allows users to be tracked again from scratch once they start using access control again.

The current specification for compatible PC hardware, network and operating systems is available on our website at the following link:- http://paxton.info/720