ISONAS™
SECURITY SYSTEMS

Crystal Matrix Software

Quick Start

Configuration Guide

Date: January 30, 2012

ISONAS Security Systems, 4720 Walnut Street, Suite 200, Boulder, Colorado 80301 800/581-0083 www.isonas.com

Table of Contents

Intended Use

The intention of quick start guide is to provide the basic configuration steps necessary for implementing a working Access Control System.

Introduction

The ISONAS Access Control system lets you define Who is allowed access. When are they allowed access, and to Where are they allowed access.

Who is defined by the Groups, People, and Badges features

When is defined by the Shifts and Holidays feature

Where is defined by the Controller Supervisor, Door and Door Group features

Permissions are used to tie the Who/When/Where together to create rules that the ISONAS Access System enforces as people enter and leave the facility.

This document assumes that the ISONAS reader/controllers are installed properly and are functional. This includes verifying network connectivity to the reader/controllers from the PC/workstation where the ISONAS Crystal Access software is running.

Two items to verify regarding the installation of the reader/controllers:

1. The reader/controller's Tamper Detector is pressed against a reflective surface.
2. The "Door Sense" wire (Blue) from the reader/controller is grounded to the "black" wire either thru a Door Sense switch, or by directly connecting it to the "black" wire.

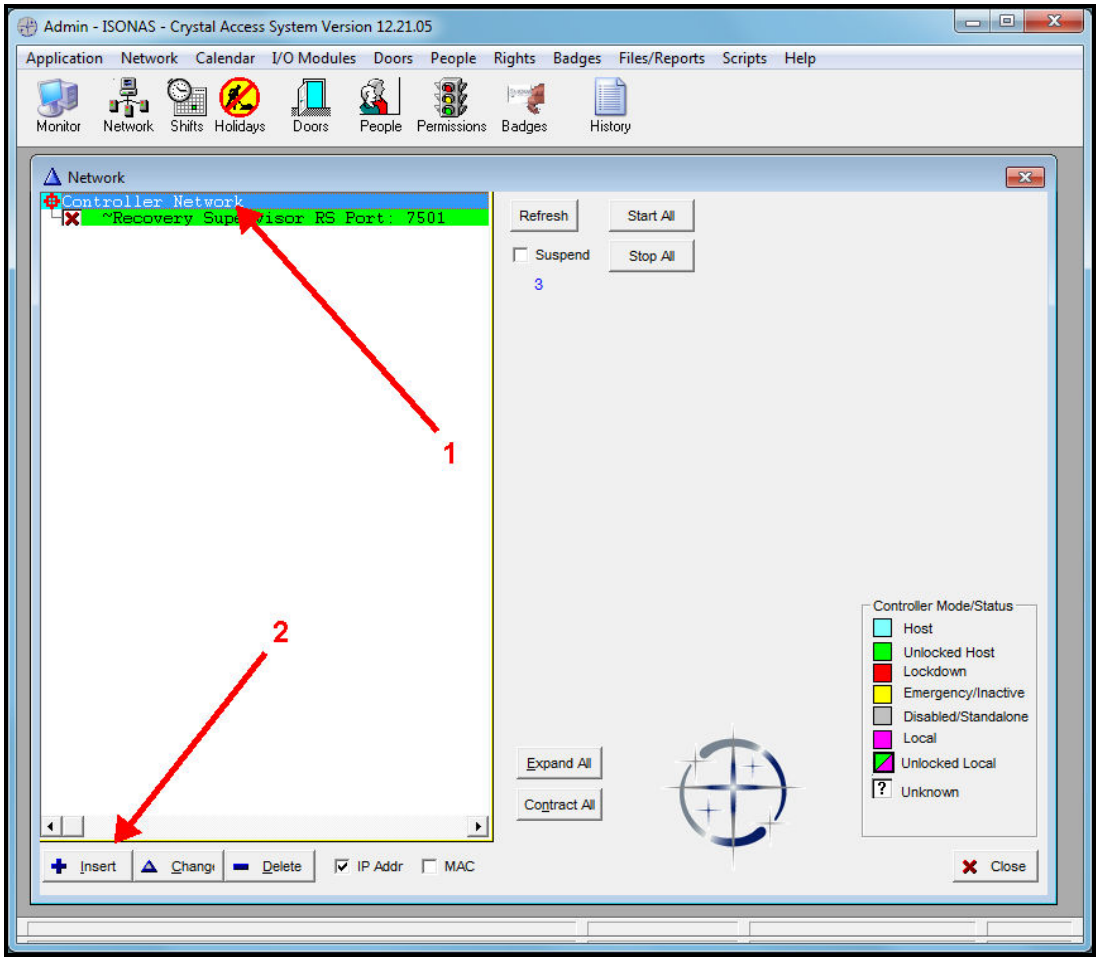
Basic Steps

There are six basic steps to configuring a working reader/controller at a door and allowing access to that door by a card/badge holder. Those steps are as follows:

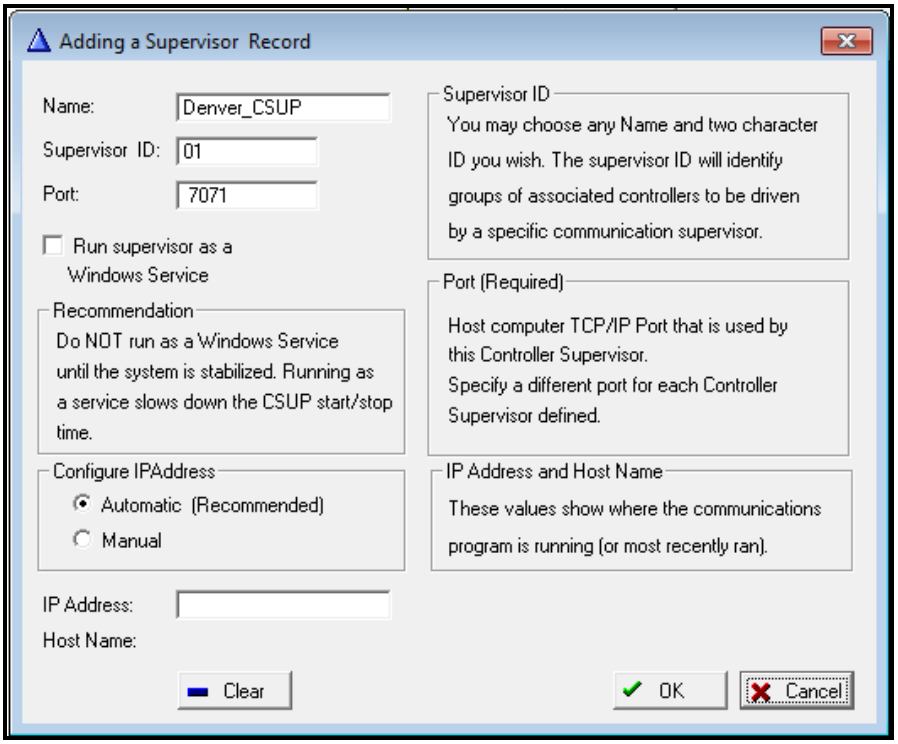
- Define a Controller Supervisor (CSUP)
- Define a Door
- Define a Group (User/Cardholder group)
- Define a Card/Badge Holder (People/Badges) with a badge
- Define a Shift (Valid Time Range)
- Assign a Permission to a Door (Shift and Group combination)

Define a Controller Supervisor (CSUP)

The first step is to define a controller supervisor (CSUP). A CSUP is a software program that will manage a set of reader/controllers (doors). You can insert a CSUP into the Crystal Access system by clicking on the "Controller Network" display line within the "Network View" display window (Arrow #1) and then pressing the "Insert" button in the lower left of the display window (Arrow #2).



