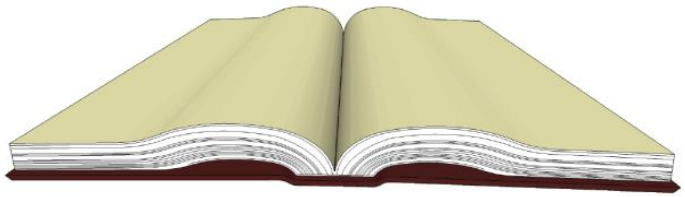
ReadyAXS

OSSI
YOUR WORLD SECURED



Documentation

ReadyAXS Reference Guide

Software Version 2.x.x

Copyright

OSSI, LLC.

OLTIS Security Systems International.

W228 N727 Westmound Dr.

Waukesha WI 53186

U.S.A.

Telephone: (262) 522-1870

Toll Free: (888) 488-2623

Trademarks

Software License Agreement

The following terms of service and end user license agreement (''EULA'') constitute an agreement between you (''Buyer'') and OSSI, LLC, and its affiliates (''OSSI''). This EULA governs your use of Software and Services (as specified below).

For purposes of this EULA ''Software'' means all software programs distributed, published or otherwise made available by OSSI or its affiliates including, but not limited to **ReadyAXS**. Software also includes updates and upgrades as well as accompanying manual(s), packaging and other written, files, electronic or on-line materials or documentation, and any and all copies of such software and its materials.

“Services” means all services made available by OSSI, including but not limited to services accessed through mobile device, by means of a browser or by other online communication method.

Software and Services are collectively referred to as ''OSSI Services”.

THE SOFTWARE IS LICENSED, NOT SOLD. YOUR USE OF THE SOFTWARE (AS SPECIFIED BELOW) IS SUBJECT TO THE TERMS AND CONDITIONS SET FORTH IN THIS EULA. BY INSTALLING, USING OR ACCESSING THE OSSI SERVICES OR ANY MATERIALS INCLUDED IN OR WITH THE OSSI SERVICES, YOU HEREBY ACCEPT THE TERMS OF THIS EULA.

If you do not accept the terms of this EULA, do not install, use or access the OSSI Services.

1. LICENSE

1.1 All software provided to Buyer shall be licensed subject to the terms and conditions of this Agreement. OSSI grants to Buyer and Buyer accepts a non-exclusive, non-transferable license to use any software and related documentation provided by OSSI pursuant to this Agreement (''Licensed Software'') for Buyer's own internal use, solely in conjunction with hardware supplied or approved by OSSI. In case of equipment failure, Buyer may use the Licensed Software on a back-up system, but only for such limited time as is reasonably required to rectify the failure.

1.2 Buyer acknowledges that OSSI may have encoded within the Licensed Software a ''license key'', establishing the usage and functionality (e.g., the number of equivalent nodes and Workstations or other features) of the software as it has been licensed to the Buyer. The usage or functionality of such Licensed Software may be expanded only upon payment to OSSI of an applicable upgrade fee. The above referenced license key shall be conveyed to Buyer upon installation of the Licensed Software or upgrade.

2. PROTECTION AND SECURITY OF LICENSED SOFTWARE

2.1 Buyer acknowledges and agrees that the Licensed Software contains proprietary and confidential information of OSSI and its third party suppliers and agrees to keep such information confidential. Buyer agrees not to allow access to the Licensed Software except by its employees having a need for such access, in keeping with its intended use as set forth herein. Such employees shall have been advised of the confidential and proprietary nature of information contained in the Licensed Software and shall have agreed to protect same.

2.2 All right, title and interest in and to the Licensed Software, other than that expressly granted to Buyer herein, shall remain vested in OSSI or its third party suppliers. Buyer shall not, and shall not permit others to: copy, translate, modify, create derivative works from, reverse engineer, decompile, encumber or otherwise use the Licensed Software,

except as is specifically authorized under this Agreement. All appropriate copyright and other proprietary notices and legends shall be retained on all Licensed Software supplied by OSSI, and Buyer shall maintain and reproduce such notices on any full or partial copies made.

3. TERM

3.1 The license shall become effective upon delivery of the Licensed Software to Buyer.

3.2 OSSI may terminate this Agreement and/or any license issued hereunder:

(a) upon written notice to Buyer if any amount payable to OSSI is not paid within thirty (30) days of the date on which payment is due;

(b) if Buyer becomes bankrupt, makes an assignment for the benefit of its creditors, or if its assets vest or become subject to the rights of any trustee, receiver or other administrator;

(c) if bankruptcy, reorganization or insolvency proceedings are instituted against Buyer and not dismissed within 15 days; or

(d) if Buyer breaches a material provision of this Agreement and such breach cannot be rectified or is not rectified within 15 days of receipt of written notice of the breach from OSSI

3.3 Upon termination of any license, Buyer shall return or destroy all copies of the respective Licensed Software. All obligations of Buyer arising prior to termination and those obligations relating to confidentiality and non-use, shall survive termination of this Agreement or of the license.

4. SUPPORT AND UPGRADES

Buyer shall receive software support and upgrades for the Licensed Software only to the extent provided for in the applicable OSSI software support program then currently in effect, and upon payment of any applicable fees.

5. CHARGES

Upon shipment of the Licensed Software, OSSI will invoice Buyer for all fees, and any taxes, duties and other charges. Buyer will be invoiced for any increased usage and functionality upon issuance by OSSI of a new software application key. All amounts shall be due and payable within thirty (30) days of receipt of invoice.

6. WARRANTIES

6.1 OSSI warrants, for a period of 90 days from the date of shipment, that the Licensed Software, as originally delivered to Buyer, will operate substantially in accordance with the functional description set out in the user manual supplied with the Licensed Software, when the Licensed Software is used in accordance with the user manual. OSSI's sole liability and Buyer's sole remedy for a breach of this warranty shall be OSSI’s good faith effort to rectify the nonconformity or, if after repeated efforts OSSI is unable to rectify the non-conformity, OSSI shall accept return of the Licensed Software and shall refund to Buyer all amounts paid in respect thereof. This warranty is available only once in respect of any Licensed Software, and is not renewed by the payment of fees for additional equivalent nodes or other increased use.

6.2 OSSI EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OR REPRESENTATIONS OF WORKMANSHIP, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, DURABILITY, OR THAT THE OPERATION OF THE LICENSED SOFTWARE WILL BE ERROR FREE.

6.3 Buyer acknowledges and agrees that the Licensed Software supplied under this contract are intended for standard commercial uses and are not specifically designed, manufactured or intended for use or resale in critical applications or hazardous environments requiring fail-safe performance and in which the failure of Licensed Software could lead directly to death, personal injury, or severe physical or environmental damage (including, without limitation, the operation or on-line control of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems). Such undertakings are considered "High Risk Activities." Suitability of Licensed Software for use in one or more High Risk Activities would require additional appropriate development and design engineering by OSSI including but not limited to the addition of appropriate redundancy and/or contingency procedures. OSSI and its suppliers explicitly disclaim any express or implied warranty of fitness for High Risk Activities and Buyer hereby agrees to release and hold OSSI harmless from liability resulting out of or in connection with implementation of these Licensed Software in High Risk Activities.

7. LIMITATION OF LIABILITY

IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF OSSI, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ANY CLAIM, REGARDLESS OF VALUE OR NATURE, EXCEED THE AMOUNT PAID PURSUANT TO THIS AGREEMENT FOR THE LICENSED SOFTWARE THAT IS THE SUBJECT MATTER OF THE CLAIM. IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF OSSI, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ALL CLAIMS EXCEED THE TOTAL AMOUNT PAID BY BUYER TO OSSI HEREUNDER. WITH THE EXCEPTION OF DAMAGES FOR THE MISUSE OR MISAPPROPRIATION OF SOFTWARE, PROPRIETARY PROPERTY OR CONFIDENTIAL INFORMATION, NO PARTY SHALL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL DAMAGES, WHETHER OR NOT SUCH DAMAGES ARE SPECIAL OR FORESEEABLE, AND/OR THE PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8. GENERAL

8.1 Under no circumstances shall either party be liable to the other for any failure to perform its obligations (other than the payment of any monies owing) where such failure results from causes beyond that party's reasonable control.

8.2 This Agreement constitutes the entire agreement between OSSI and Buyer with respect to the subject matter referenced and supersedes all prior oral and written communications. No alteration or amendment to this Agreement shall be valid unless the same shall be in writing and signed by authorized representatives of both parties.

8.3 If any provision of this Agreement is held to be invalid, illegal or unenforceable, it shall be deemed severed and the remaining provisions shall continue in full force and effect.

8.4 The Licensed Software may contain freeware or shareware obtained by OSSI from one or more third party source(s). No license fee has been paid by OSSI for the inclusion of any such freeware or shareware, and no license fee is charged to Buyer for its use.

BUYER ACKNOWLEDGES AND AGREES THAT THE THIRD PARTY SOURCE(S)

PROVIDE(S) NO WARRANTIES AND SHALL HAVE NO LIABILITY WHATSOEVER IN RESPECT OF BUYER'S POSSESSION AND/OR USE OF THE FREEWARE OR SHAREWARE.

8.5 OSSI shall have the right, at its own expense and upon reasonable written notice to Buyer, to periodically inspect Buyer's premises and such documents as it may reasonably require, for the exclusive purpose of verifying Buyer's compliance with its obligations under this Agreement.

8.6 Any notice provided hereunder shall be sent to the party's respective address, or to any other such address as may be specified from time to time. Notices shall be deemed to have been received five days after deposit with a post office when sent by registered or certified mail, postage prepaid and receipt requested.

8.7 If the Licensed Software is being acquired by or on behalf of any unit or agency of the United States Government, the following provision shall apply: If the Licensed Software is supplied to the Department of Defense, it shall be classified as "Commercial Computer Software" and the United States Government is acquiring only the rights specified in this License Agreement as defined in DFARS 227.7202-1(a) and 227.7203-3(a). If the Licensed Software is supplied to any other unit or agency of the United States Government, rights will be defined in Clause 18-52.227-86(d) of the NASA Supplement to the FAR.

8.8 Buyer shall comply with all export regulations pertaining to the Licensed Software in effect from time to time. Without limiting the generality of the foregoing, Buyer expressly warrants that it will not directly or indirectly export, re-export, or transship the Licensed Software in violation of any export laws, rules or regulations of Canada, the United States or the United Kingdom.

8.9 No term or provision of this Agreement shall be deemed waived and no breach excused unless such waiver or consent is in writing and signed by the party claimed to have provided such waiver or consent. No waiver by either party of any right, failure to perform or of any breach by the other party hereunder, shall be deemed to be a waiver of any other right hereunder or of any other breach or failure by such other party, whether of a similar nature or otherwise.

8.10 This Agreement shall be governed by and construed in accordance with the laws of Wisconsin. The application of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded. It is the express wish of the parties that this Agreement and all related documents be drawn up in English. C’est la volonté expresse des parties que la présente convention ainsi que les documents qui s’y rattachent soient rédigés en anglais.

Table of Contents

Table of Figures

Installation of Software

Basic PC Requirements

Intel Core 2 Duo 2
50 GB Hard Drive
1 GB RAM
10/100 NIC

Operating System Supported by the Software

Windows XP SP3
Windows 7
Windows Server 2003 SP2
Windows Server 2008
Windows Server 2008 R2

Software Setup

As part of best practices, it is usually wise to save and close all programs before beginning any installation of software. As part of the installation for this software, the computer may need to reboot. Therefore, close all other programs before beginning the installation process.

Insert the CD. Run “setup.exe”. If your computer does not have the Microsoft .NET Framework installed, you will be presented with EULA for the Microsoft .NET Framework which the software requires to run. Select “Accept” to install the .NET Framework.

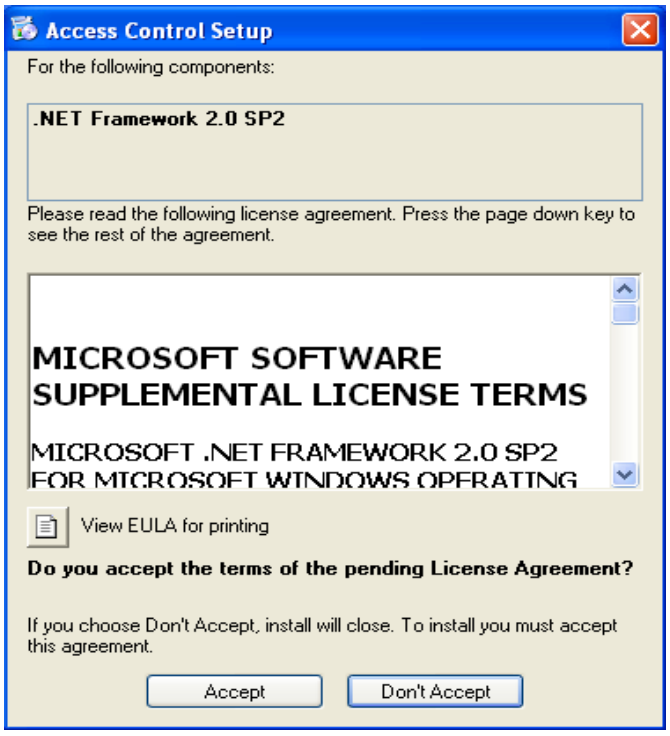


Figure 1 – Setup Dialog for the .Net Framework

You will encounter the following error if your computer is running Windows XP SP2 or older. You must abort and install Service Pack 3.

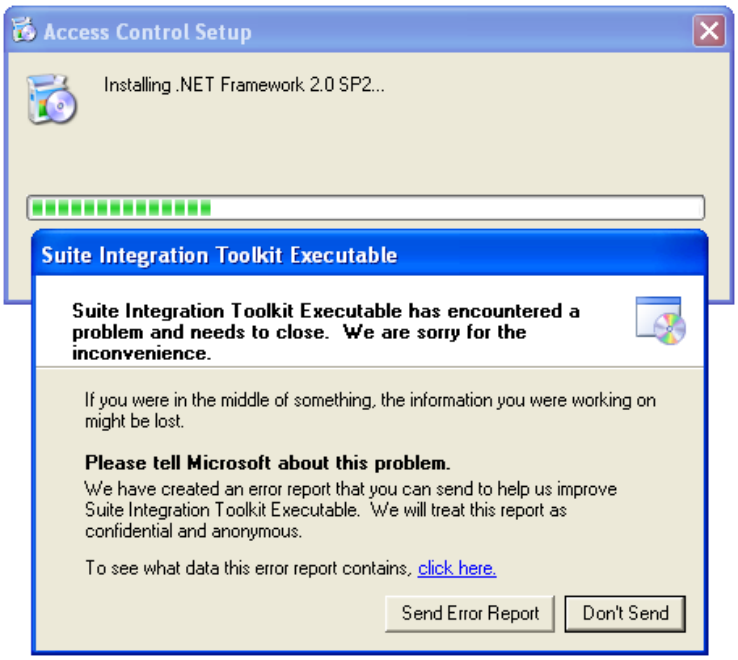


Figure 2 - Windows XP SP2 Error

Once the .Net Framework installs, the computer must be reboot before proceeding.

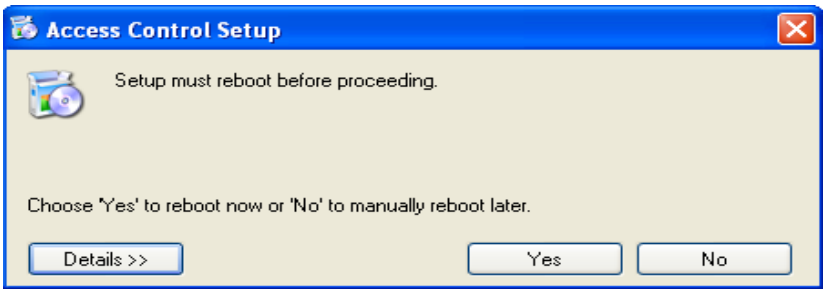


Figure 3 - Setup Dialog Requesting Reboot

Select “Yes”.

If your computer already has the .NET Framework, it will not need to reboot.

At this point, the “Access Control Setup Wizard” dialog will appear and installation continues. The wizard will guide you through the rest of the installation process.

Figure 4 - ReadyAXS Setup Wizard

Select “Next”.

You will then be asked to select the installation folder.

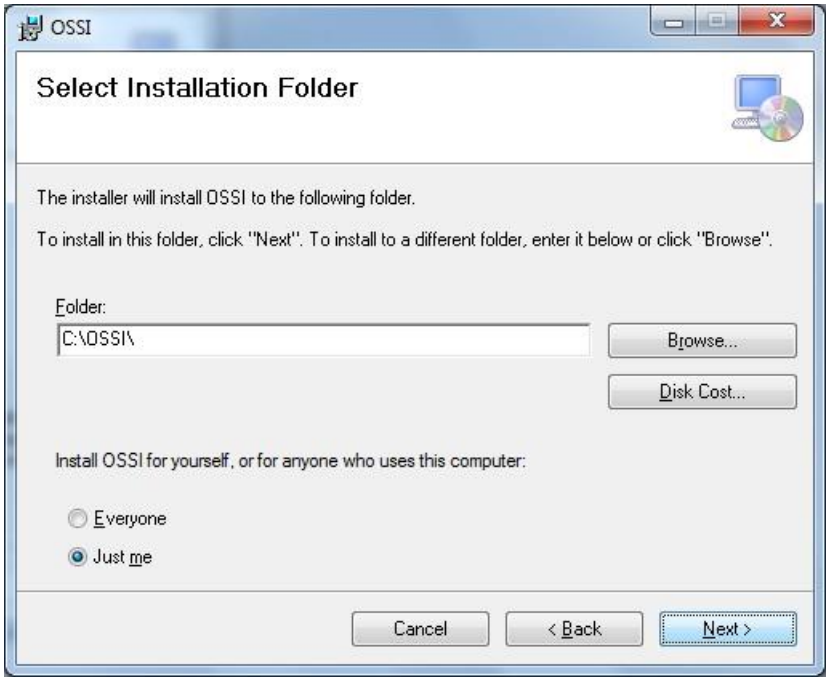


Figure 5 - Select Installation Folder

Select “Next”.

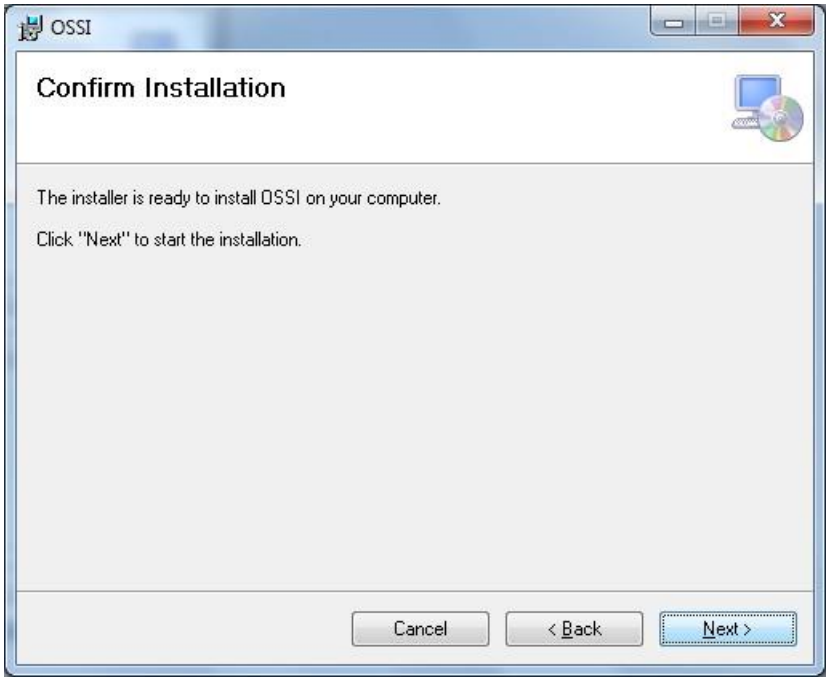


Figure 6 - Confirm Installation

You have provided all the information necessary to complete the installation. By selecting “Next”, you will confirm that the information provided is correct and the software will be installed.

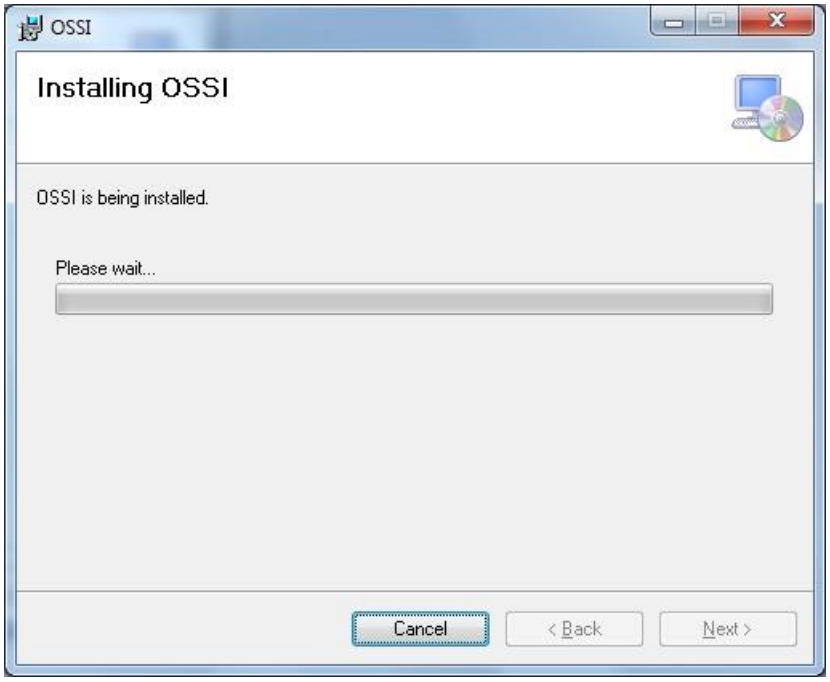


Figure 7 - Installation Progress Dialog

Pressing “Cancel” at any time will abort the installation.

Once the installation is complete, the following dialog appears.

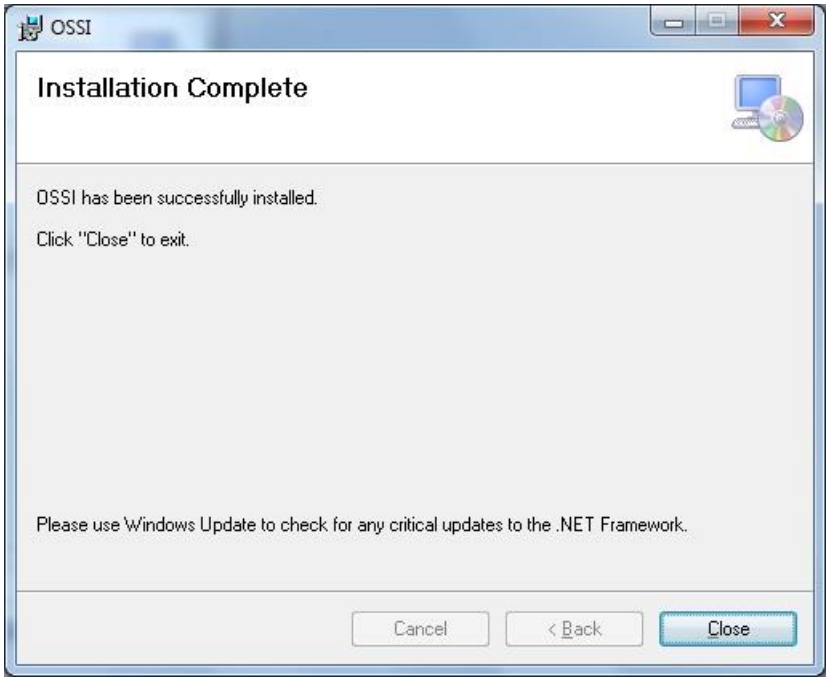


Figure 8 - Installation Complete Dialog

Select “Close”.

Following the install, this icon  will appear automatically on the desktop.

Uninstall

To uninstall ReadyAXS, use the appropriate Control Panel to do so. For WindowsXP, use “Add or Remove Programs”. For Windows 7, it is called “Programs and Features”. The software uninstalls in the standard way.

Login

Click the  icon on the desktop or from the Start menu select All Programs. Look for the same icon and OSSI at the root level. The ReadyAXS login screen will appear.

Figure 9 - ReadyAXS Login Screen

The default user name is "master" and the password is "m".

After successful login, the ReadyAXS main screen will appear:

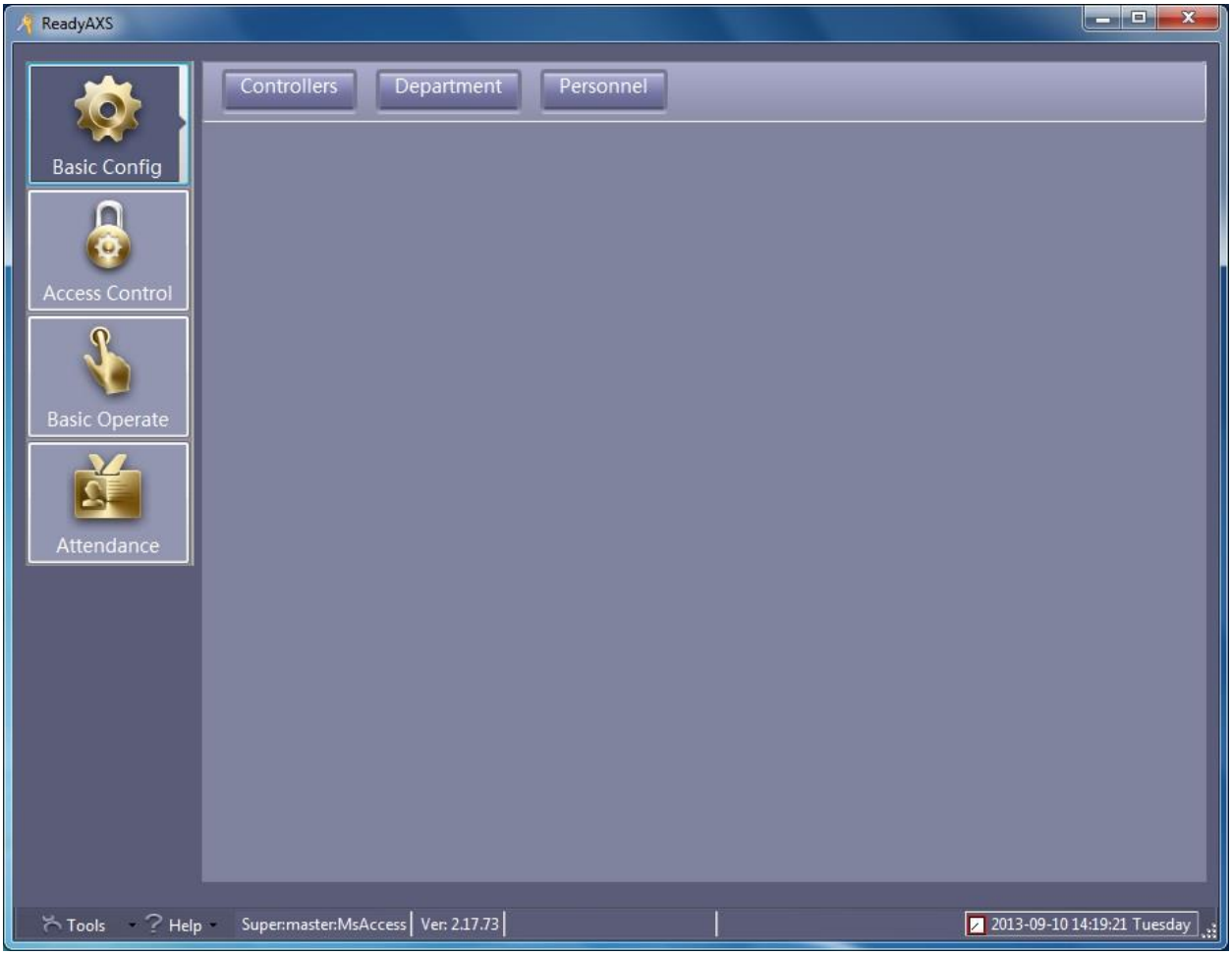


Figure 10 - ReadyAXS Main Screen

The ReadyAXS main screen contains a vertical column of buttons on the left known as the mode buttons, the region to the right of said buttons known as the page, and the status bar across the bottom. The content of the page changes depending on the mode selected. But it will usually display a header region of buttons above a table of information related to the button pressed. As we explore each mode, this will become clearer.

ReadyAXS comes up ready for you to begin configuring your system displaying the **Basic Config** mode and context.

Basic Config

In **Basic Config** mode, you can manage controllers, departments, and personnel. Click on the "Basic Config" button in the mode menu to enter **Basic Config** mode.

Controllers

To set up your controllers select "Basic Config" mode. In the basic configuration region header, click the "Controllers" button.

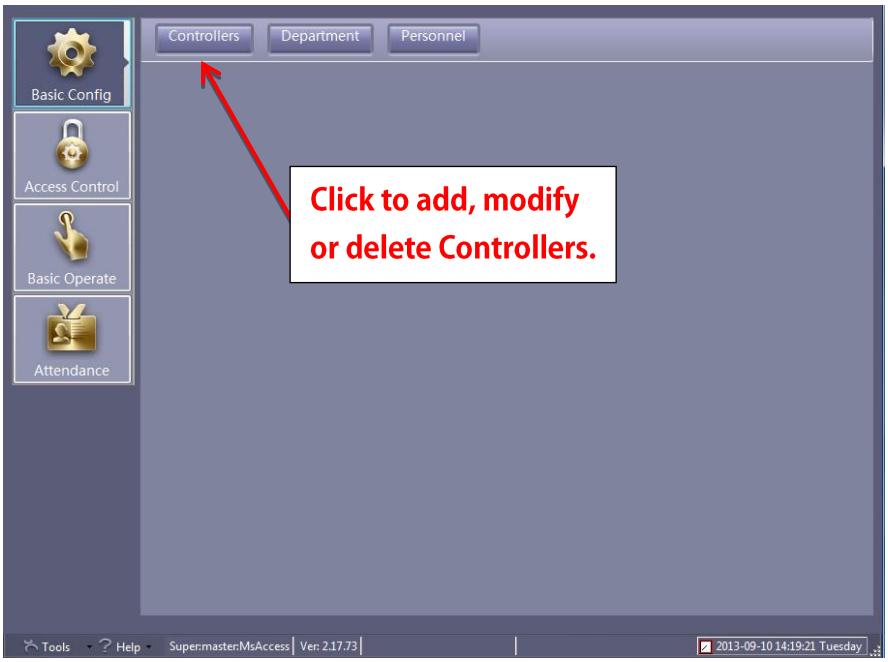


Figure 11 – Controllers Button on the Basic Config Screen

The Controllers page displays to the right of the mode buttons and below the page header buttons.

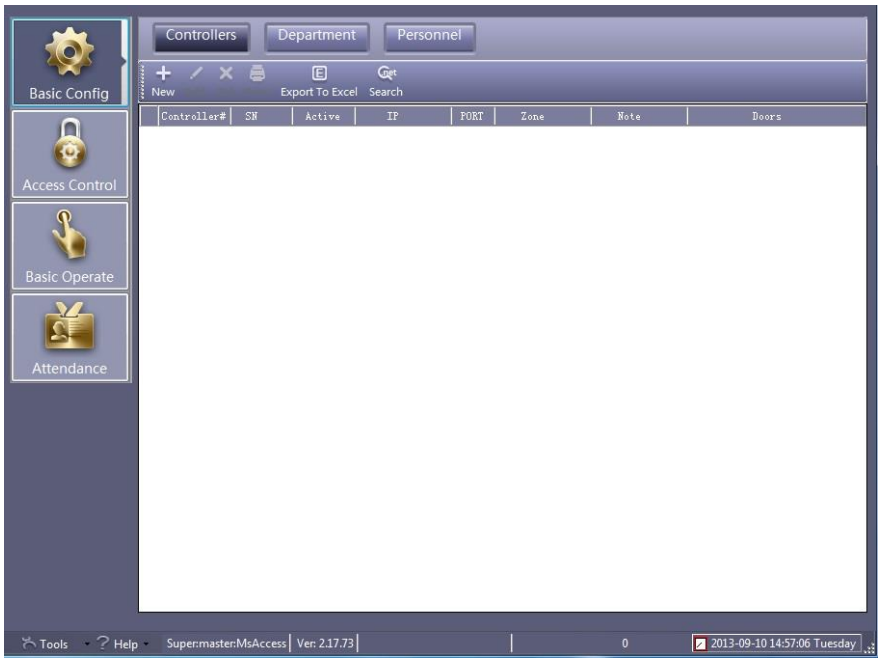


Figure 12 - Controllers Page

Initial IP Setup of Controller

The simplest way to add controllers to the system is to do so automatically. If the controllers are powered up and connected to the TCP/IP network, they can be discovered by and clicking on the "Search" button in the toolbar.

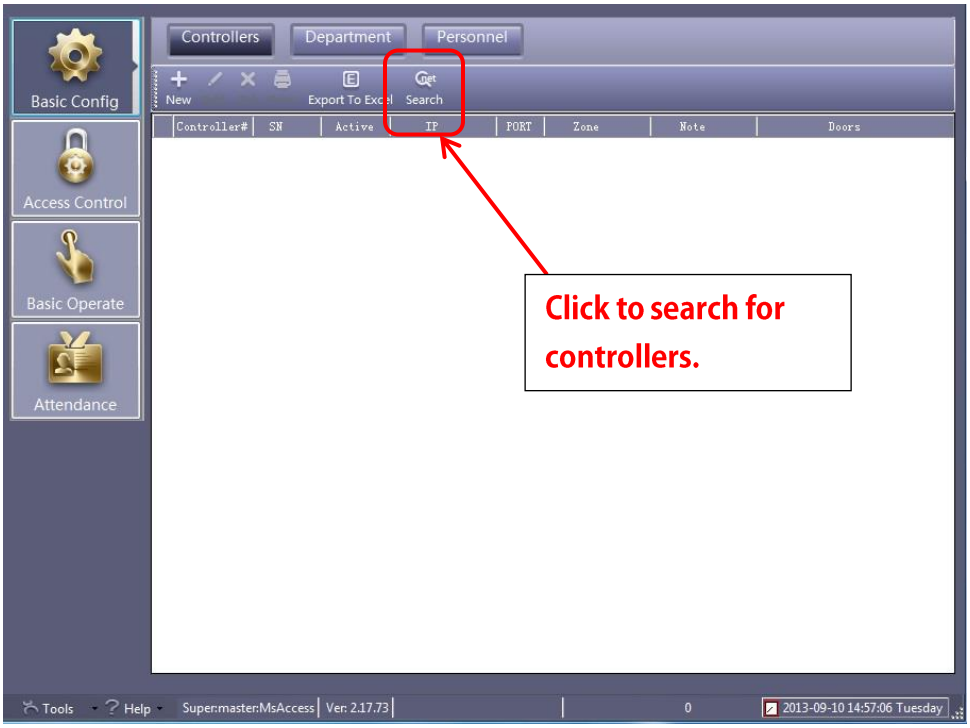


Figure 13 – Search Tool on the Controllers Page

Searching the network for attached controllers should take 3 to 5 seconds. Once the controllers are located on the network they will appear in the "Search Controller" window.

Since the controllers all have the same default IP address, 192.168.0.0, you will need to know the serial numbers of your controllers and where they are located on your site. If you don't have that information readily available, you can connect the controllers one at a time, have ReadyAXS search and locate it then configure and save the IP settings. Repeat this process until all controllers are connected and configured.

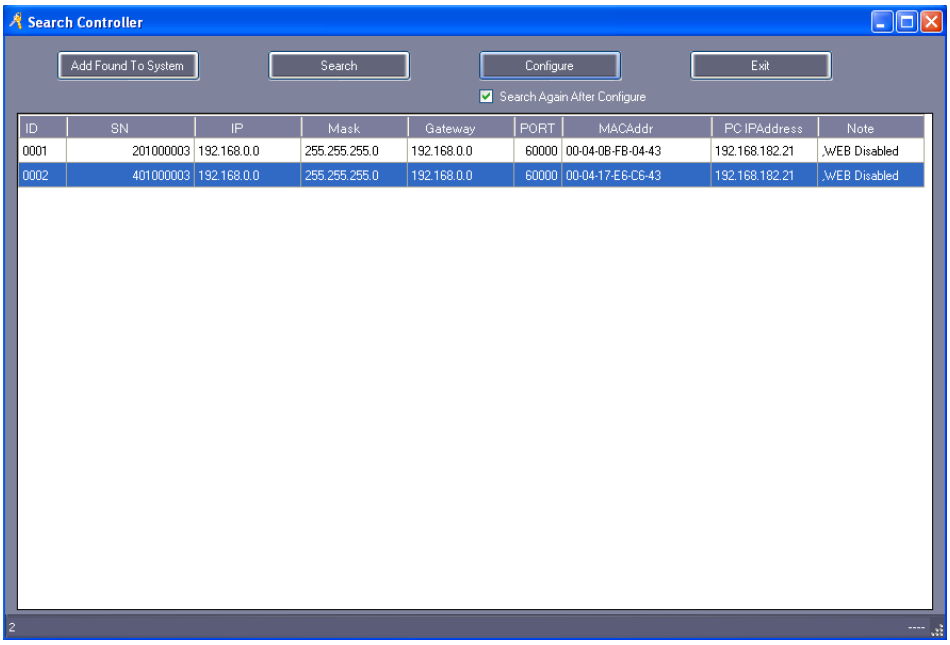


Figure 14 - Search Controller Dialog after successful "Search"

Highlight the desired controller and Select **"**Configure". The IP configuration screen will appear.

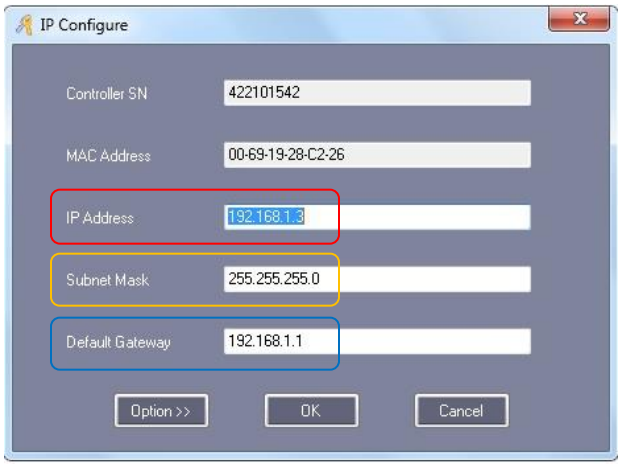


Figure 15 - IP Configuration Screen

In the appropriate boxes, type in the IP address, subnet mask, and gateway address. Then select "OK". Do this for every controller.

To save the controllers and their configuration you must click 

on the "Search Controller" dialog. None of the changes will go into effect until you do so.

Editing Controllers

After your IP settings for the controllers are established, you may edit the controllers.

From the “Controllers” screen highlight the controller and select “Edit”.