Once the “Insert” button is pressed, the following display window will appear:



Enter a unique name of the CSUP that will manage your doors. This name will be used to reference the Controller Supervisor within the application.

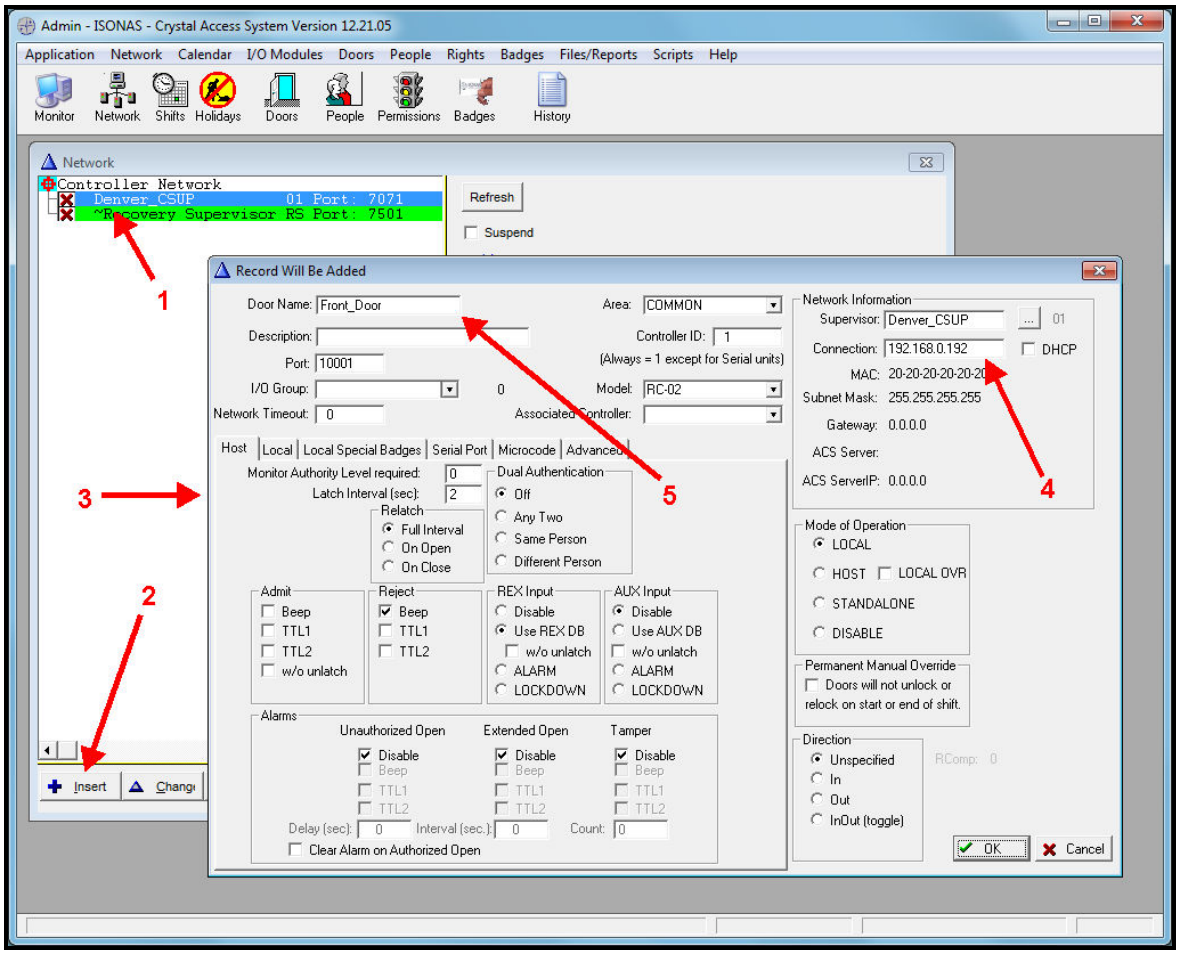
The “Supervisor ID” is a 2 character abbreviation that uniquely identifies the CSUP program within your application.

The port number is like a mailbox within your PC/workstation that the CSUP will use to receive and send messages to the Administrator program. It must be unique and not used by any other application within the PC/workstation that the ISONAS Crystal application is running on. Typically, you can select a port number in the range of 7071 – 7098. If you define more than one CSUP supervisor, be sure to select a different port number for each.

For now, make sure the “Run supervisor as a Window Service” is **NOT** checked. When the entry fields are defined, click the “OK” button to add and close the “insert” window.

Define a Door

The next step is to add a door to the CSUP. This is done by selecting the CSUP (1) that was just added and then selecting the "Insert" button (2).



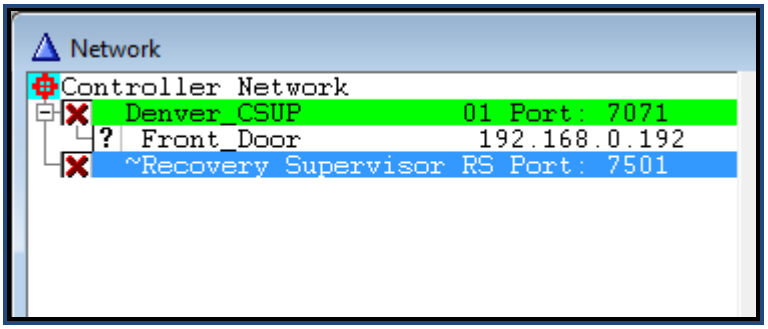
The "Door Detail" window (3) appears

The door's TCP/IP address (4) needs to be specified and is either the address set at the factory, found on the label of the reader/controller, prefixed by "Addr:" or the address you specified, if you have re-addressed the reader/controller to a new TCP/IP address. (For re-addressing reader/controllers, refer to the "Plug and Play" application section of the Software Reference Guide.). The example shows the IP Address as being 192.168.0.192.

Enter a unique name for the door (5). Optionally, enter a description of the door

The rest of the fields can be left with their default values. When the entry fields are defined, click the "OK" button to add and close the "door detail" window.

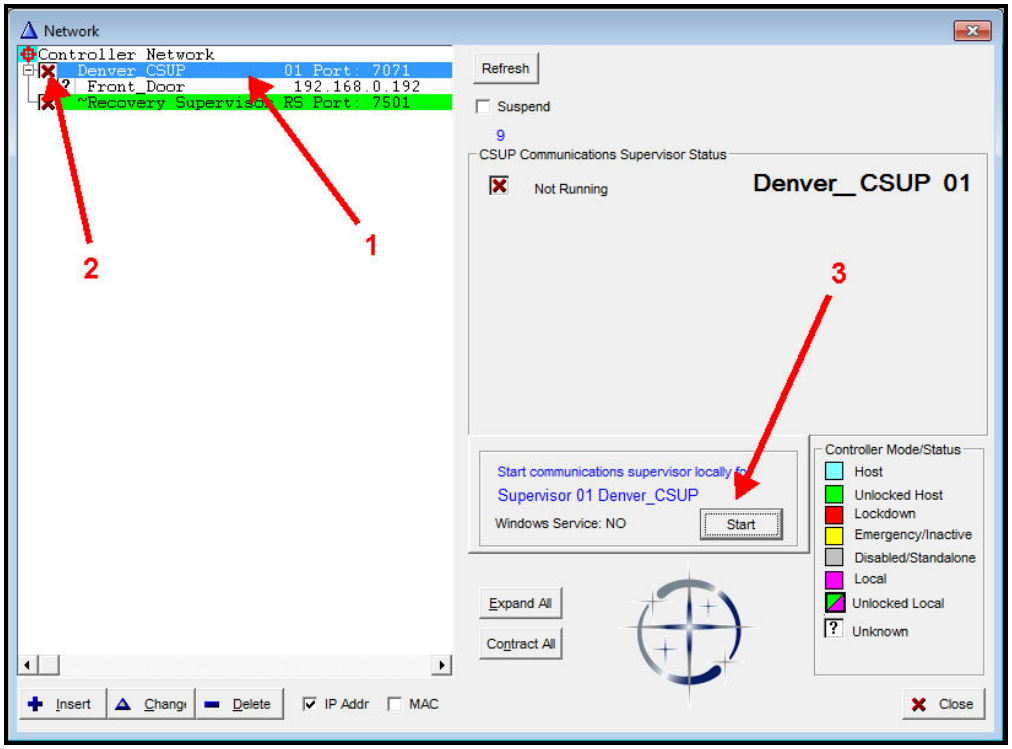
In the Network View, use the “Expand All” button to display all items defined in the network The new door will appear in the list.