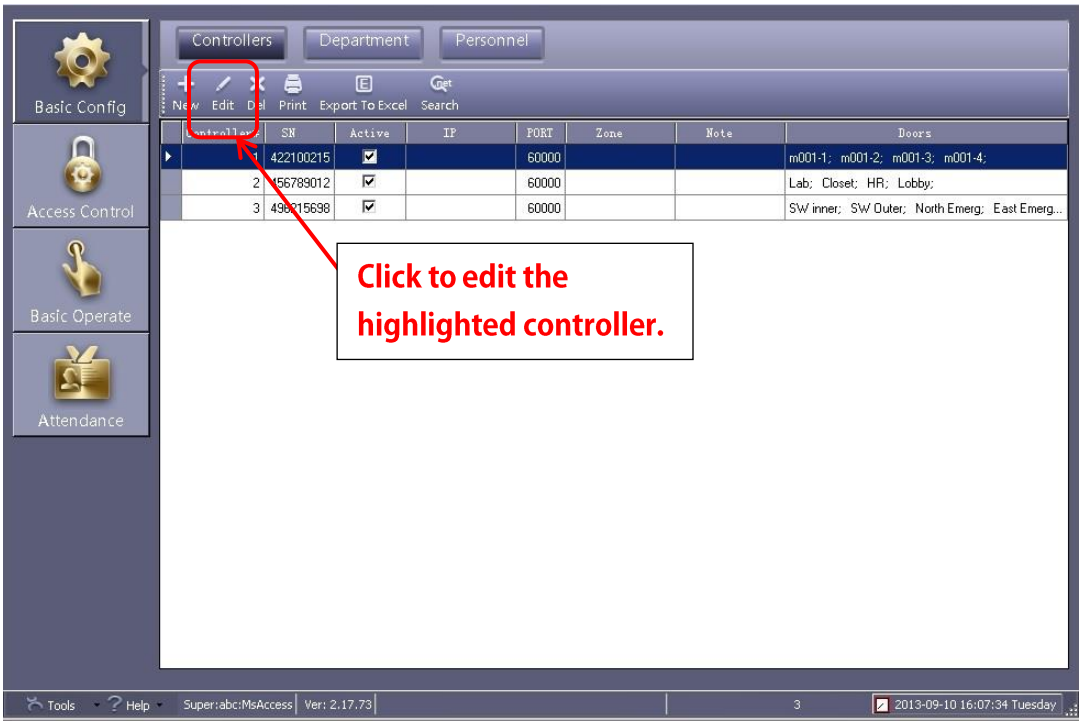


Figure 16 - Edit Tool on the Controllers Page

The Edit Controller dialog appears.

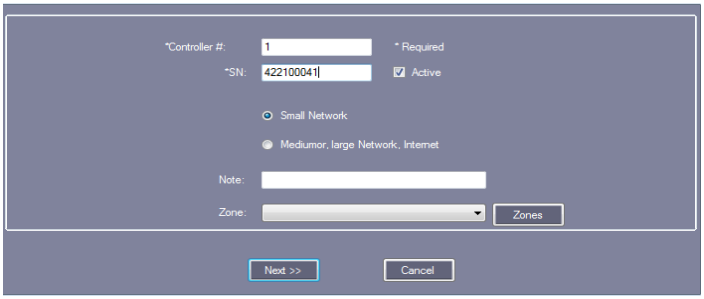


Figure 17 - Edit Controller Screen

From the Edit Controller screen, the administrator can modify the following information:

- The “Controller #” is automatically assigned. ***It should not be changed.***
- The “SN” is automatically populated and ***should not be changed.***
- The “Active” checkbox indicates the state of the controller. Only active controllers are visible when assigning access privileges.
- The radio buttons entitled “Small Network” and “Medium, Large, Internet” ***should not be changed*** as these settings were established when the IP settings were configured.
- The “Note” field can be used to identify the controller location, description, and date of service.
- The “Zone” drop down list allows the administrator to logically group controllers to reflect their physical location.

Select “Cancel” to exit without saving. To continue on to editing the doors, select “Next >>”.

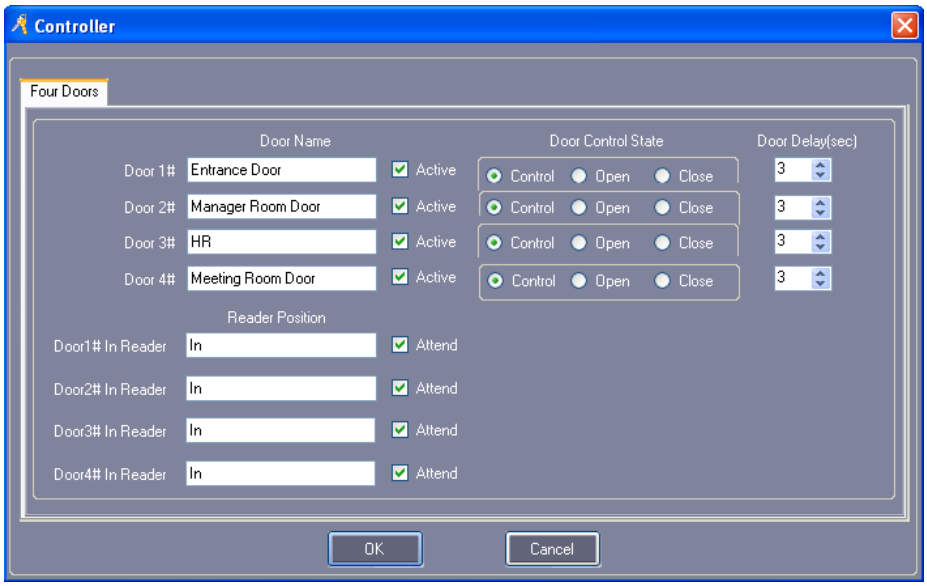


Figure 18 - Doors Configuration Screen

When editing the controllers the following parameters can be modified on a door by door basis:

- The Door Name
- The "Active" checkbox which shows if the reader attached to that door is active
- The "Door Control State" radio buttons which indicate the state of the door
    - "Control" indicates the reader is active and ready to be used to control access
    - "Open" indicates the relay will remain open (not used very often)
    - "Closed" indicates the relay will remain closed (not used very often)
- The "Door Delay" drop down box which indicates how long the relay will activate on a valid card read or Request to Exit (REX)
- The "Reader Position" which is used for attendance reports only. Each reader can be either an "In" reader or an "Out" reader
- The "Attend" checkbox which when checked will include that reader in attendance reports

Select "OK" to commit and save the changes. Select "Cancel" to exit without saving.

Department

Adding departments will allow you to organize the card users. These departments are more about time periods and location than they are about organizational departments. They are about who has accesses to what and when. If your sales department has the same time schedule, say 8:00am to 5:00pm Monday to Friday, then create a sales department. If your maintenance staff has two or three shifts, then create a department branch for each shift.

All departments and branch departments behave the same. Branches may help you organize the departments logically. For example, the Maintenance Department has three shifts. Add a Top Tier for Maintenance then add branches for Shift 1, Shift 2, and Shift 3. Or the other way around might work. Your facility has three shifts; each shift has different groups of people. Add a Top Tier for each shift and branches for the groups of people in each shift.

Careful planning of departments, considering time schedules and locales, will make assigning access privileges later on much easier. Departments aren't necessary if all card users will have the same access 24/7.

Add Top

To add a department, click on “Department” at the top of the **Basic Config** screen.

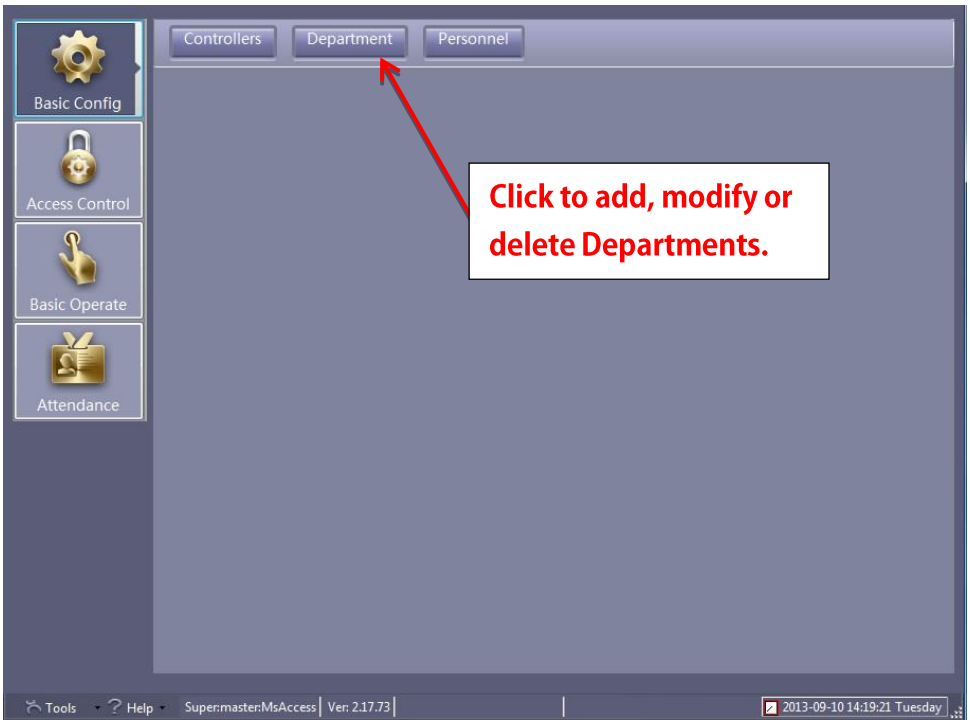


Figure 19 - Department Button on the Basic Config Screen

The Department Page will display. You must define the top tier department and then if necessary the branch tiers. First, select the “Add Top” tool to add the top tier.

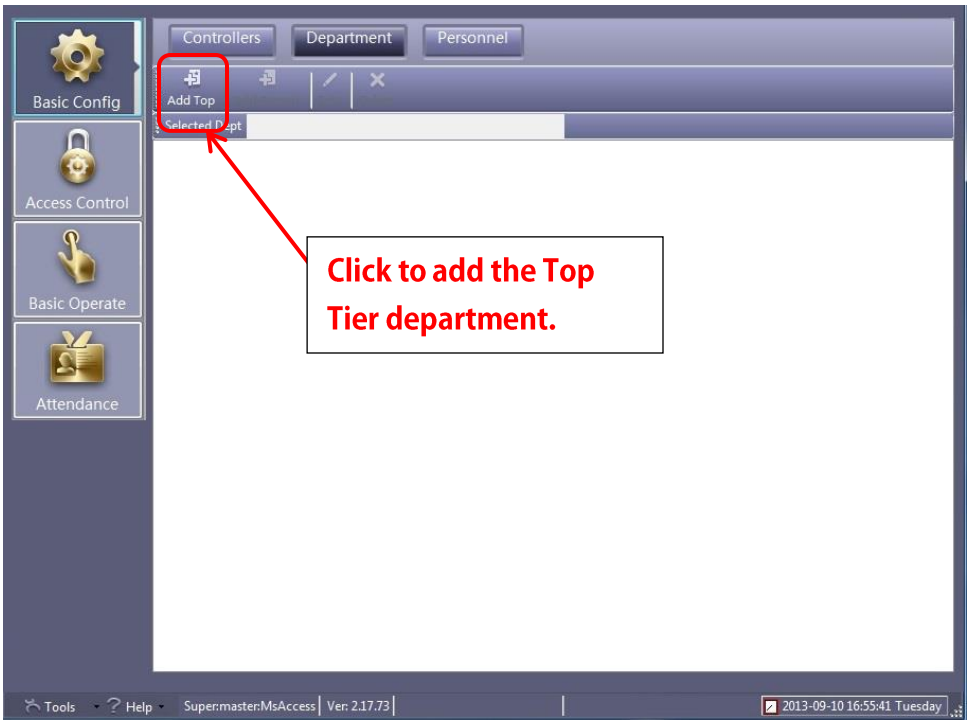


Figure 20 – Add Top Tool on the Department Page

The “Add Top” dialog appears. After inserting your top tier department description select “OK” to save it. “Cancel” will exit without saving.

Figure 21 – Add Top Dialog

Add Branch

To add a branch department, highlight the top tier department from which to branch. Then click the “Add Branch” tool.

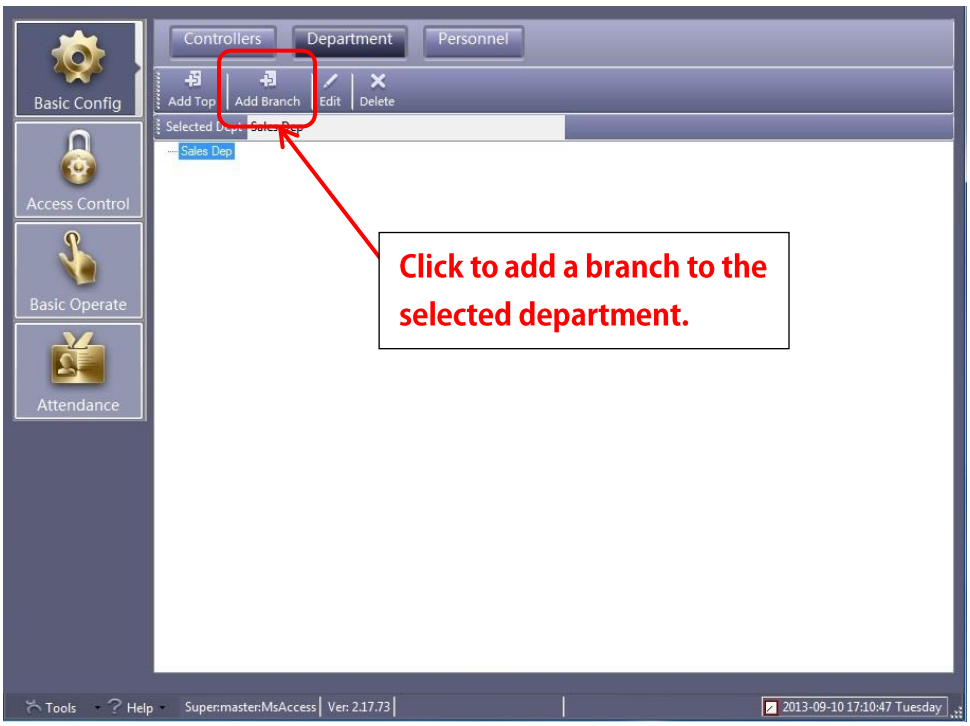


Figure 22 - Add Branch Tool on the Department Page

Personnel

The “Personnel” button allows you to add and edit users. Users are card holders, people with cards that will be granted or denied access. Users and card holders are used interchangeably.

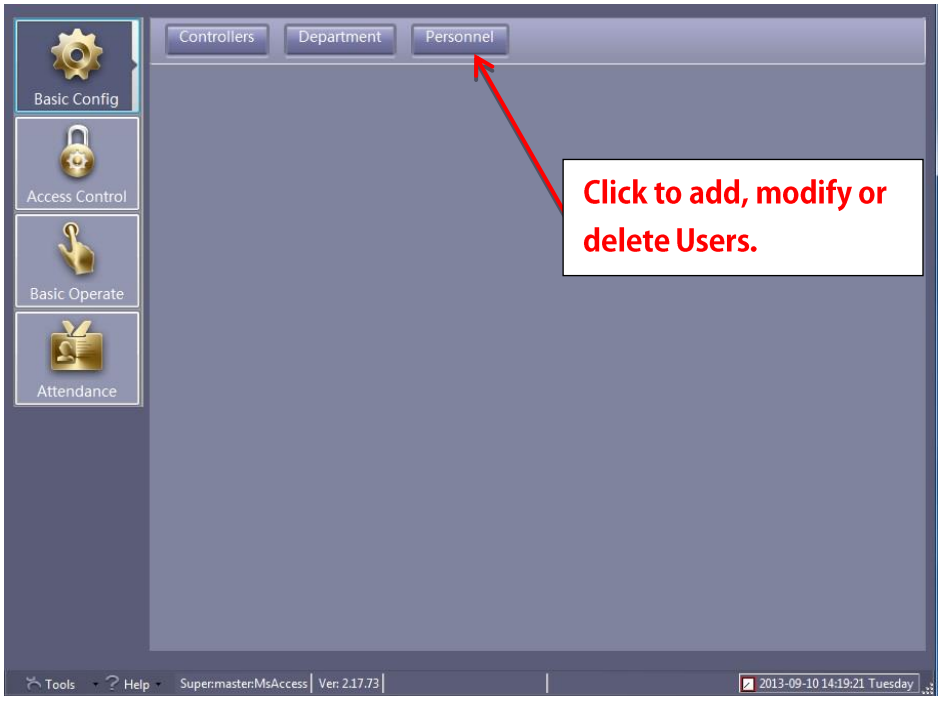


Figure 23 - Personnel Button on the Basic Config Screen

Adding Users Individually

Adding card holders, or users, individually is done by selecting the “Add” tool on the Personnel screen.

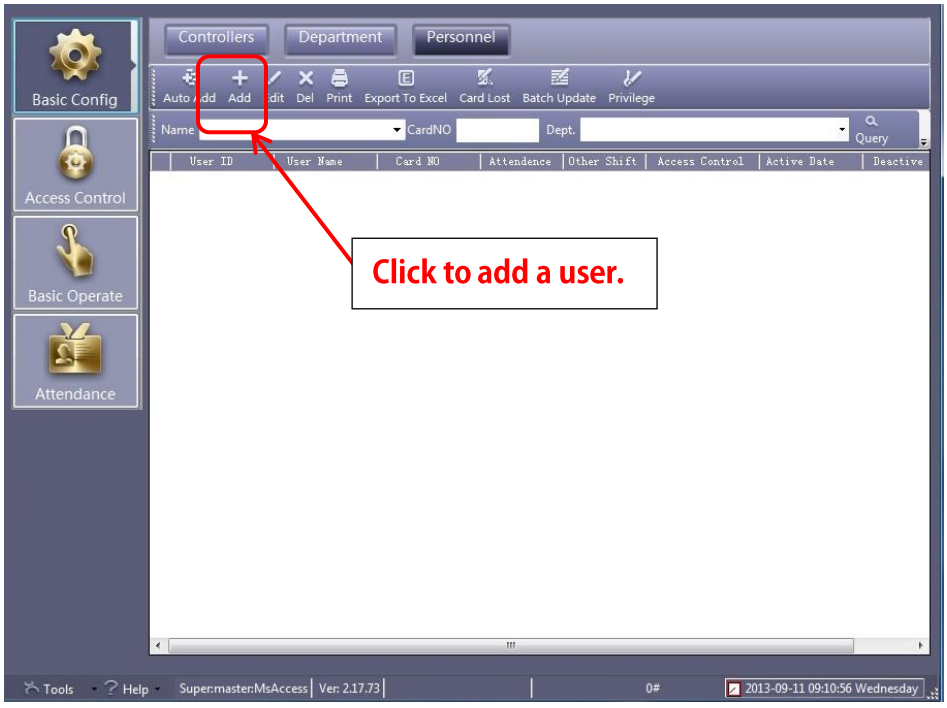


Figure 24 - Add Tool on the Personnel Page

A blank User dialog will appear.