In our case the CSUP, “Denver_CSUP”, is managing the door “Front Door”.

Starting the CSUP program

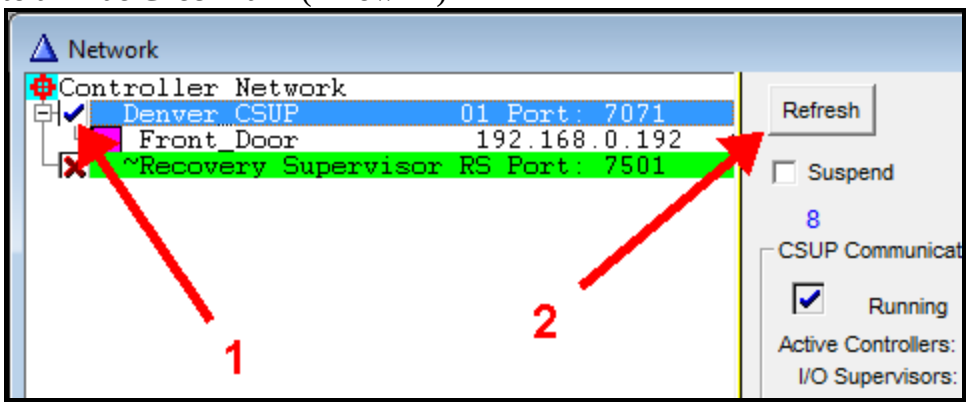
To start the communications between the Access System and the door, you click on the CSUP listed in the “Network” window (Arrow #1).



Note the CSUP’s status is shown with a red “X” (Arrow #2). When the CSUP is selected, the window will display a “Start” button for that CSUP (Arrow #3). Clicking this button will start communication to each of the doors listed for that CSUP.

ISONAS Security Systems, 4720 Walnut Street, Suite 200, Boulder, Colorado 80301 800/581-0083 www.isonas.com

There will be a delay (about 15 seconds) and the checkbox next to the CSUP should change from a “Red X” to a “Blue Checkmark”(Arrow #1)



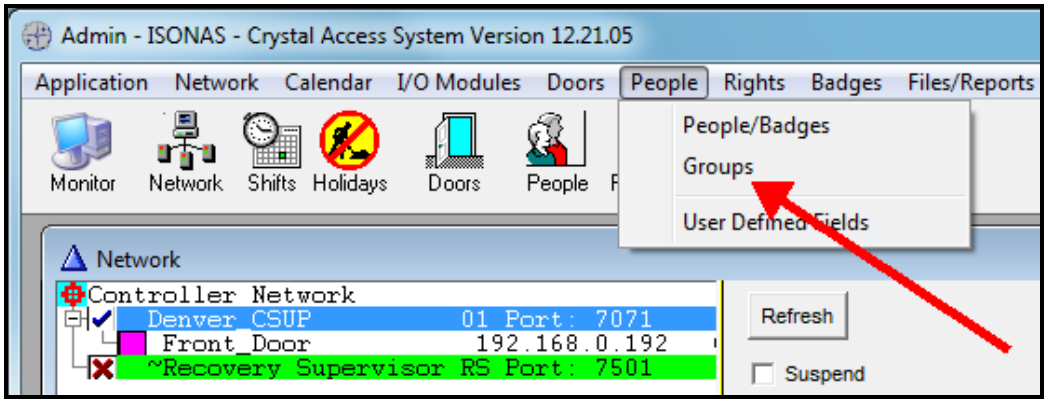
If the “Red X” does not change, wait 30 seconds and click on the “Refresh” button (Arrow #2).

If that does not clear the “Red X”, then there is a problem with the configuration or network that will need to be investigated. See the ISONAS Installation and Wiring Procedure manual for more information.

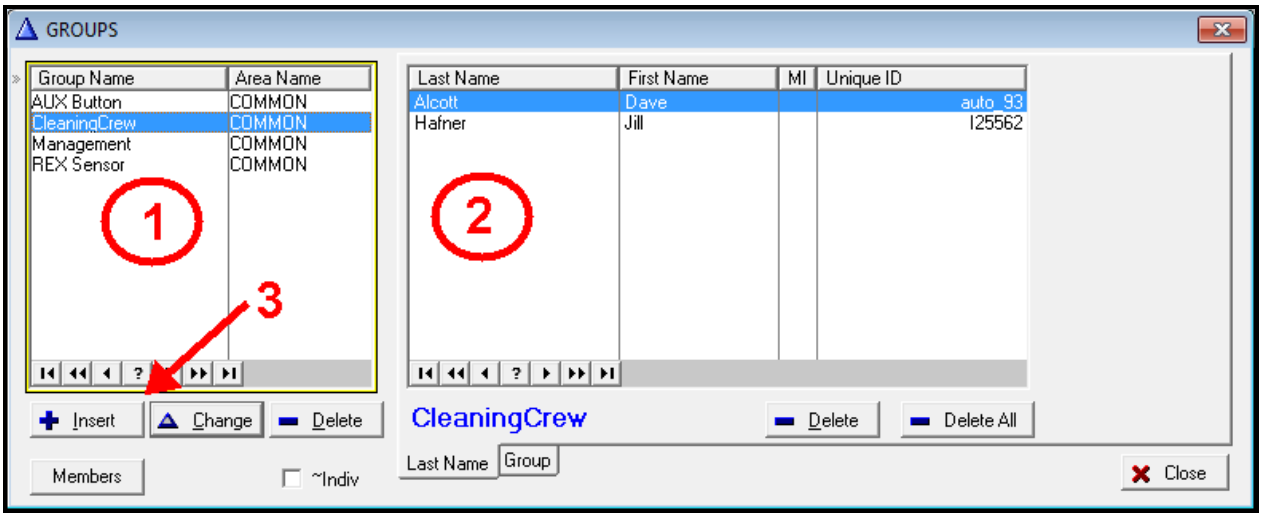
ISONAS Security Systems, 4720 Walnut Street, Suite 200, Boulder, Colorado 80301 800/581-0083 www.isonas.com

Defining Groups of Users

Users are assigned to a Group, and then Groups are given permission to access a door or set of doors. Users can be assigned to multiple Groups. Groups can be defined after the users are defined in the system, but logically, within a new system, it makes sense to define the Groups first. To display the current list of user Groups, select the "People" menu option and the "Groups" submenu option.



This will display the following display window:



This display shows any existing user groups.
The Group List (Box #1) shows the currently defined groups
The Member List (Box #2) displays the members of the currently selected group.

ISONAS Security Systems, 4720 Walnut Street, Suite 200, Boulder, Colorado 80301 800/581-0083 www.isonas.com

Adding a new user group is done by clicking the left “Insert” button to display the user group definition window (Arrow #3).