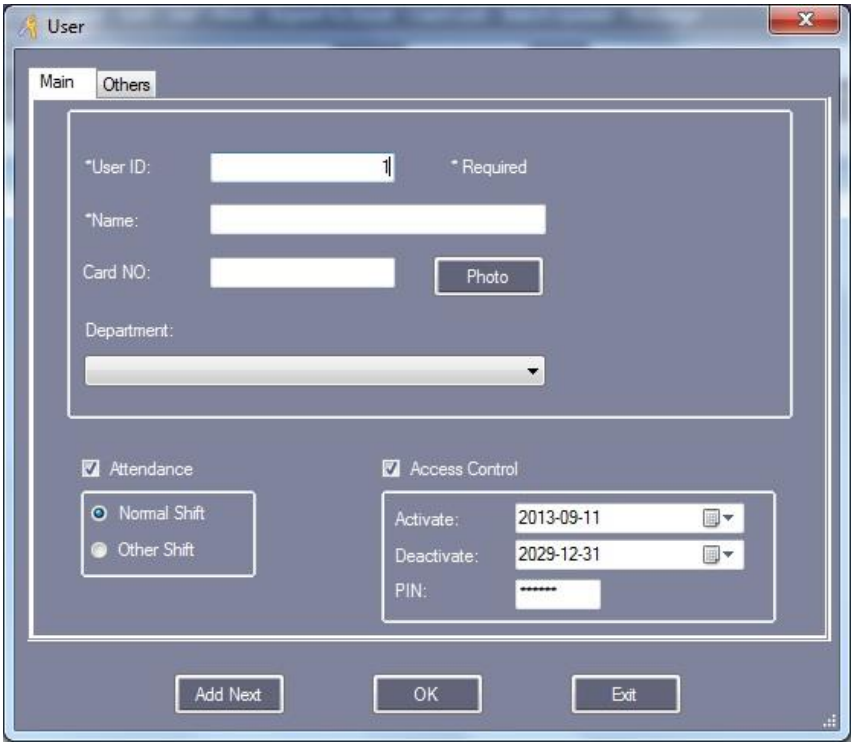


Figure 25 - Add User Dialog

Editing User Information

To edit an existing user's information, highlight the desired user then click on the "Edit" tool.

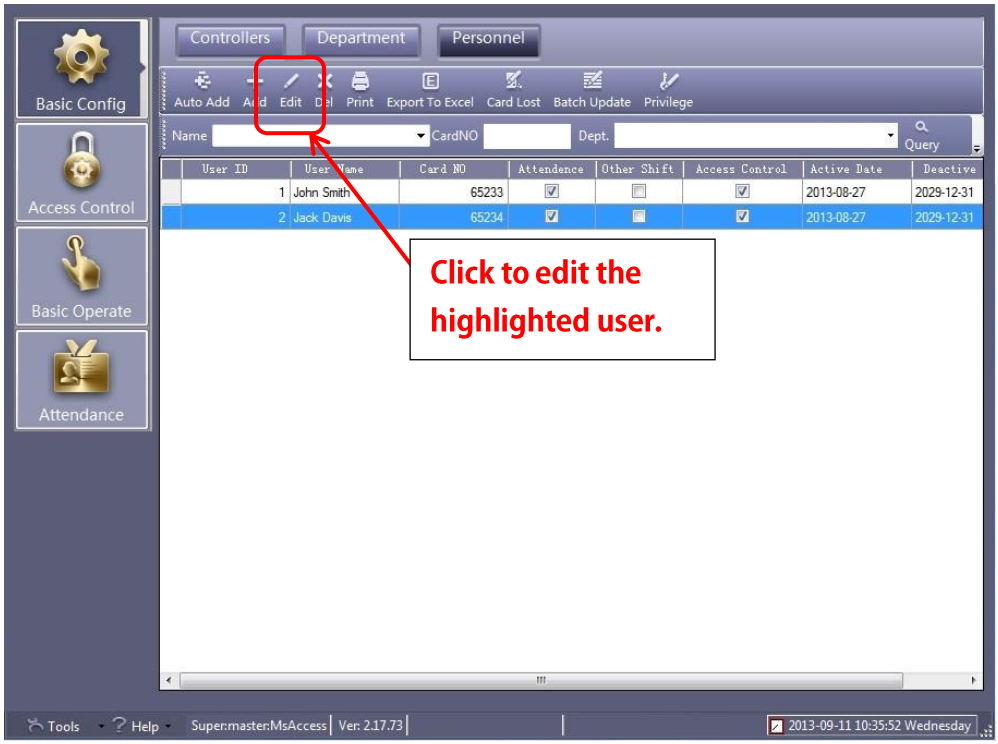


Figure 26 – Edit Tool on the Personnel Page

Figure 27 - Sample User Screen

The following information can be modified:

- The “User Number” is used by the system to uniquely identify a user. It is a simple counter. The first user entered is user number 1; the second is number 2; etc. The system will generate this number automatically. **Do not modify this number.**
- The “Name” field allows you to insert the name of the card holder.
- The “Card NO” field is the card number assigned to this user. It is usually located on the front of the card. If site codes are being used at your site, prepend the site code to the card number. For example, if the site code is 156 and the card number 65532, enter 15665532 in this field.
- The “Department” drop down box is a list of the defined departments. Chose the one the user belongs to.
- The “Attendance” check box indicates whether the user will be included in attendance reports.
- The “Access Control” check box must be checked for this user to have access rights.
- The “Activate and Deactivate” fields are dates the user’s credentials/card will be active.

If your site uses site codes, you must include the site code as part of the Card NO. The card NO is the site code and the number on the card. Prepend the site code to the card number with no spaces. For example:

Site Code: 156
Card Number: 65532
Card NO: 15665532

After entering the card holder information, select “OK” to save the information to the database.

Alternately, you can click the “Add Next” button on the “Personnel” screen.

Auto Add

When adding personnel you can “Auto Add” cards to the system. Using “Auto Add”, you can swiftly enter cards by scanning or in bulk, making assigning cards to users simpler and faster.

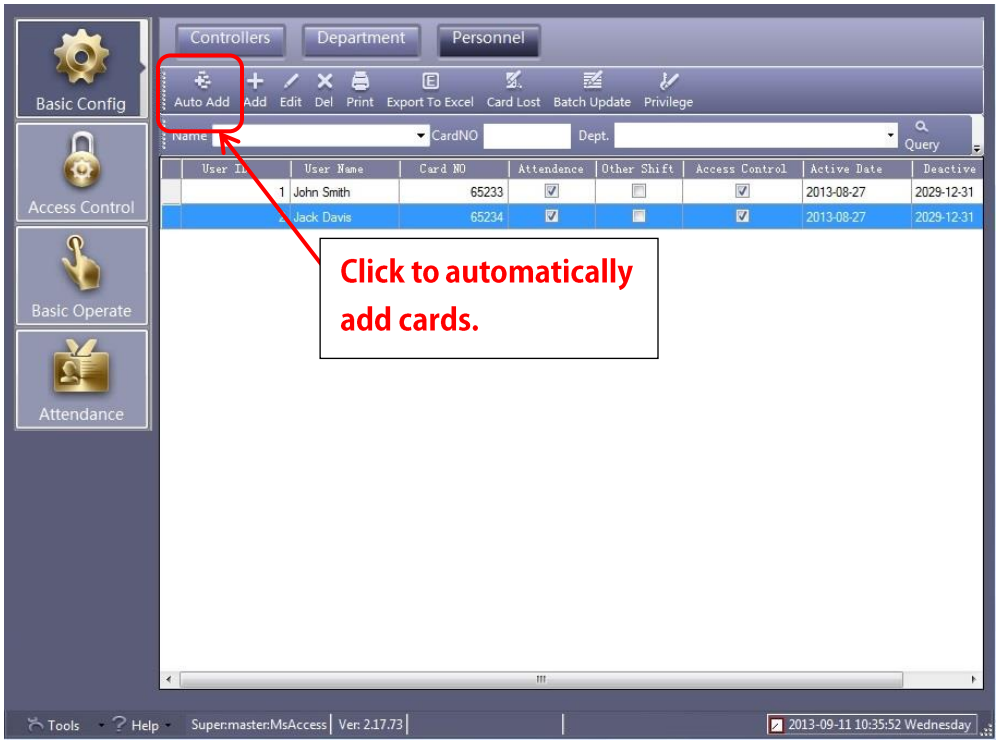


Figure 28 - Auto Add Tool on the Personnel Page

Auto adding cards to the system is done using a USB reader attached to the computer, by selecting an active door on the system or by manual batch input. After selecting “Auto Add” on the “Personnel” screen, you must click on the radio button for the desired method.

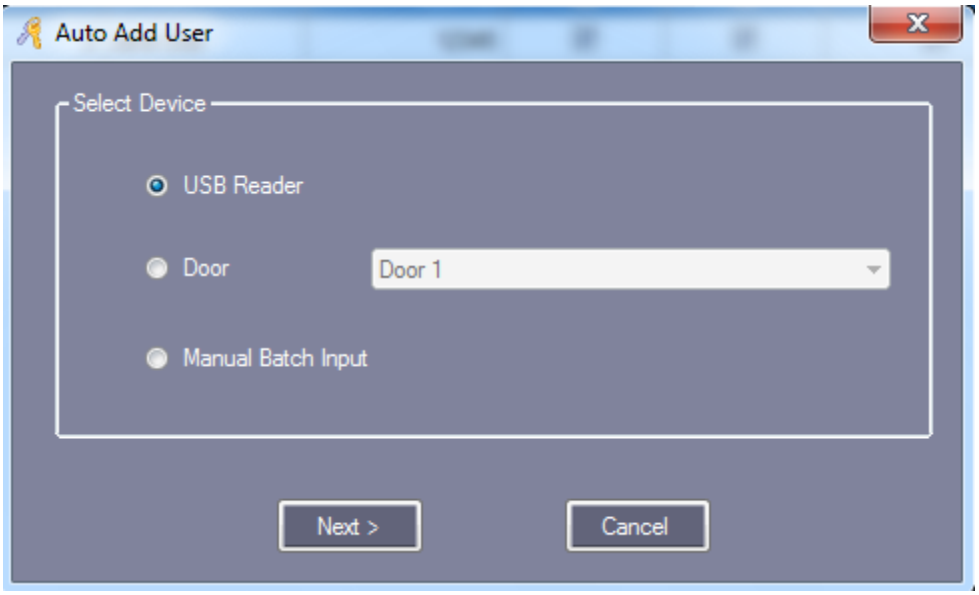


Figure 29 - Auto Add User Method Dialog

Select “Next>” when the method has been selected. The “Auto Add User” dialog for the chosen method appears.

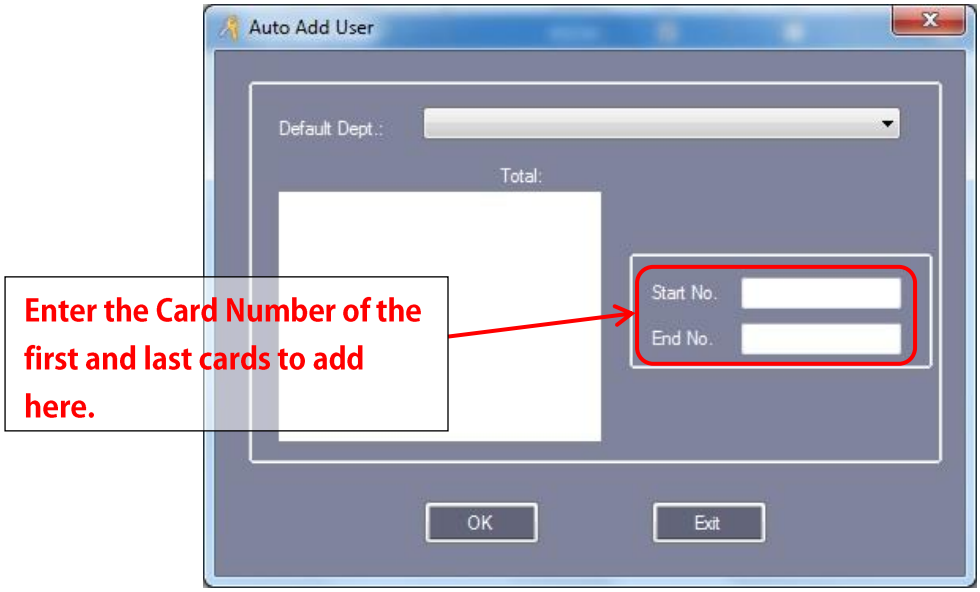


Figure 30 - Auto Add User Dialog for Manual Batch Input

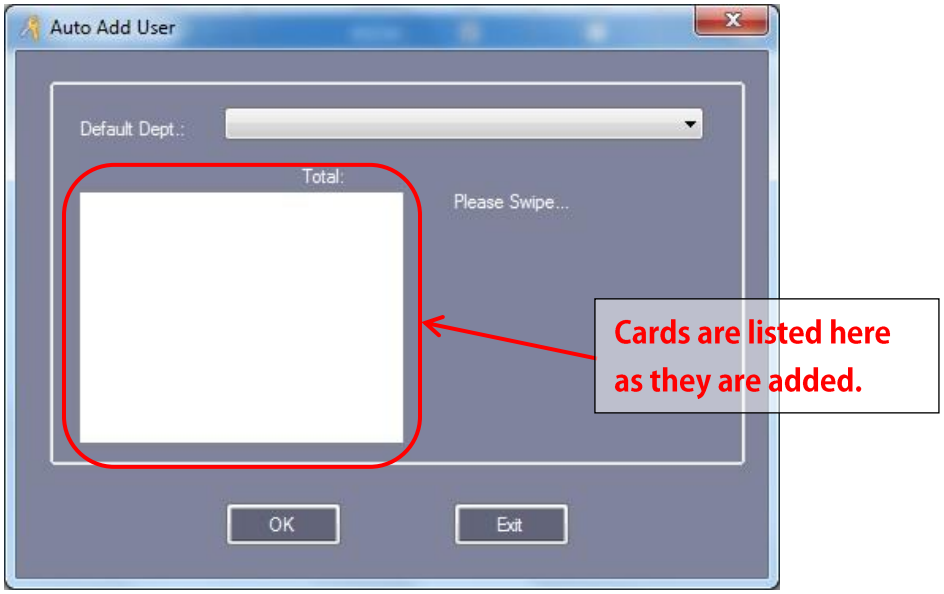
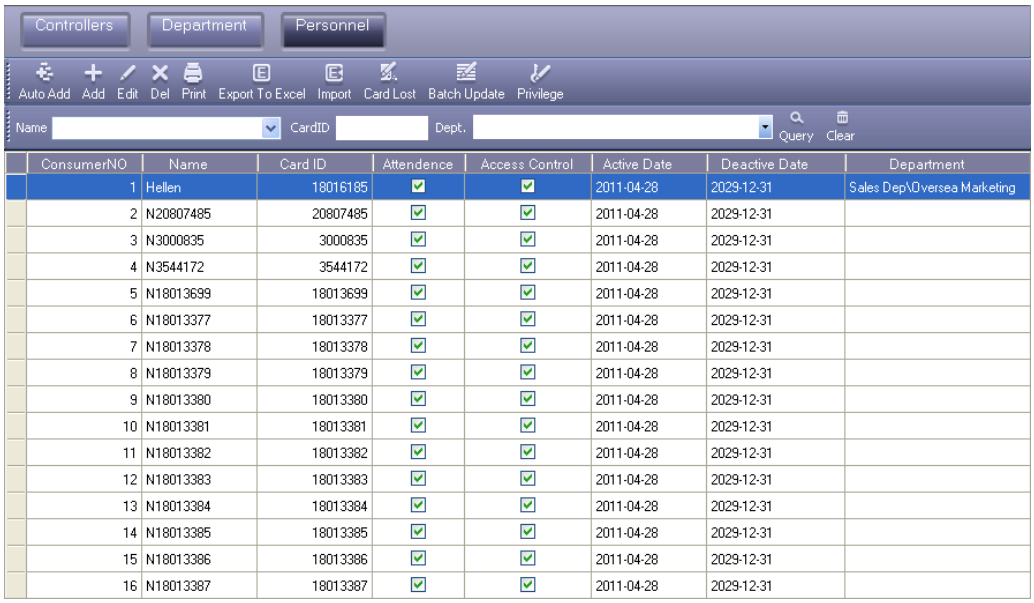


Figure 31 - Auto Add User Dialog for USB Reader and Door

If you have defined departments, a default department can be selected from the list. This will be the department for all of the cards added.

Select “OK”, after all cards have been added.

When cards are auto added the default Name is “N + ‘Card Number’”.



ConsumerNO	Name	Card ID	Attendence	Access Control	Active Date	Deactive Date	Department
1	Hellen	18016185	☑	☑	2011-04-28	2029-12-31	Sales Dep\Oversea Marketing
2	N20807485	20807485	☑	☑	2011-04-28	2029-12-31	
3	N3000835	3000835	☑	☑	2011-04-28	2029-12-31	
4	N3544172	3544172	☑	☑	2011-04-28	2029-12-31	
5	N18013699	18013699	☑	☑	2011-04-28	2029-12-31	
6	N18013377	18013377	☑	☑	2011-04-28	2029-12-31	
7	N18013378	18013378	☑	☑	2011-04-28	2029-12-31	
8	N18013379	18013379	☑	☑	2011-04-28	2029-12-31	
9	N18013380	18013380	☑	☑	2011-04-28	2029-12-31	
10	N18013381	18013381	☑	☑	2011-04-28	2029-12-31	
11	N18013382	18013382	☑	☑	2011-04-28	2029-12-31	
12	N18013383	18013383	☑	☑	2011-04-28	2029-12-31	
13	N18013384	18013384	☑	☑	2011-04-28	2029-12-31	
14	N18013385	18013385	☑	☑	2011-04-28	2029-12-31	
15	N18013386	18013386	☑	☑	2011-04-28	2029-12-31	
16	N18013387	18013387	☑	☑	2011-04-28	2029-12-31	

Figure 32 - Personnel Page with Users

Card Lost

If a user has lost his or her card, you can register the lost card, and distribute a new card with the same access privileges.

Highlight the user that has lost the card on the “Personnel” screen. Select the “Card Lost” tool on the “Personnel” Page.

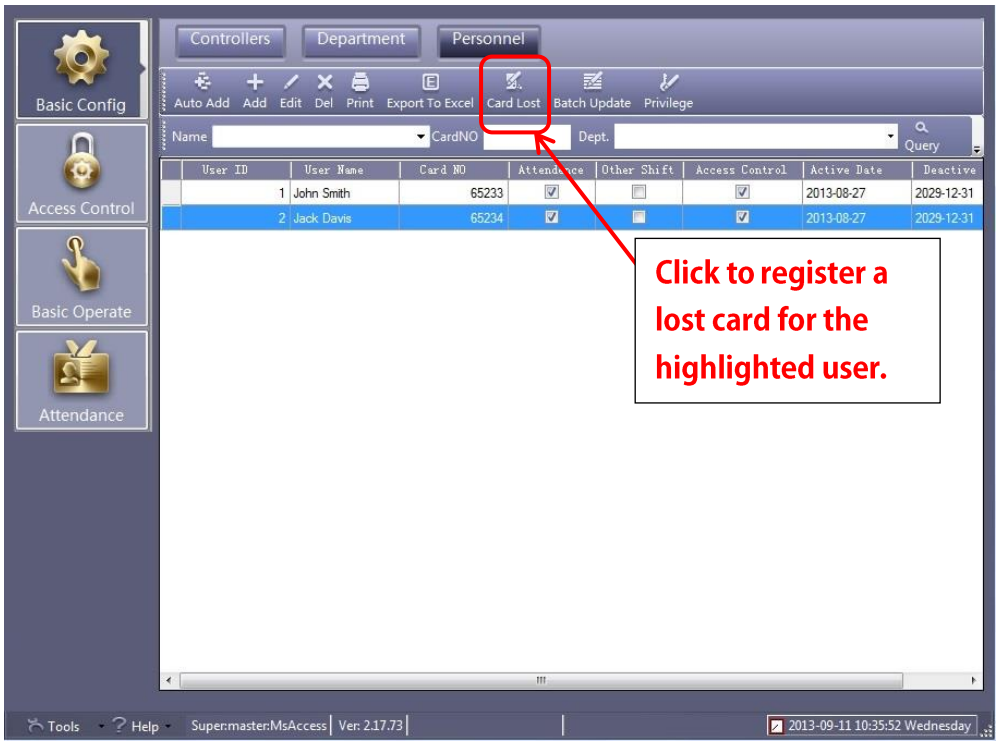


Figure 33 - Lost Card Tool on the Personnel Page

In the “Card Lost” dialog, type in the new card number. Select “OK” to save; “Exit” to quit without saving.