Enter a unique user group name (ex. “Staff”). Verify the Area Name is “Common”.
Click the “OK” button. This will save the user group name and display the new name in the “Groups” name list.

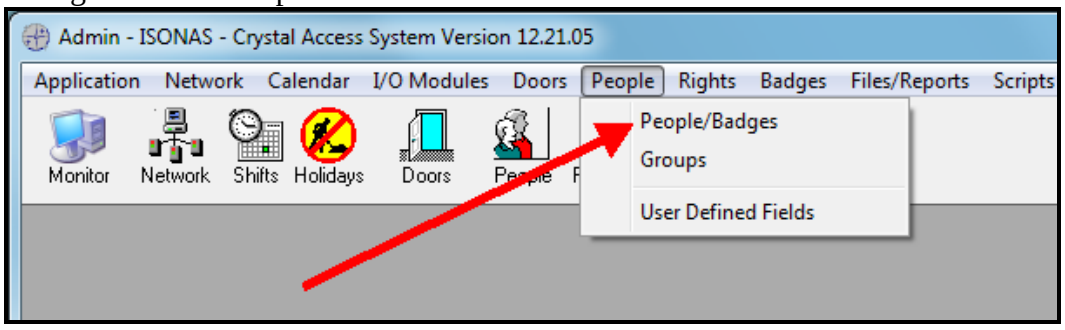
Repeat these steps to add the Groups you wish to use. Some Groups that are commonly used include:

- Management
- Visitors
- CleaningCrew
- Maintenance
- Off Hours

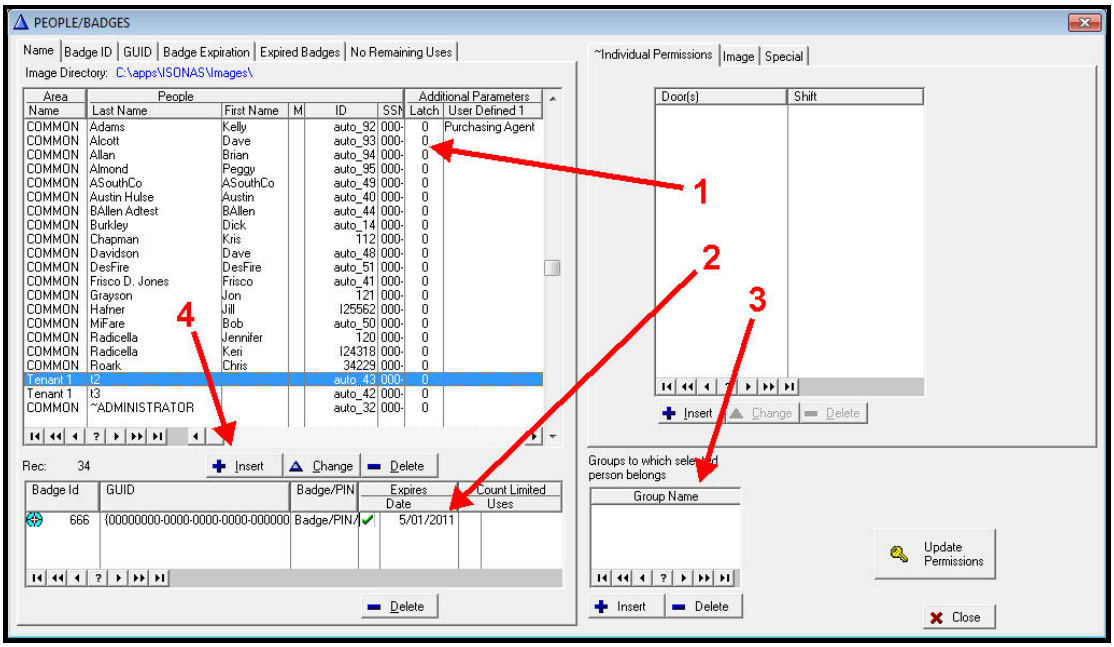
When you are finished adding Groups, Select the “Close” button on the Groups window.

Defining Users and their Associated Badges

Each user of the Access Control System must be defined within the application so that they can be authorized access through doors. This is done by selecting the “People” menu option and the “People/Badges” submenu option.

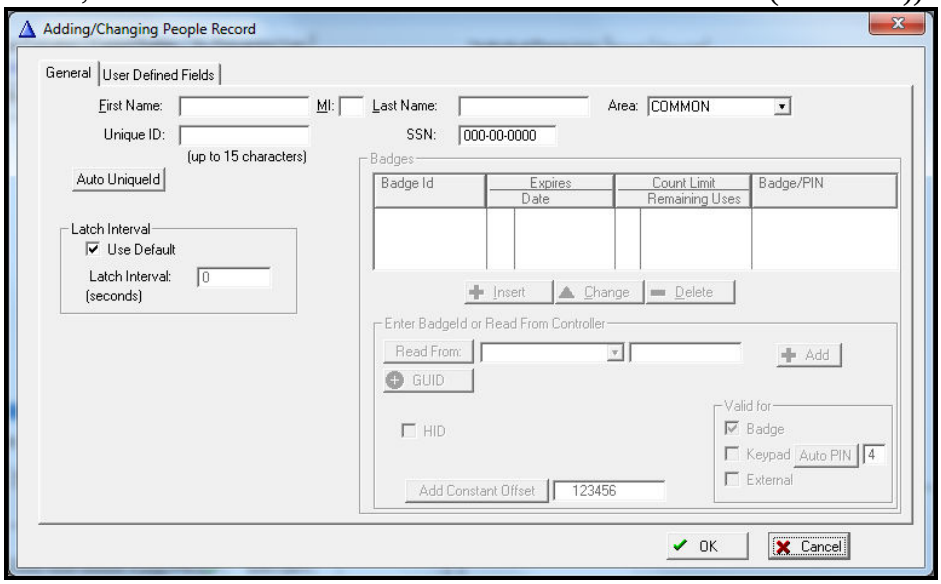


This will display the “People/Badges” window where people (users) and their associated badges can be defined and changed.



User List (Arrow #1) displays the Users that have been defined.
Badge List (Arrow #2) displays the Badges that have been assigned to the selected user
Group List (Arrow #3) displays the Groups that have been assigned to the selected user

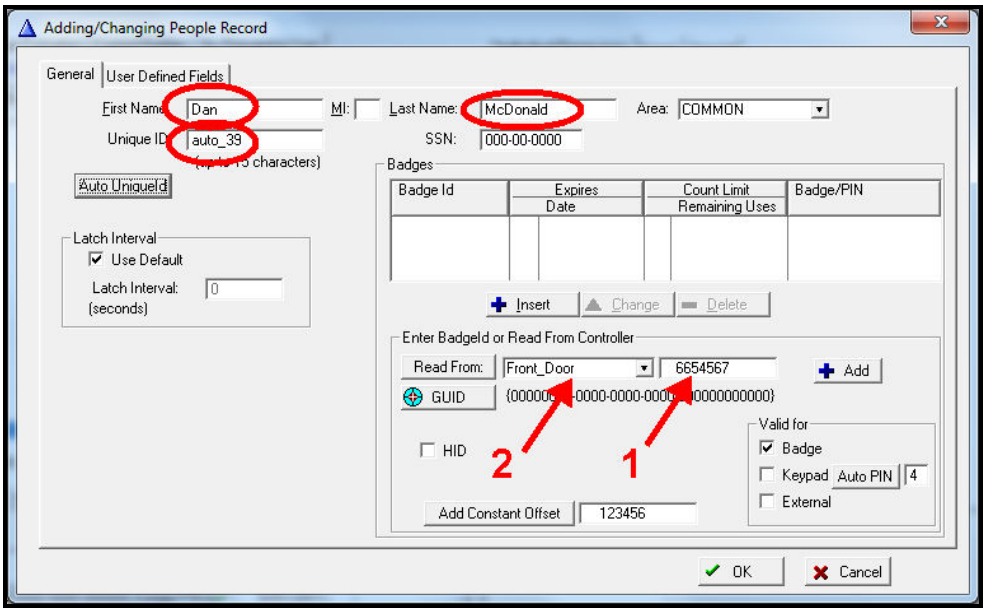
To add a new user, click the “Insert” button located under the User List (Arrow #4))



Enter the users name (Last name is required). The "Unique ID" must be defined. You can supply a "Unique ID" for the user (like their employee ID, etc) or let the application generate one for you by clicking the "Auto Unique ID" button.

Once the Unique ID Field has a value, then Badges for the user can be assigned.

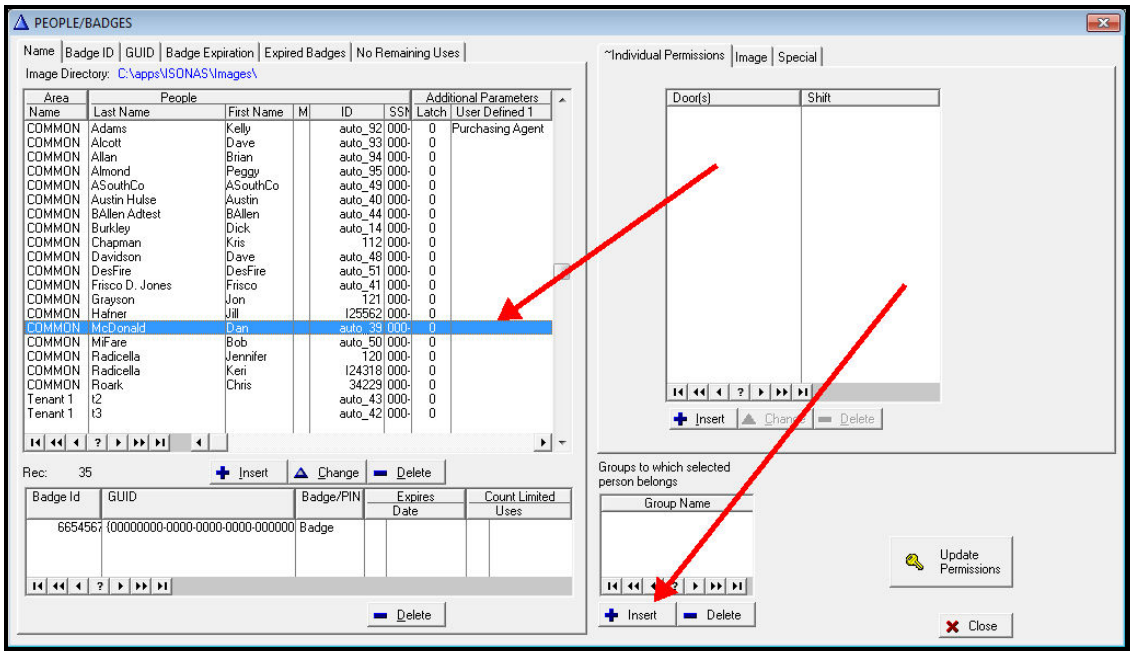
If you are using ISONAS badges, then enter a badge id into the "Enter BadgeId or Reader From Controller" entry field (1) and clicking on the "Add" button within the "Adding/Changing People Record" window. This will add an entry to the list of badge IDs. ISONAS Badge IDs are printed with labels affixed to the keyfob/badge/thin card.



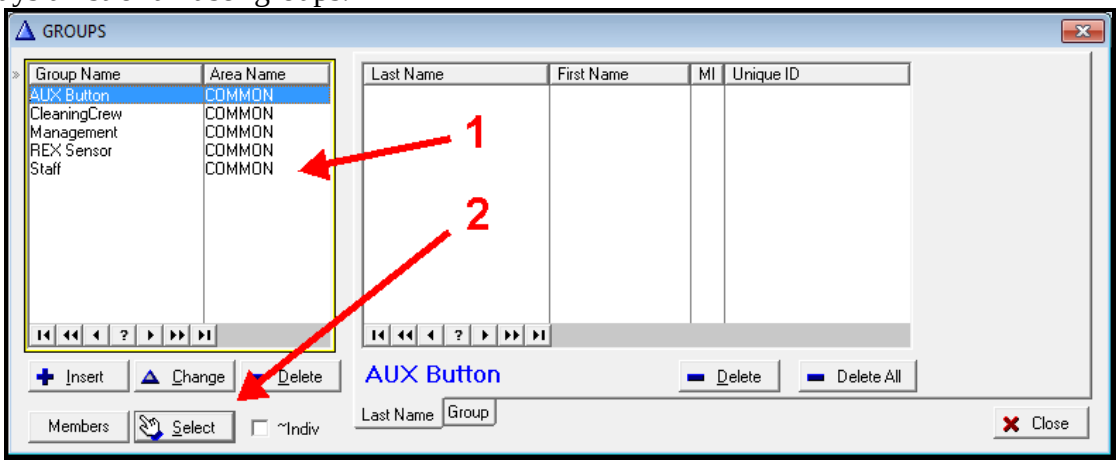
If you are using HID badges or need to read a badge for its ID, then

Select the Door associated with that reader/controller in Door list (Arrow #2)
Scan the HID Badge at an ISONAS reader/controller.
Click on the "Read From" button.
The Badge field (Arrow #1) will be populated with the ISONAS / HID Badge number.
Click on the "Add" button

When done assigning all the badges, keyfobs and/or thin card numbers to this user, click the "OK" button to save and close the add/change window. You will notice that the new user has been added to the list of user within the access control system and all their associated badges, keyfobs and/or thin card ID have been assigned



Each user has to be assigned to at least one user group. This is done by selecting the user within the list of users and clicking on the "Insert" button located under the Group Name list. This displays a list of all user groups.



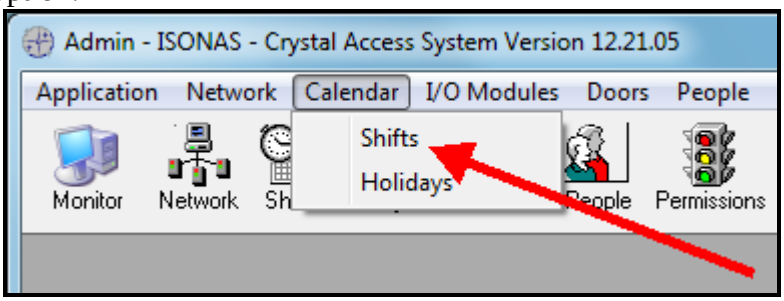
Select the Group Name you want the user to be associated with (Arrow #1) and click the "Select" button (Arrow #2). This will display the selected user group name in the "Group Name" list for the user. Repeat this step to add all the necessary group names to the user.

Repeat these steps to add the remaining users to the system.