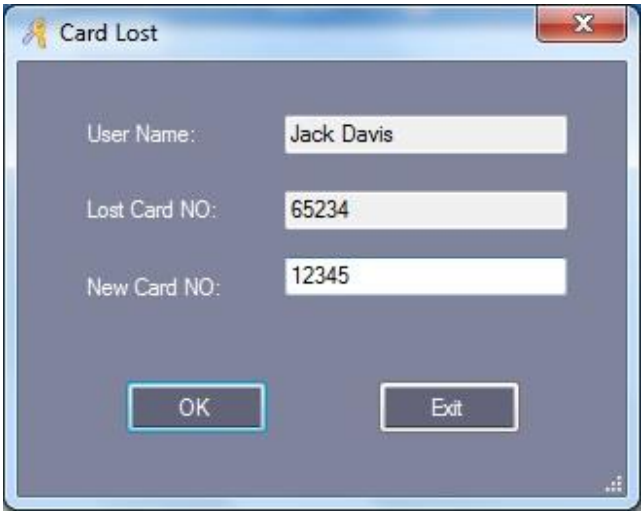


Figure 34 - Card Lost Dialog

The lost card is deactivated and the new card is activated with the same access privileges as the deactivated card.

Access Control

In **Access Control** mode, you can manage access privileges, time profiles, peripheral controls, passwords, anti-passback, inter lock, multi-card, first card open and the task list. Each of these is a button in the page header. They may not all fit in the region, but you can get to them by either right-clicking on the region to popup a context menu or click on the dropdown arrow on the right to expose the hidden buttons.

To switch to **Access Control** mode, click the “Access Control” button in the mode menu on the left.

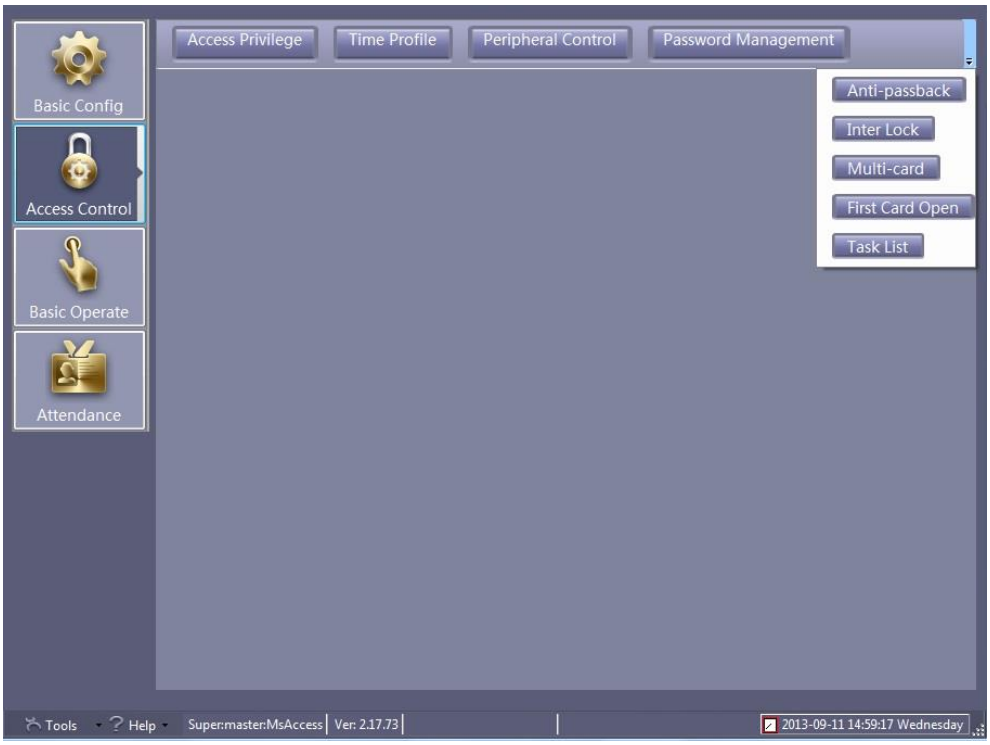


Figure 35 - Access Control Mode with All Buttons Displayed

This is where you define when and how your site will be accessed and assign that access to users.

Time Profile

A time profile is a block of time and days for which users will have access. For example, if your company’s the standard work week is Monday through Friday from 8:00 am to 5:00 pm; you should create a time profile for it. Does your company have evening hours? Weekend hours? You will need time profiles for all the time periods that define when your facilities will be accessed.

The “Time Profile” Page allows you to create time periods that will be assigned to users or groups of users to grant access to doors during these time periods.

Click the “Time Profile” button to display the “Time Profile” Page.

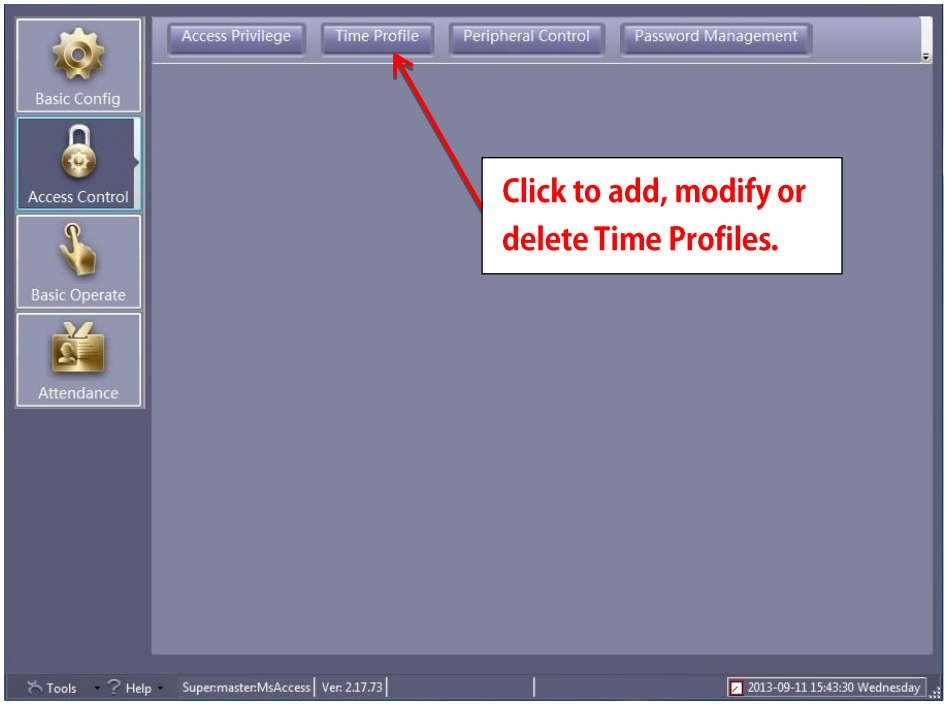


Figure 36 – Time Profile Button on Access Control Screen

Adding a Time Profile

To add a new time profile, click the “New” tool on the “Time Profile” Page toolbar.

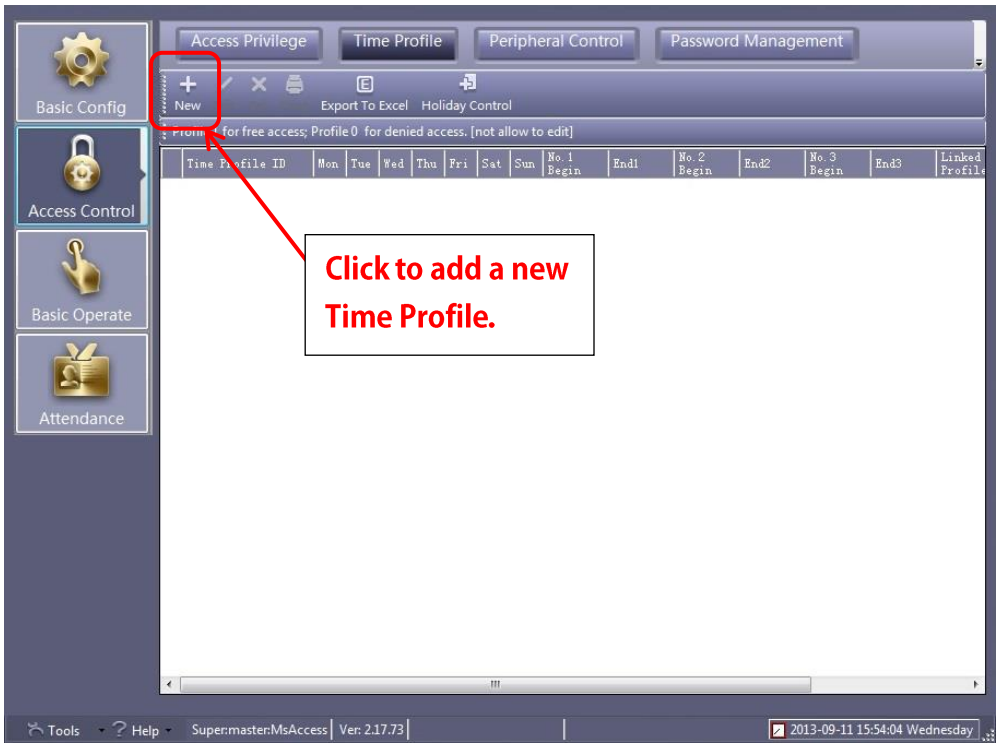


Figure 37 - Edit Tool on the Time Profile Screen

A new “Time Profile” dialog appears.

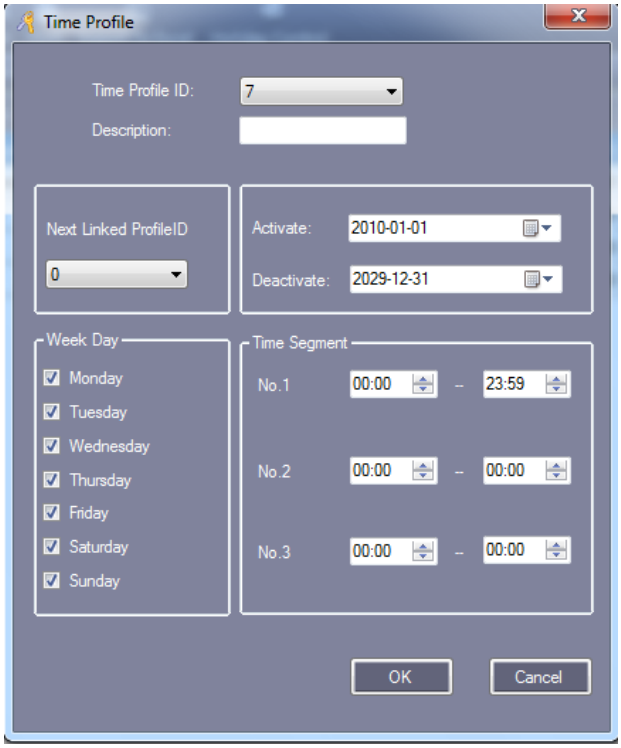


Figure 38 – Blank Time Profile Dialog

Editing a Time Profile

To edit a “Time Profile”, highlight the target profile, then click the “Edit” tool in the toolbar.

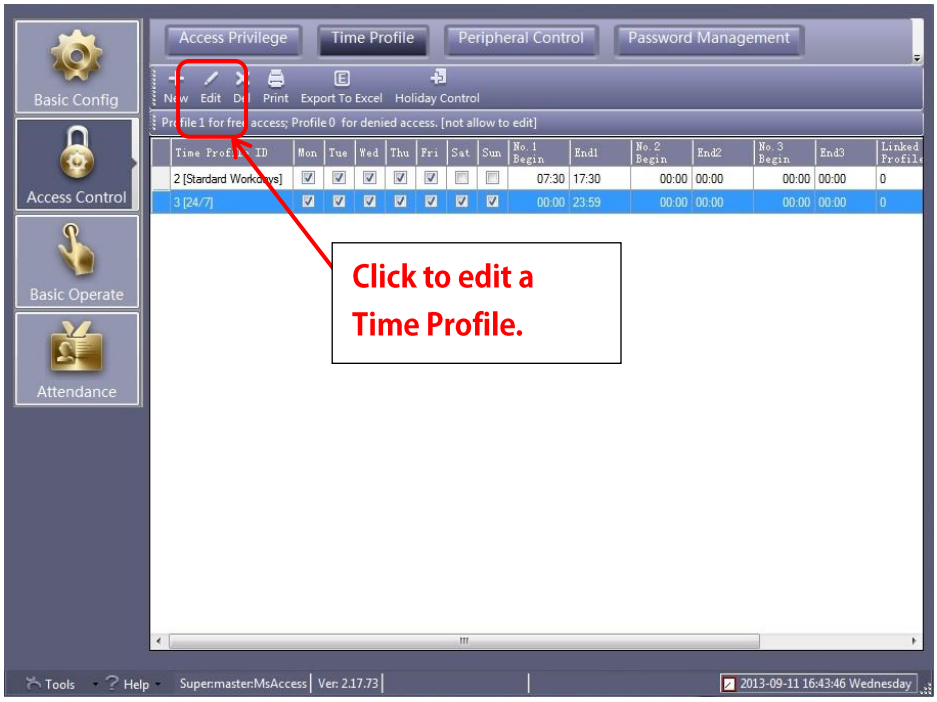


Figure 39 - Edit Tool on the Time Profile Page

The highlighted profile displays in the Time Profile dialog.

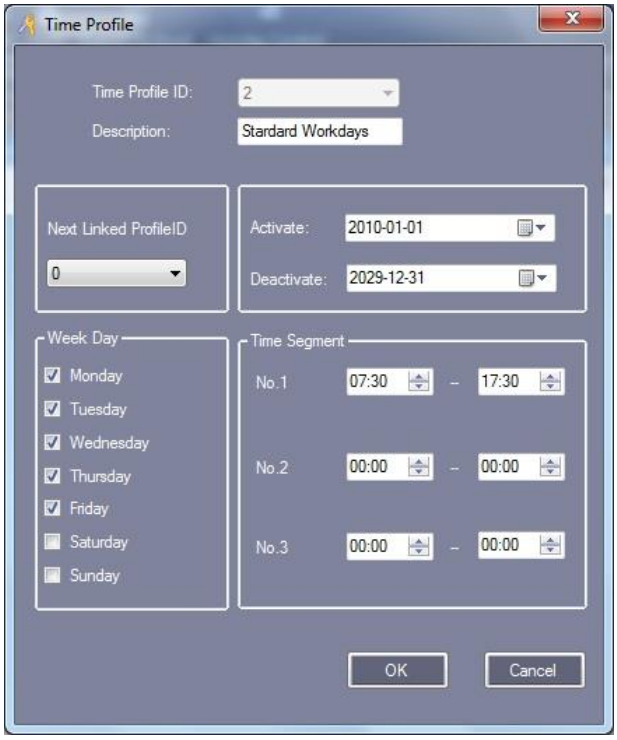


Figure 40 - Sample Time Profile Dialog

The following information can be modified:

- The “Time Profile ID” is used by the software and is automatically incremented for each profile. **Do not modify this number.**
- The “Description” box allows name for the “Time Profile” for example (Standard Workdays)
- The “Next Linked Profile ID” drop down box allows you to link more than one profile together if there is a need for more than 3 time segments within a “Time Profile”
- The “Activate and Deactivate” box specifies the dates this “Time Profile” is active.
- The “Week Day” group allows you to choose the days of the week that the “Time Profile” is active.
- The “Time Segment” box allows you to create segments of time that the “Time Profile” is active.

Click “OK” to save the “Time Profile”; click “Cancel” to leave without saving.

Access Privilege

Access privileges are how you link time profiles, doors and cards. On the “Access Control” Screen select “Access Privilege”.

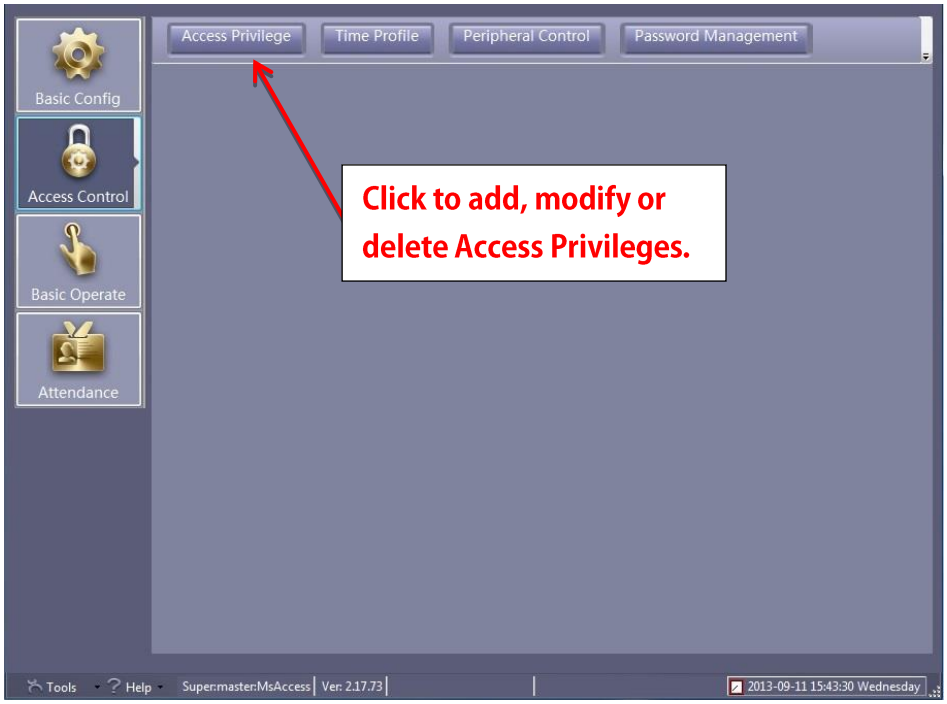


Figure 41 – Access Privilege Button on the Access Control Screen

Change Privileges

To add an access privilege, click the “Change Privileges” tool.

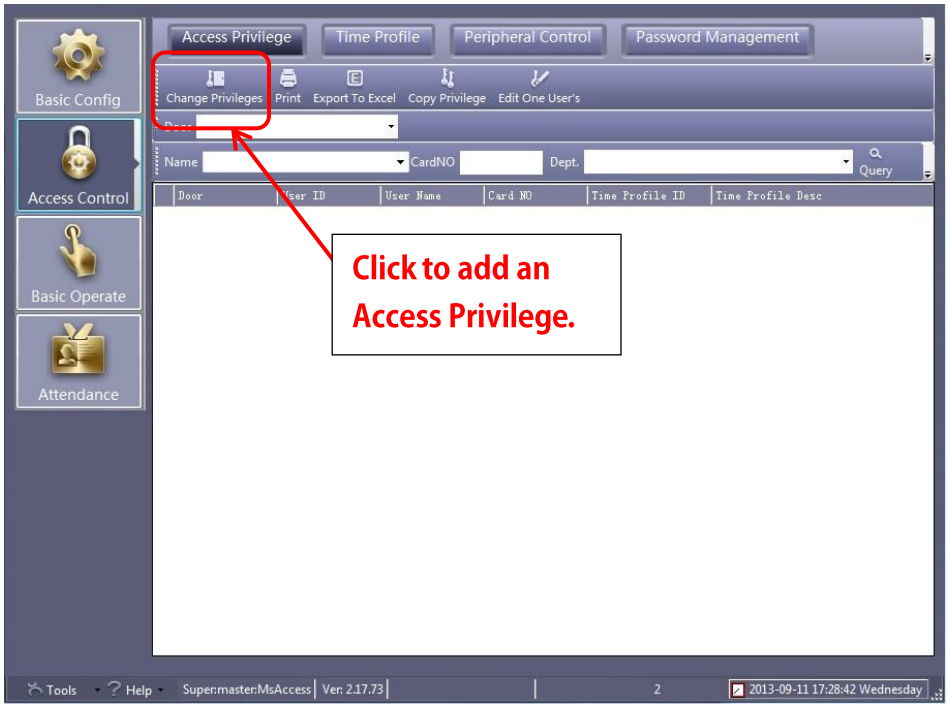


Figure 42 – Change Privileges Tool on the Access Privilege Page

Clicking on the “Change Privileges” tool brings up the “Access Privileges Assignment” dialog.