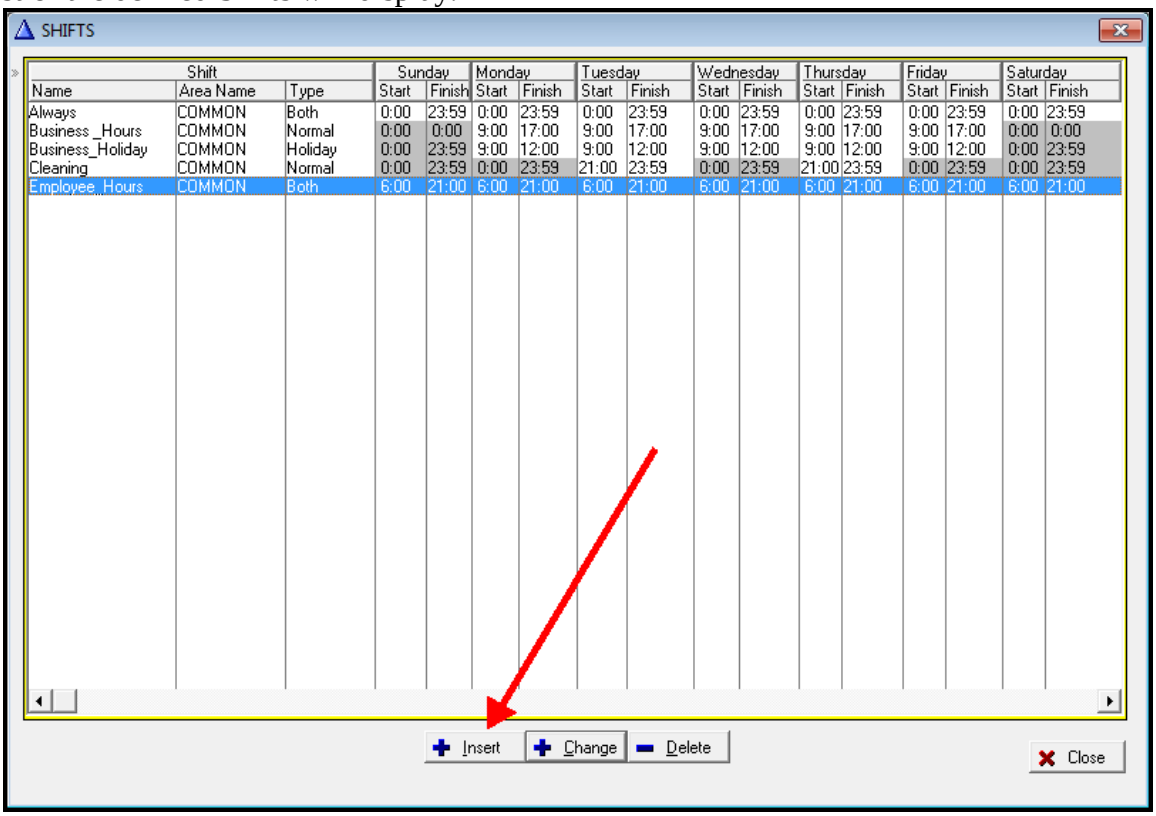
When finished, click the People/Badges window's "Close" button

Defining Shifts/ Authorized Time Ranges

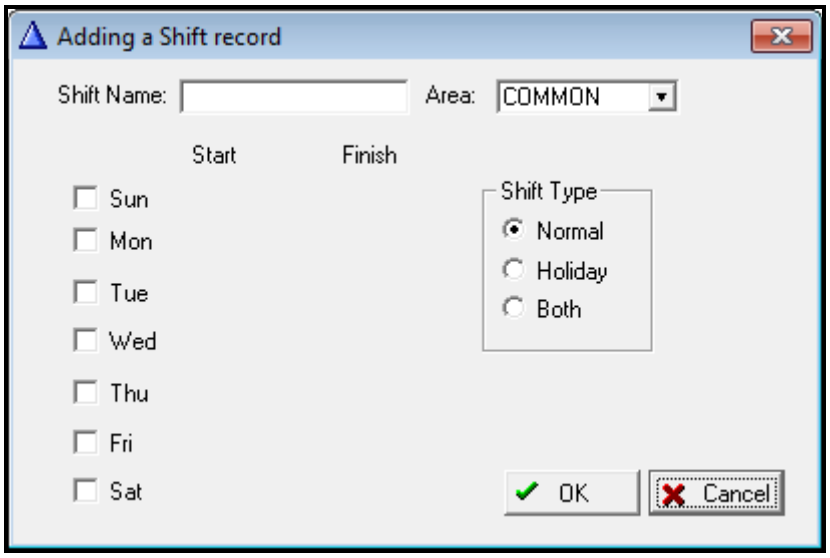
Users are authorized at a door based, in part, on the day of the week and the time of day. These authorization time ranges are defined as "Shifts". Select the "Calendar" menu option and the "Shift" submenu option.



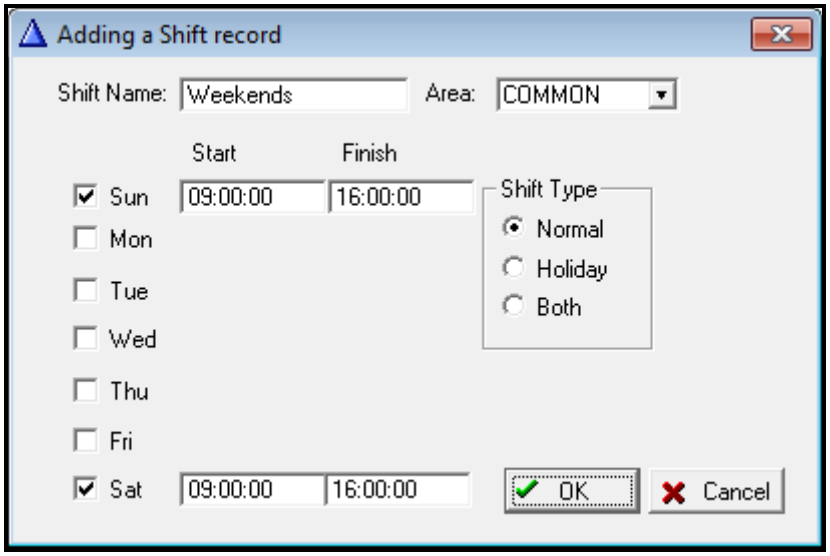
A list of the defined Shifts will display.



New shifts can be added by clicking on the "Insert" button.



A shift has to be uniquely named (like “Weekends”). For each day of the week, an authorized time range can be defined.
This time range is specified in military time (00:00 – 23:59).



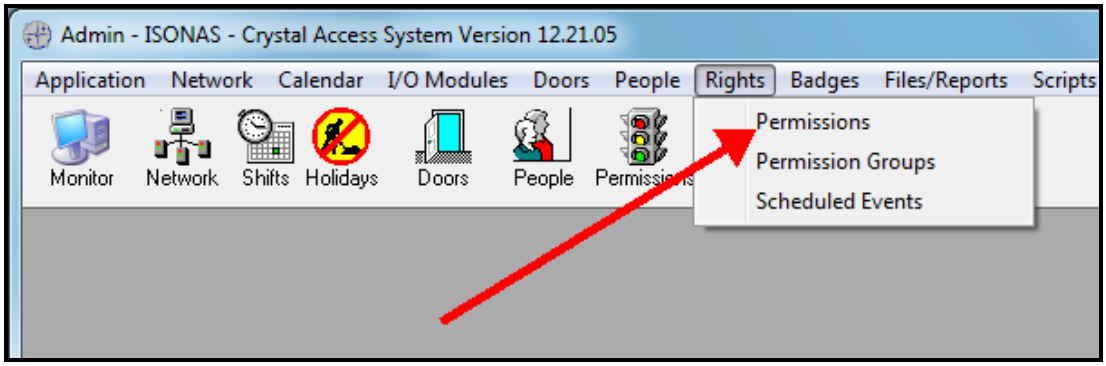
When done defining the time ranges for the shift, click the “OK” button to save and close the shift definition window.

Add all of the necessary shifts and then close the “Shifts” list window.

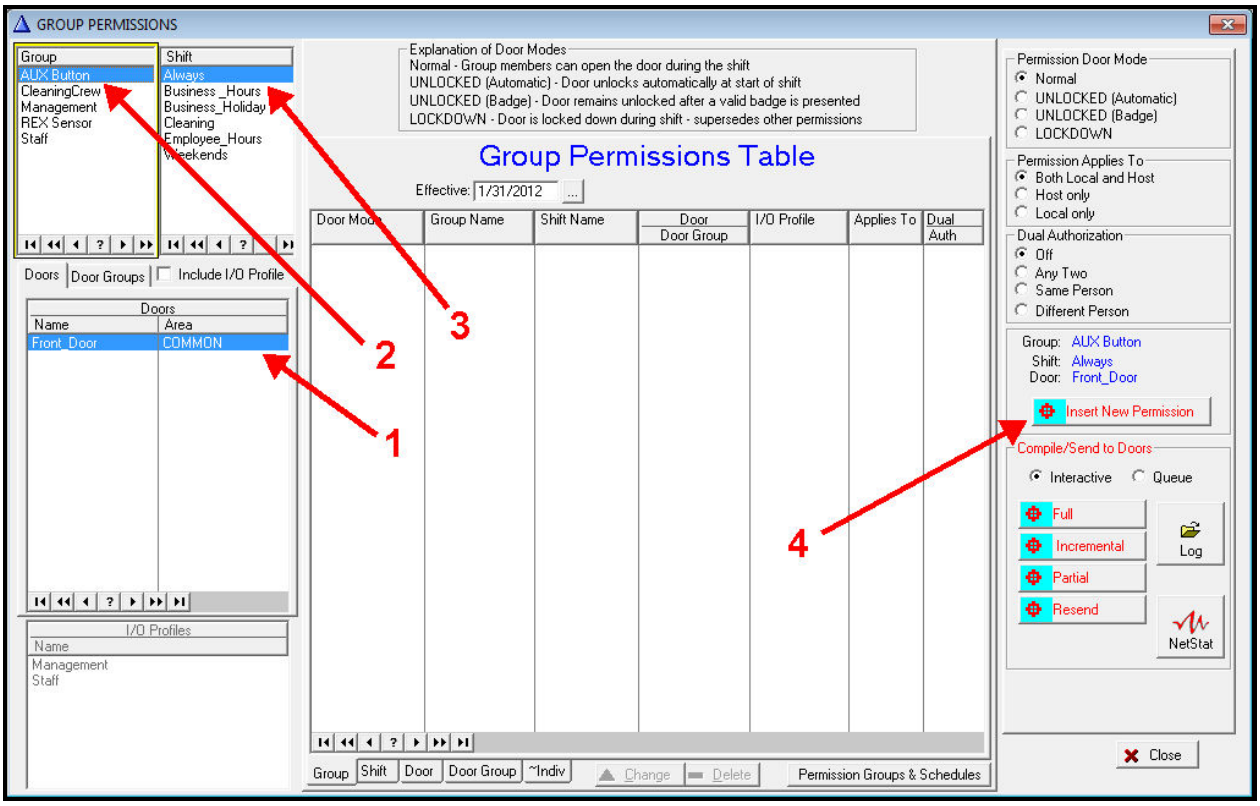
Assigning a Permission to a Door/Assigning Authorizations of User Groups to a Door

Now you will configure the system to grant access to a door, during a specified time period, to a group of users.

This is accomplished by defining “Permissions” at a door. To do this, Select the “Rights” menu item and the “Permissions” submenu item.



This will display the “Permissions” window.



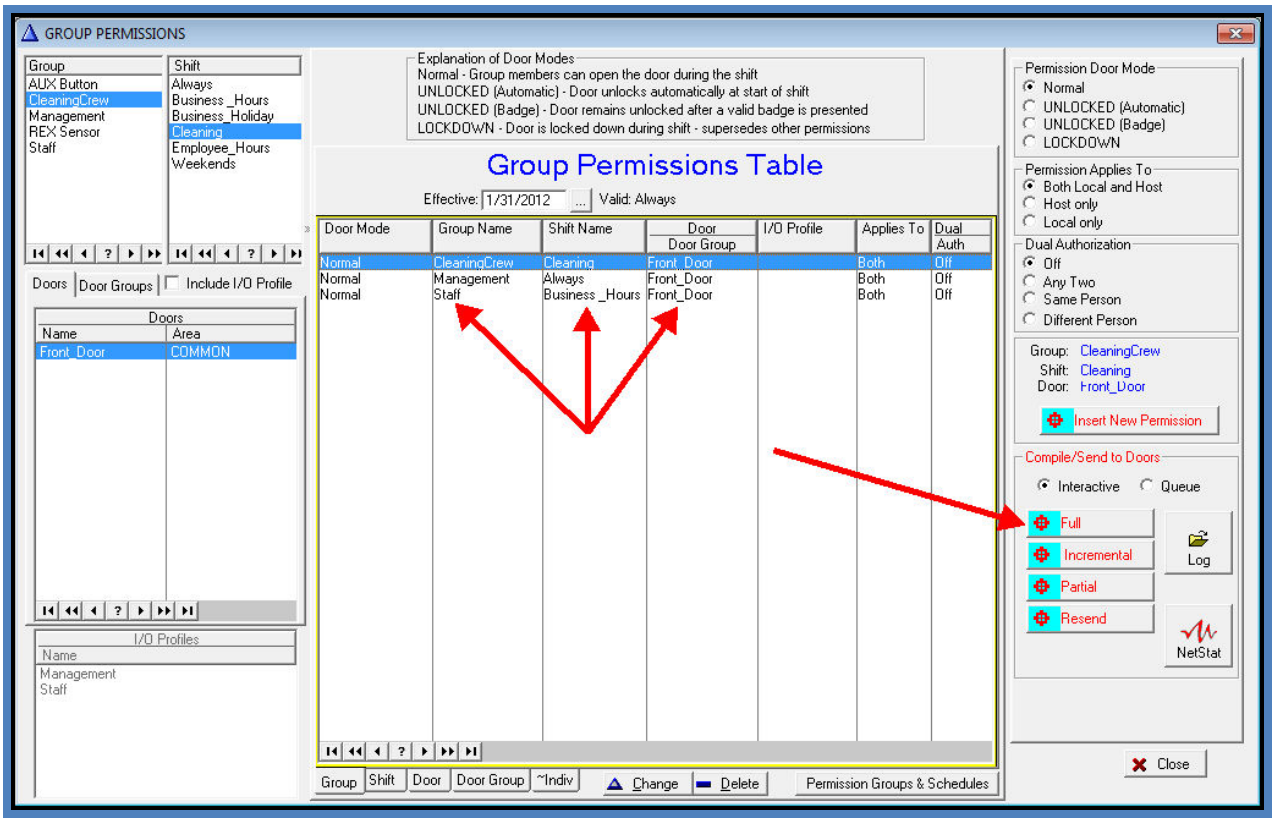
To create a “permission” for a door, you must first select a door to assign the permission to (Arrow #1).

For your chosen door, select the “Group” (user group) to authorize at the door (Arrow #2),

Select the “Shift” (time range) of time that the group with be authorized (Arrow #3).