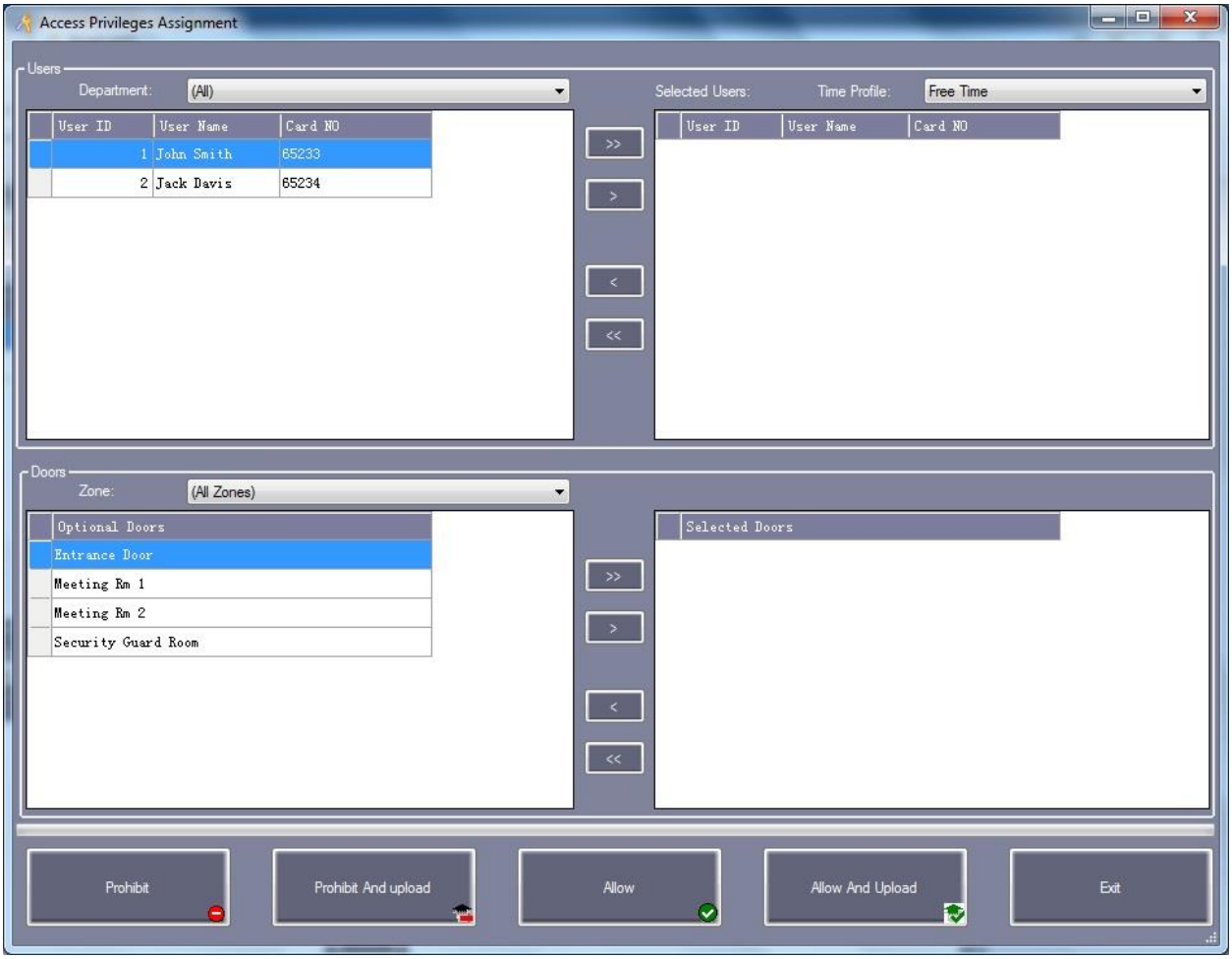


Figure 43 - Access Privileges Assignment Dialog

For each access privilege you most specify at least one user and one door. To save the access privilege click on either of the “Allow” buttons or the “Prohibit” buttons as appropriate for the privilege. The “…And Upload” buttons save the privilege and send it to the controllers.

For the most part, the “Prohibit” buttons will rarely be used. By default, a door will deny access to any card unless it has been granted permission by an access privilege. The only time a specific prohibition is needed would be if a user is part of a group that has access privilege but the user himself shouldn’t. We will assume that all access privileges we write from here on out are to allow access.

The “Department” drop down menu allows you to select users by a particular department. After selecting a particular “Department” the users that are in that department will populate the “Users” box.

In the “Users” list box, highlight the user or users. Click 

and move them to the “Selected Users” list box to the right. To move all of the users, click 

. To remove a user from the “Selected Users” list box, click 

. The highlighted user will be moved back to the “Users” list box on the left. To move all of the users out of the “Selected Users” list box click 

.

From the “Time Profile” drop down menu select the desired time profile. During this time profile

the users will be allowed access.

The “Doors” list box lists all of the available doors on the system. These are the doors that are marked “Active”. You can select any combination of doors and move them to the “Selected Doors” list box to the right similarly to moving users to the “Selected Users” list box. This will give the selected users the ability to pass through the selected doors during the specified time established by the selected “Time Profile”.

Click “Allow and Upload” to save the defined access privilege and upload it to the controllers for the selected doors. Clicking “Allow” will save the access privilege, but won’t send it to the controllers. Only use this button if there are many access privileges to add or modify to limit the number of times upload is performed. See the **Basic Operate** chapter to upload access privileges.

Viewing Access Privileges

To view access privileges, you must query the database using the query toolbars.

Figure 44 - Database Query Toolbars

To see all of the defined access privileges leave all of the fields blank and click “Query”. You can search the database by Door, Name, CardNO, or Department in any and all combinations.

Peripheral Control

Peripheral Control is where alarms are specified per controller as well as set up the hardware configuration for optional external boards with four extra relays. In addition, a threat code can be set up and assigned to a controller.

Click the “Peripheral Control” button on the Access Control screen.

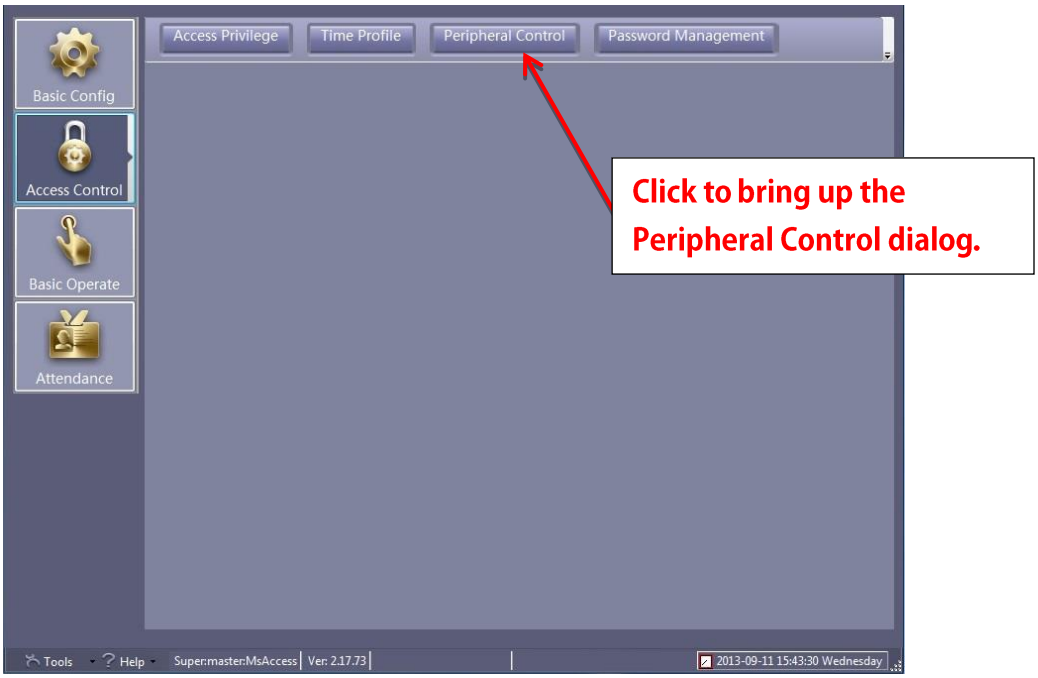


Figure 45 - Peripheral Control Button on the Access Control Screen

The “Peripheral Control” dialog appears. It displays all of the defined controllers.

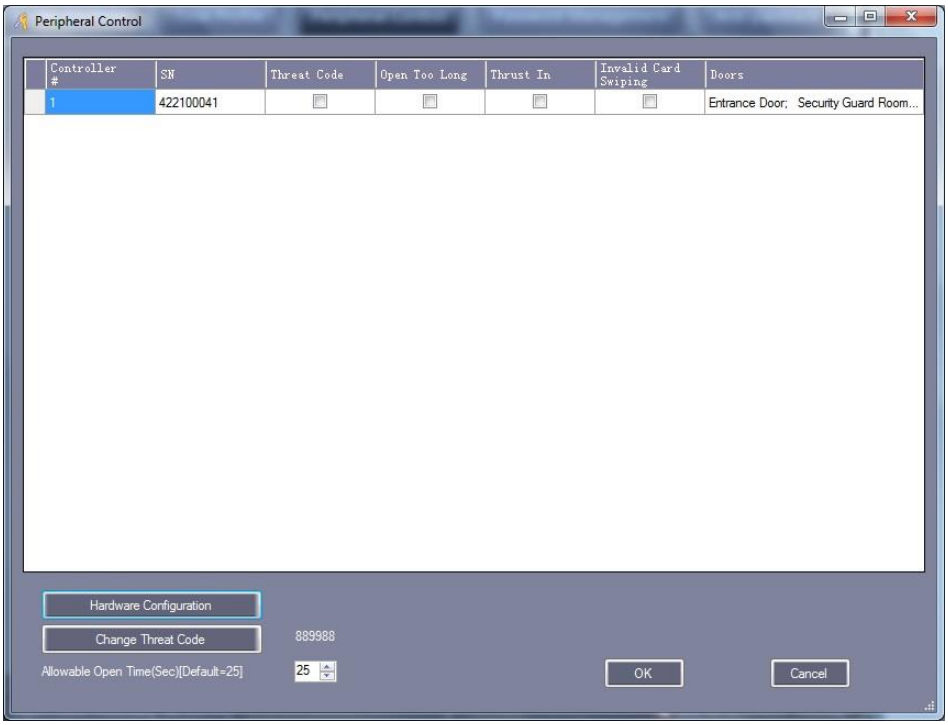


Figure 46 - Peripheral Control Dialog

Alarms

There are three alarm conditions that ReadyAXS reports. Those alarm conditions are “Open Too Long”, “Thrust In” (a.k.a. “Door Forced”), and “Invalid Card Swiping”. On a controller by controller basis, you decide which alarms, if any, will be reported by the controller. When an alarm occurs, it will appear on screen when ReadyAXS is in “Monitor Mode”. See **Basic Operate** for more information on “Monitor Mode”.

To activate an alarm simply click on the check box under the corresponding header for the controller. When you are done, upload the changes to the controllers. See **Basic Operate** for more information on uploading.

"Open Too Long" Alarm

The "Open Too Long" alarm means the door was open longer than the allowable time. The default allowable time is 25 seconds. To change the duration, modify the "Allowable Open Time" number in the lower left portion of the "Peripheral Control" dialog. This is a global number.

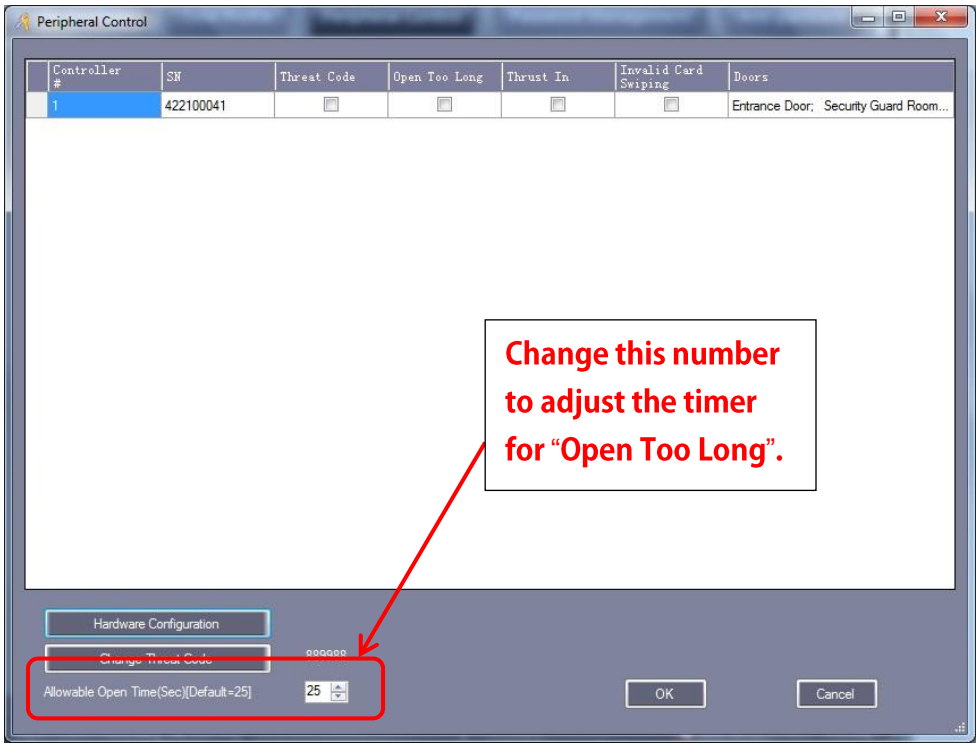


Figure 47 - Allowable Open Time Highlighted on the Peripheral Control Dialog

"Thrust In" Alarm

When a door is forced open, the "Thrust In" alarm is triggered.

"Invalid Card Swiping"

The "Invalid Card Swiping" alarm is triggered when an invalid card is used.

Hardware Configuration

For each controller, there may be up to four external boards or terminal blocks. *This is optional equipment.*

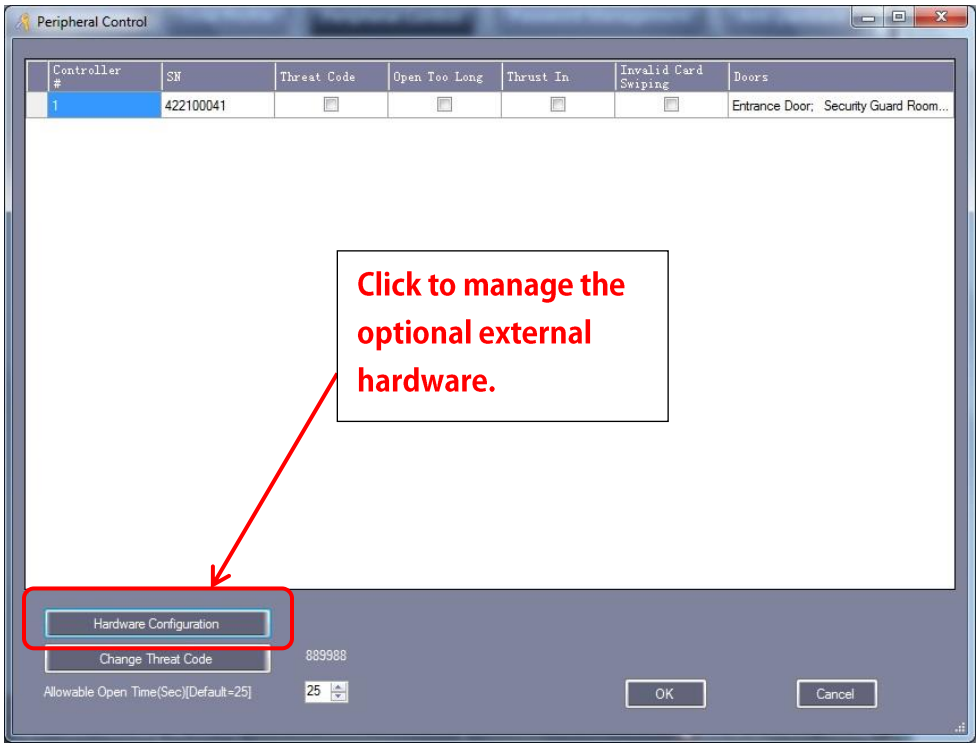


Figure 48 - Hardware Configuration Button on the Peripheral Control Dialog

Highlight the controller then click the “Hardware Configuration” button to bring up the Peripheral Control Board dialog for that controller.

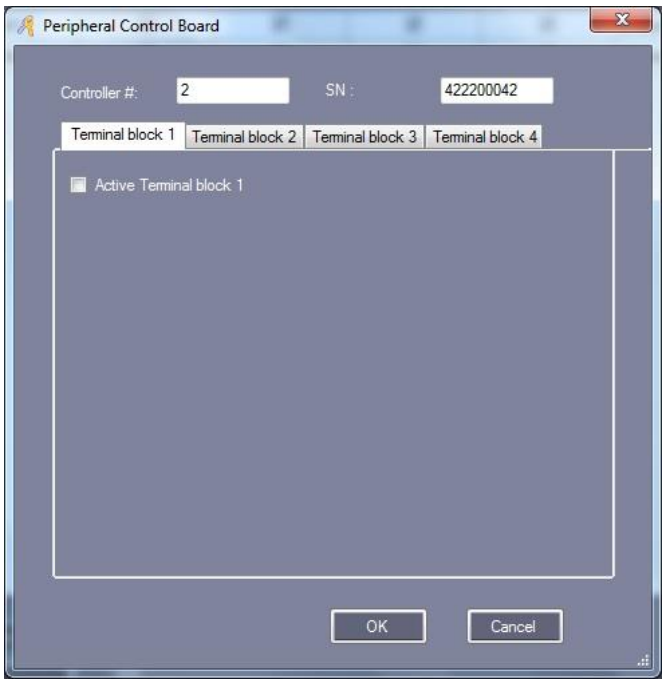


Figure 49 - Peripheral Control Board Dialog

The dialog has a tab for each external board. The tabs are labeled “Terminal block 1” for the

first board, “Terminal Block 2” for the second board and so forth. By default, all of the terminal blocks are inactive which makes senses since they are optional. To activate a terminal block, click the “Active Terminal block” checkbox.

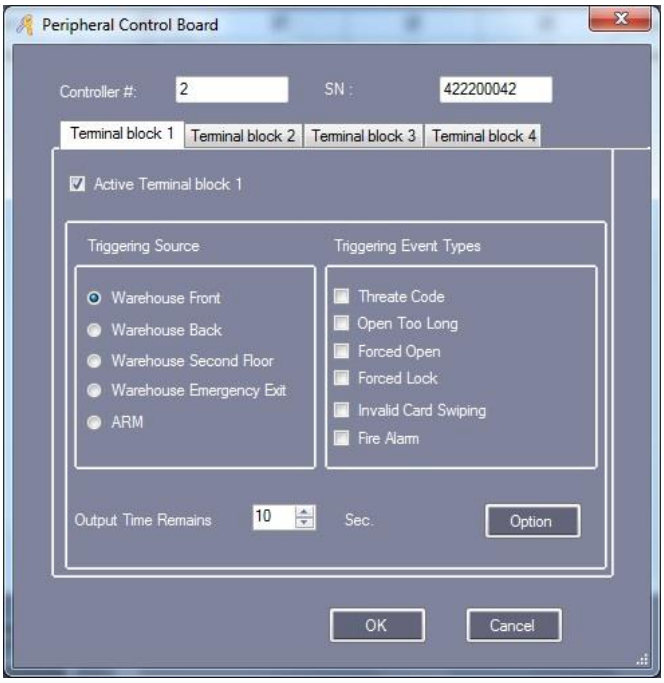


Figure 50 - Peripheral Control Board Dialog with an Active Terminal block

There are two ways to trigger the relay for a terminal block. One is on alarm and the other is on valid card read.

Trigger On Alarm

To link activating a terminal block to an alarm, you must specify the trigger source and the trigger event type(s). There can be only one trigger source but multiple trigger event types. Click the radio button next to the door that will act as the trigger source and click the checkboxes for the alarms that will serve as the trigger event types. Click “OK” to save and “Cancel” to quit.

To control how long the relay is active, click on the “Option” button.

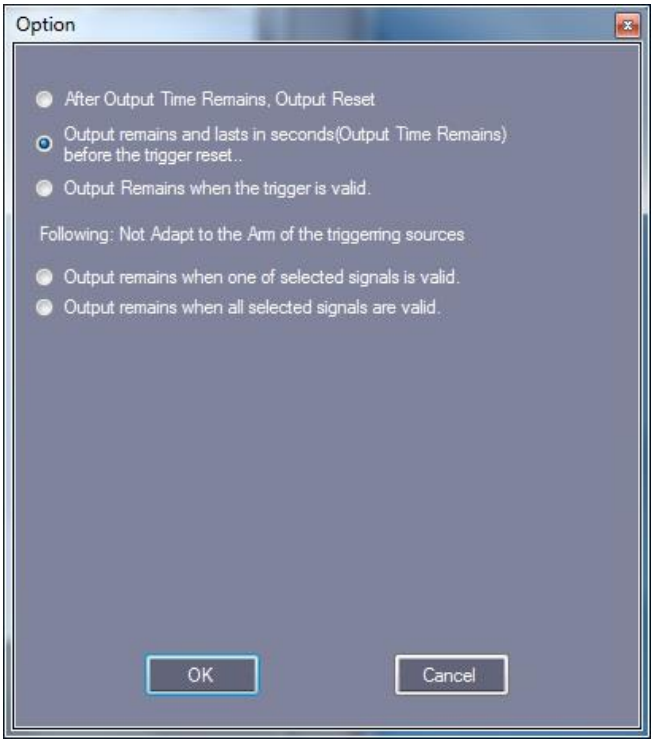


Figure 51 - Option Dialog

Select one of the top three radio buttons to set how long the terminal block is active.

- “After Output Time Remains, Output Reset” – The terminal block will remain active for the duration of the “Output Time Remains” timer defined on the “Peripheral Control Board” dialog.
- “Output remains and lasts in seconds (Output Time Remains) before the trigger reset..” – The terminal block is active for “Output Time Remains” seconds or until the trigger event resets whichever ends first.
- “Output Remains when the trigger is valid” – The terminal block is active until the trigger is reset.

For example, suppose terminal block 1 is wired to an alarm bell. And suppose terminal block 1 is triggered by “Open Too Long” and “Output Time Remains” is set to 25s. If the first option is selected, when the door that is the trigger source is “Open Too Long” the bell will ring for 25s even if the door is closed.

If option two is selected, the bell will ring for 25s or until the door is closed, whichever is shorter.

If option three is selected, the bell will ring until the door is closed.

To upload the changes, you must use the Upload button in **Base Operate** mode.

Trigger On Valid Card Read

To link activating a terminal block to a valid card read, click the “Option” button. And select either “Output remains when one of the selected signals is valid” or “Output remains when all selected signals are valid”. The list of possible signals will appear.

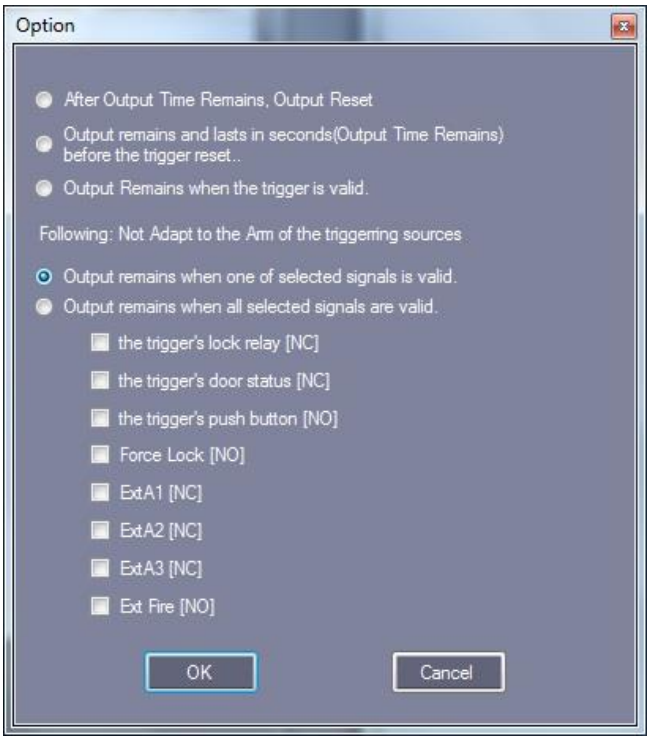


Figure 52 - Options Dialog with Signals

Select “the trigger’s lock relay”. The lock relay will fire on a valid card read. If this box is checked, then when a valid card read triggers the lock relay, the terminal block will fire as well.

To upload the changes, you must use the Upload button in **Base Operate** mode.

Password Management

A door can be opened in one of three ways:

- A valid card swipe,
- A valid card swipe with a Personal Identification Number (PIN), or
- The controller’s password

The Password Management screen is where the PINs for the users and the passwords for the controllers are defined, modified, enabled, and disabled.

On the Access Control screen, click the “Password Management” button to bring up the Password Management dialog.

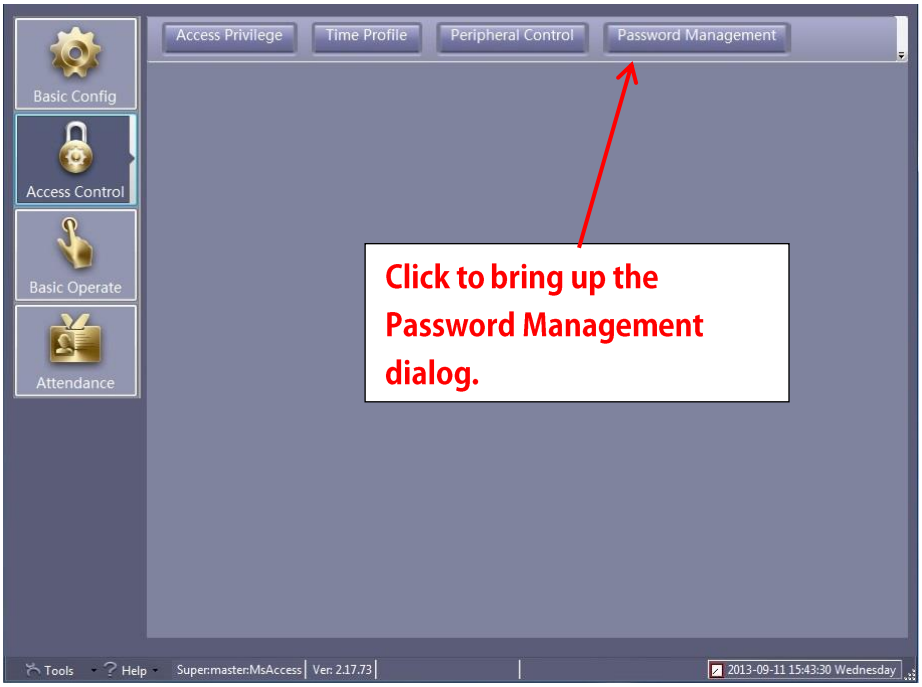


Figure 53 - Password Management Button on the Access Control Screen

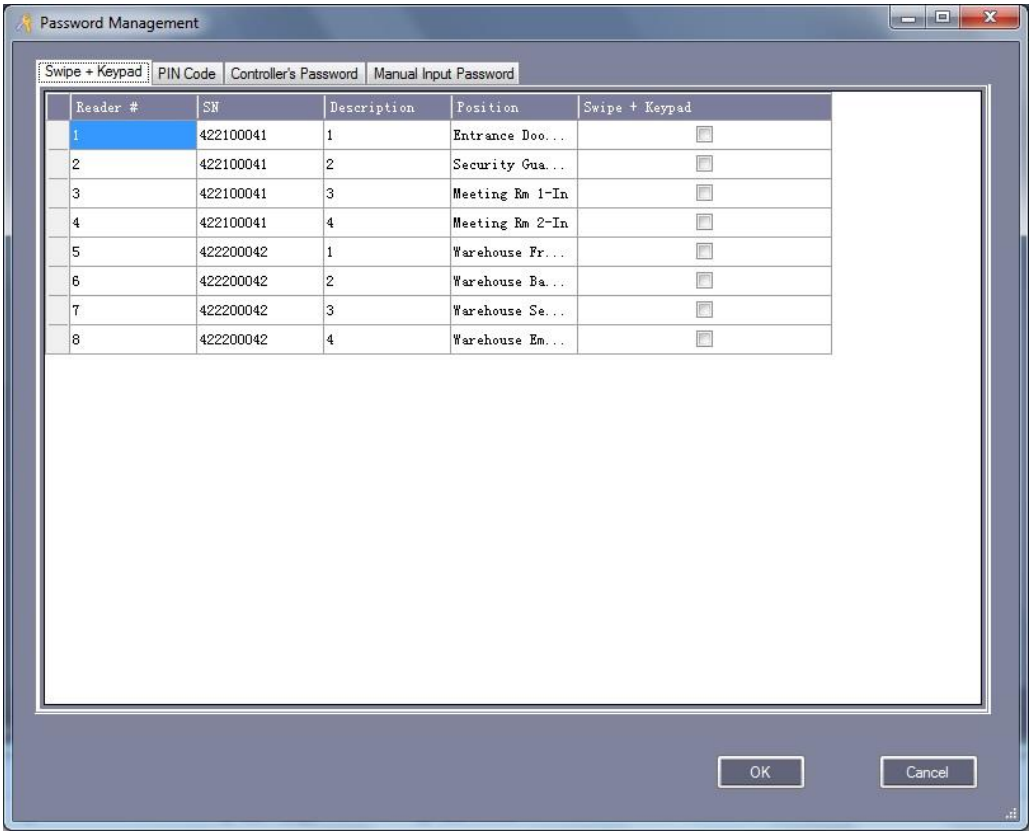


Figure 54 – Swipe+Keypad Tab of the Password Management Dialog

There are several tabs on this dialog.

- Swipe+Keypad – define which readers require swipe and keypads
- PIN Code – enter the PIN codes for users here
- Controller's Password – enter the controller's passwords here
- Manual Input Password – define which readers can accept the manual entry of the card in lieu of a card swipe ***NOT RECOMMENDED***

Swipe+Keypad tab

This tab lists every active reader in your system. For those readers where both card swipes and keypads are required, click the checkbox for "Swipe+Keypad". For a user to gain access at these doors the card must be swiped and then the PIN entered followed by the '#' key. The PIN can be any length; therefore, the '#' key demarks the end of the PIN.

To upload the changes, you must use the Upload button in **Base Operate** mode.

PIN Code tab

Click on the “PIN Code” tab to manage the PIN codes for the users.

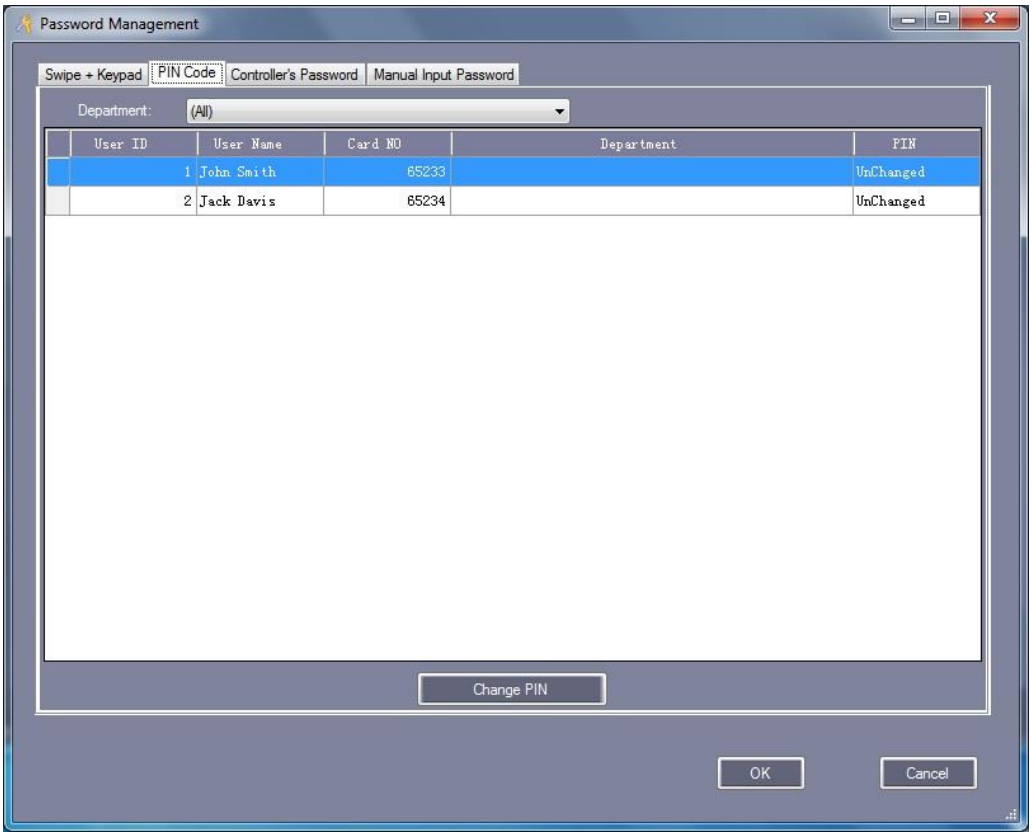


Figure 55 - PIN Code Tab of the Password Management Dialog

Locate and highlight the user then click “Change PIN”. Or you man double-click the user. Either way the “Change PIN” dialog pops up.

Figure 56 - Change PIN Dialog

Have the user type in the PIN and confirm it. The characters will be masked as they are typed. Click “OK”. The dialog will disappear and the PIN column for that user will say “*Changed*” until the next upload to the controller.

You may manage the PIN for a specific user via “Personnel” page in **Basic Config** mode.

To upload the changes, you must use the Upload button in **Base Operate** mode.

Controller's Password tab

Each door in your system can have up to 4 passwords that can be used without card swipes. Those are defined on the Controller's Password tab.

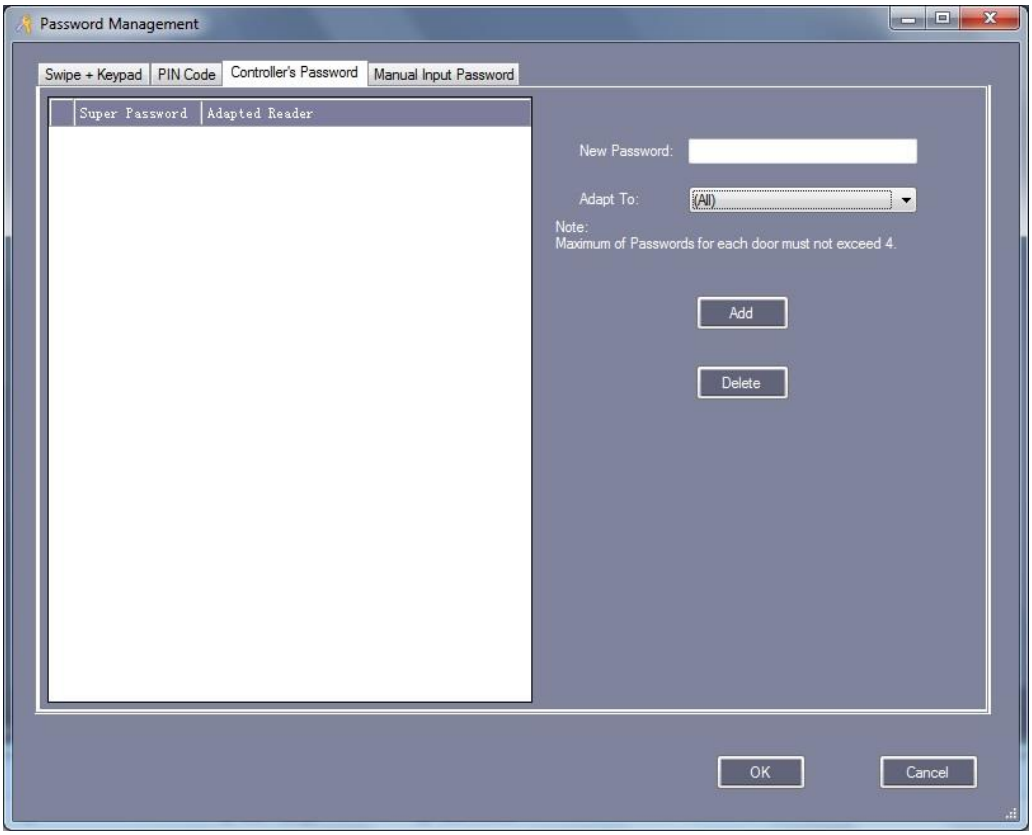


Figure 57 - Controller's Password Tab of the Password Management Dialog

Using the "Adapt To:" drop down menu, select the door to assign a password. It can be for all doors or a specific door. Type the password in the "New Password:" field. Then click the "Add" button. It will appear in the password list box to the left.

This password is called a super password because it is the password for the door independent of the user. PINs are personal, super passwords are for anyone using the door.

You can remove a password by highlighting it in the password list box then clicking "Delete".

To keep all of the changes made, click "OK". To quit without saving, click "Cancel".

To upload the changes, you must use the Upload button in **Base Operate** mode.

Manual Input Password tab

This is a work in progress. It is intended to provide a means for a user to input the card number and PIN instead of using a card swipe.