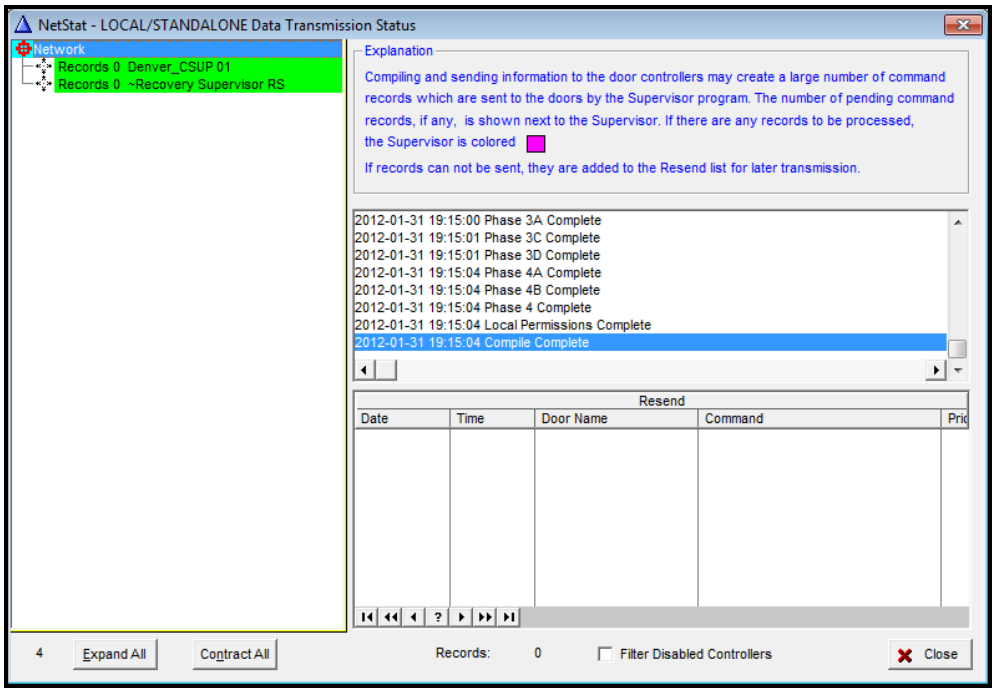
Make sure the “Permission Door Mode” option is set to “Normal” and the “Permission Applies to” option is set to “Both Local and Host”.

To create this permission, click the “Insert New Permission” button (Arrow #4). This will add the permission to the Permission Table.

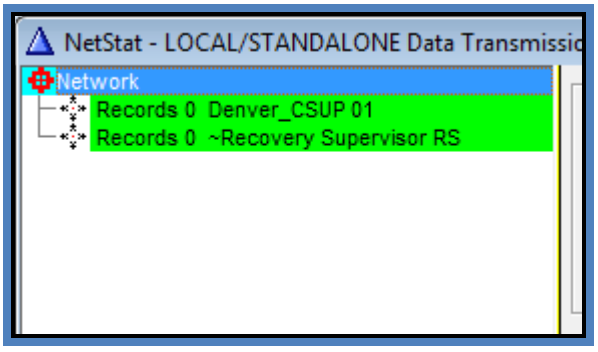


In the example, the “Front Door” has been assigned a permission consisting of the “Administration” user group authorized for the “Business Hour” shift. Create as many permissions as necessary.

When finished assigning permissions, you can click the “Full” button to “compile” the permissions. A window appears showing the status of the download process, which configures the reader/controller at the door with the data that it needs to function in standalone.



Once the download finishes, the NetStat window's CSUP entry will change color to Green.

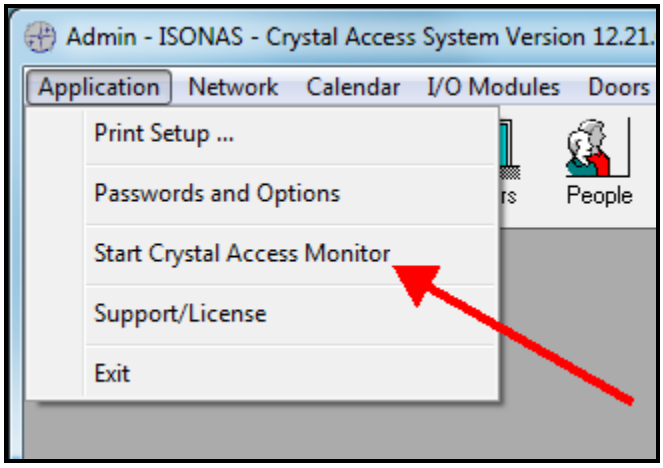


When finished, click on the NetStat window's"Close" button

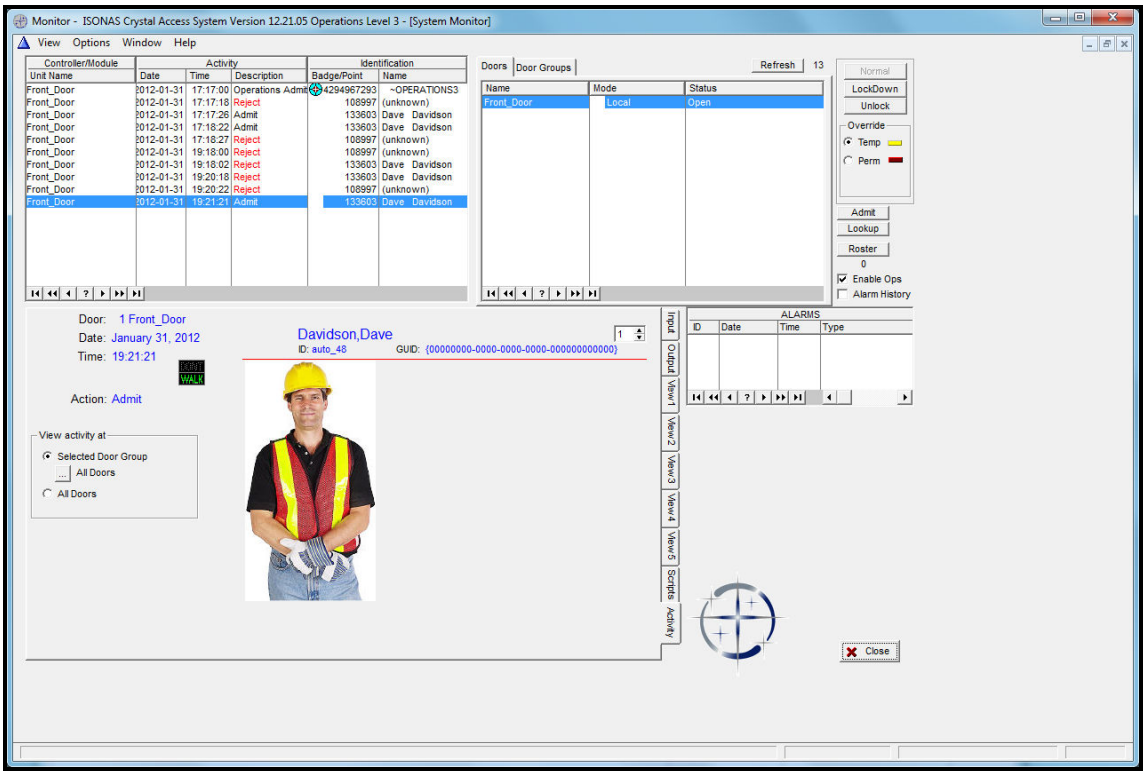
Testing the configuration

To test the system, you should run the “Monitor” application, and present one of the badges you just added to the system.

Select the “Application” menu option and the “Start Crystal Access Monitor” submenu option.



Once the Monitor appears, present the badge that you just assigned to the reader-controller. The history listing will show the badge presentation, and if the permissions allow entry, the person will be admitted.



Present a badge to the door reader/controller, and verify the activity appears in the activity list The badge will be accepted or rejected, depending on how you configured the system to handle that group/person/badge (Who), at that door (Where), during that time (When).

Congratulations,

You have just finished configuring the ISONAS Access Control System.