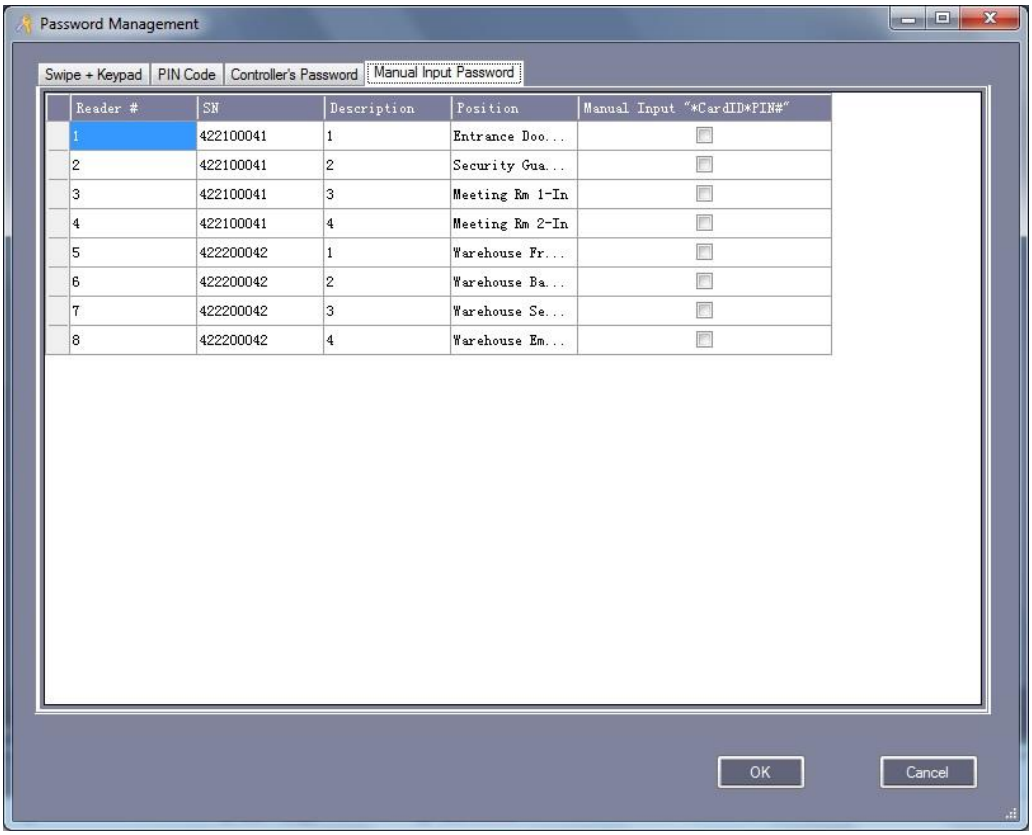


Figure 58 - Manual Input Password Tab on the Password Management Dialog

By clicking on the checkbox in the column 'Manual Input "*CardNO*PIN#"', that reader accepts manual input of the card number *and* PIN. The user enters his card number and PIN instead of swiping his card and entering his pin. The user must start the process by pressing the '*' key. Then he keys in his card number followed by the '*' key again. Then he enters his PIN followed by the '#' key.

To upload the changes, you must use the Upload button in **Base Operate** mode.

Anti-passback

Anti-passback prevents a user from swiping to gain access and then handing his card to someone else to use as well. Without this control more persons than the authorized user could access a controlled area with a single unique badge.

ReadyAXS implements anti-passback by combining readers on a controller as in or out. Once a card has been used to gain access via a controller, it cannot be used again until it has been used at a designated reader to exit the area. Readers are designated as in or out readers.

To configure anti-passback, select “Anti-passback” in **Access Control** mode. If the button is not visible, you may need to right-click on the button header to find the hidden options.

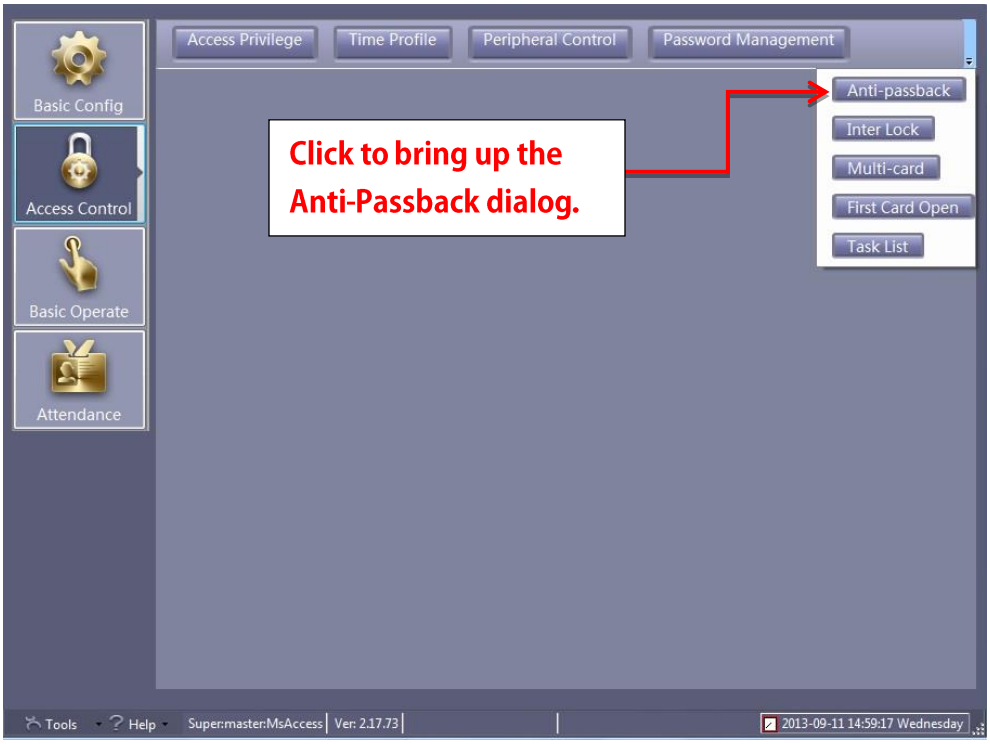


Figure 59 - Anti-Passback Button on the Access Control Screen

The “Anti-Passback” dialog lists the controllers in your system.

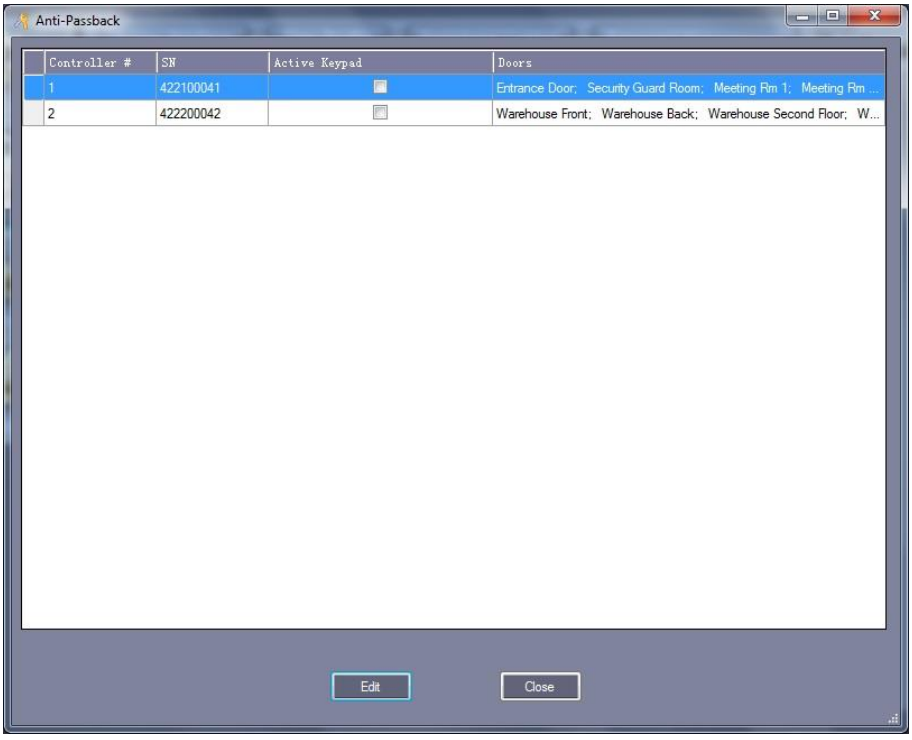


Figure 60 - Anti-Passback Dialog

Highlight a controller that will be used for anti-passback then click the “Edit” button.

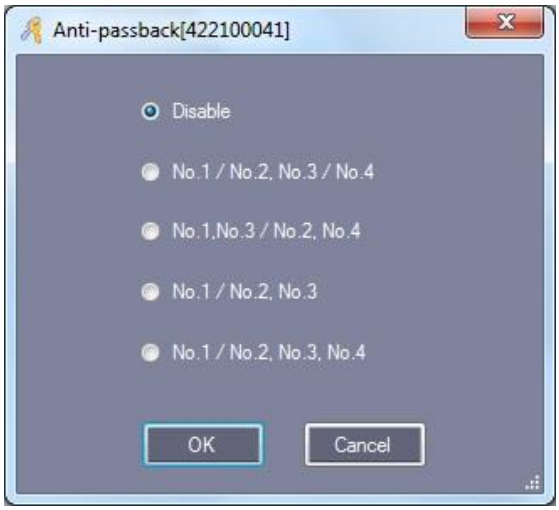


Figure 61 - Anti-passback Configuration Dialog

The radio buttons on the “Anti-passback Configuration” dialog define the possible choices for anti-passback settings.

- Disable – this controller is not performing anti-passback
- No. 1/No. 2, No. 3/No. 4 – Readers 1 and 2 are coupled with Reader 1 being the “In” reader and Reader 2 is the “Out” reader. Readers 3 and 4 are coupled where Reader 3 is the “In” reader and Reader 4 is the “Out” reader.
- No. 1, No. 3/No .2, No. 4 – Readers 1 and 3 are “In” readers. Readers 2 and 4 are “Out” readers. Once use either of the “Out” readers regardless of the “In” reader used to gain access.
- No. 1/No .2, No. 3 – Reader 1 is the “In” reader, Readers 2 and 3 are “Out” readers. Reader 4 is not included in anti-passback.
- No. 1/No. 2, No. 3, No. 4 – Reader 1 is the “In” reader, the other three are “Out” readers.

Clicking “OK” will save the changes for this controller. “Cancel” will quit without saving.

To upload the changes, you must use the Upload button in **Base Operate** mode.

ReadyAXS Anti-Passback is a hard anti-passback system. NO re-entry without a corresponding exit is permitted.

Inter Lock

Two doors are defined as interlocking when only one of the two doors can be open at a time. The second door will not open until the first door is closed even if a valid card swipe occurs.

Select the “Inter Lock” button on the **Access Control** screen. If the button is not visible, you may need to right-click on the button header to find the hidden options.

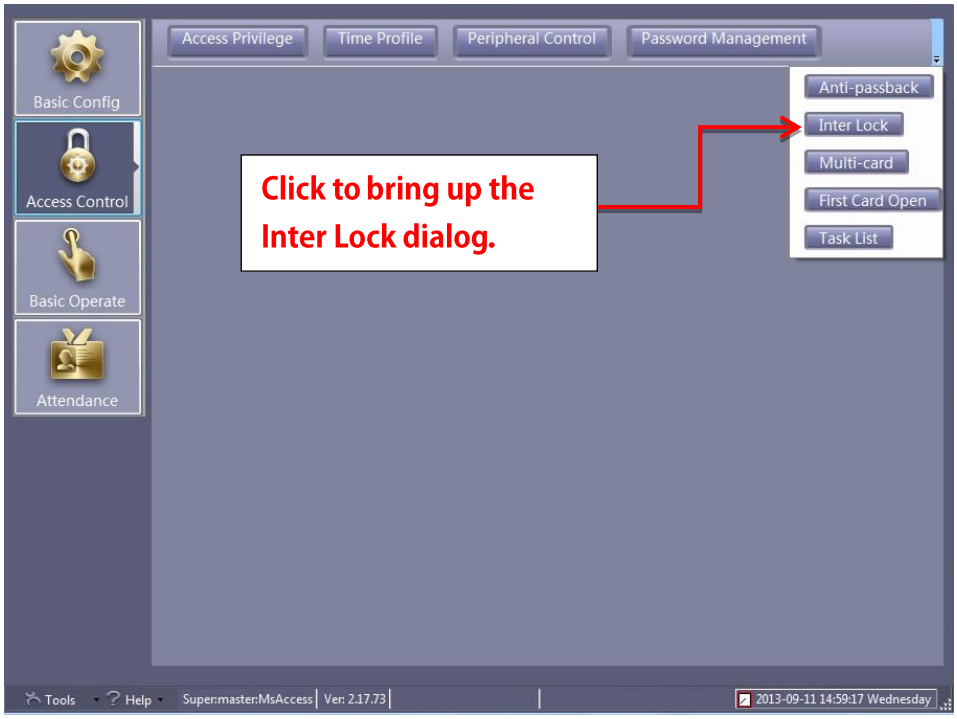


Figure 62 - Inter Lock Button on the Access Control Screen

It is important to understand that the actual interlocking occurs at the controller level. Interlock definitions cannot split across controllers. Each door involved in an interlock definition must be part of the same controller.

The “Inter Lock” dialog is where the interlocking door combinations are defined.

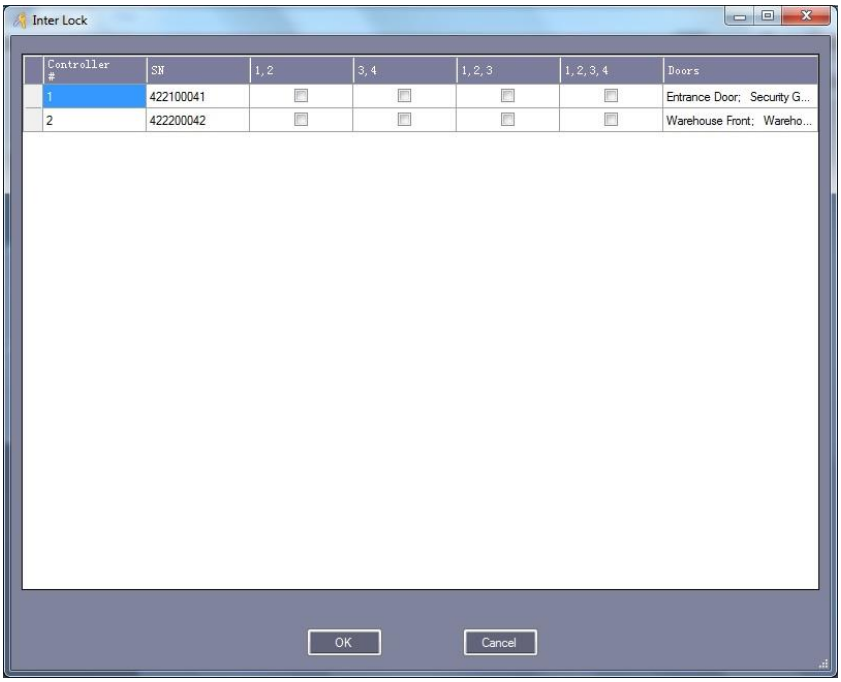


Figure 63 - Inter Lock Dialog

The inter lock options are:

- 1,2 - Doors 1 and 2 inter locked
- 3,4 - Doors 3 and 4 inter locked
- 1,2,3 - Doors 1, 2, and 3 inter locked
- 1,2,3,4 - All doors inter locked

Doors 2 and 4 cannot be inter locked together alone. Neither can doors 1 and 3. But you can have two sets of inter locking doors by selecting both [1,2] and [3,4].

Once all of the inter locks are defined, click “OK”. The definitions will be saved but not uploaded to the controllers. You must use the “Upload” button in **Base Operate** mode.

Multi-Card

Multi-Card is ReadyAXS’s implementation of the “2 Man” rule. To gain access through a controller, two or more different valid card swipes must occur before the door relay will fire. To configure Multi Card, select “Multi-card” in **Access Control** mode. If the button is not visible, you may need to right-click on the button header to find the hidden options.

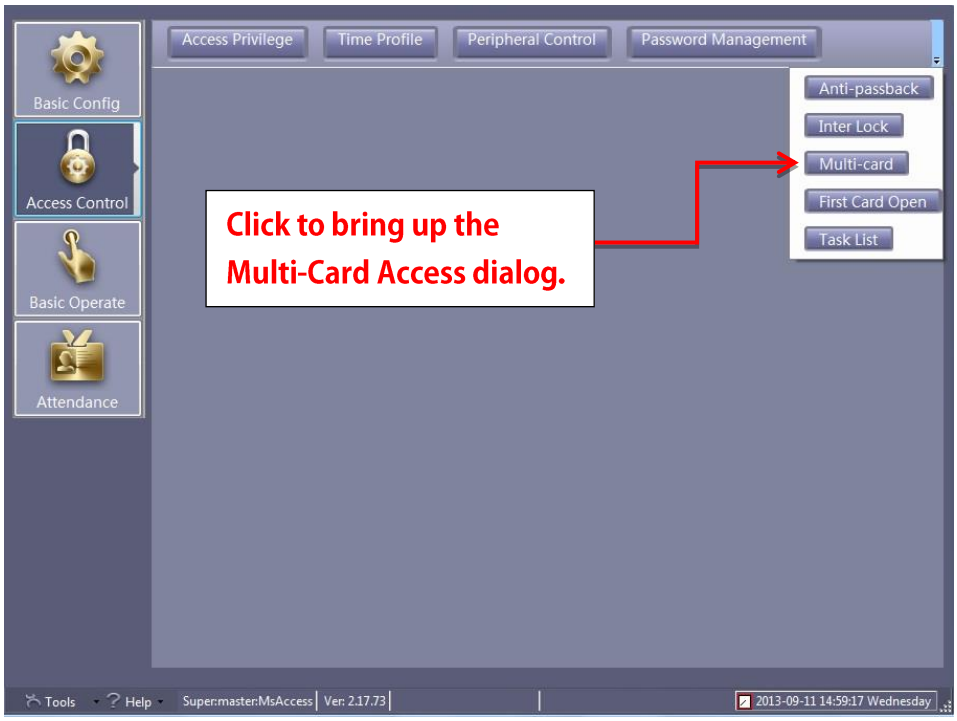


Figure 64 - Multi-card Button on the Access Control Screen

The “Multi-Card Access” dialog lists all of the doors in your system. Highlight the door that requires two or more cards for entry. Then click “Edit”.

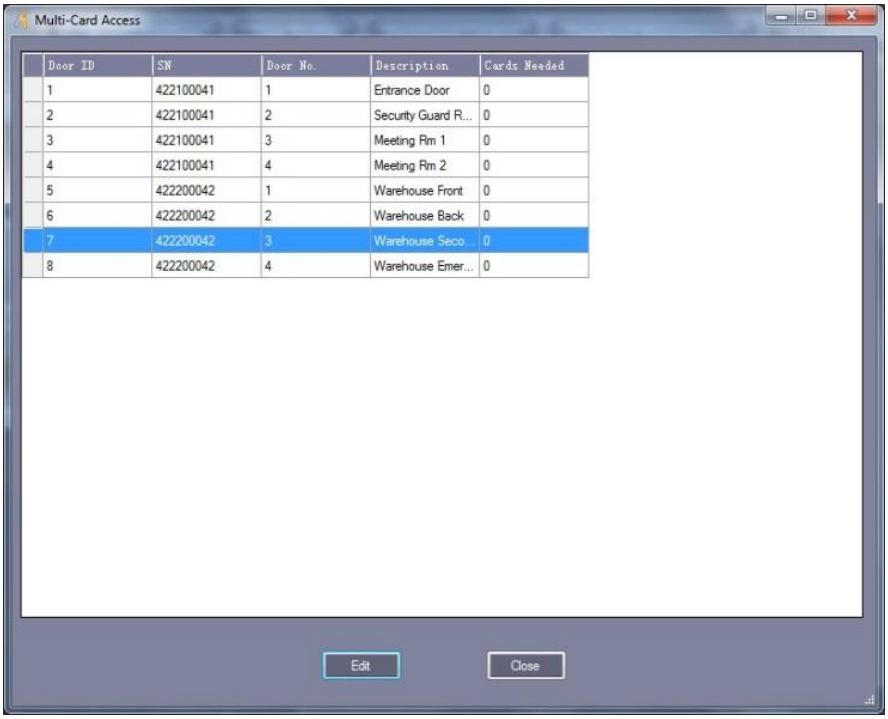


Figure 65 - Multi-Card Access Dialog

The “Multi-Card Configuration” dialog will appear. If the multi-card feature for the selected door is inactive, the “Multi-Card Configure” dialog will only have a checkbox for “Active”.

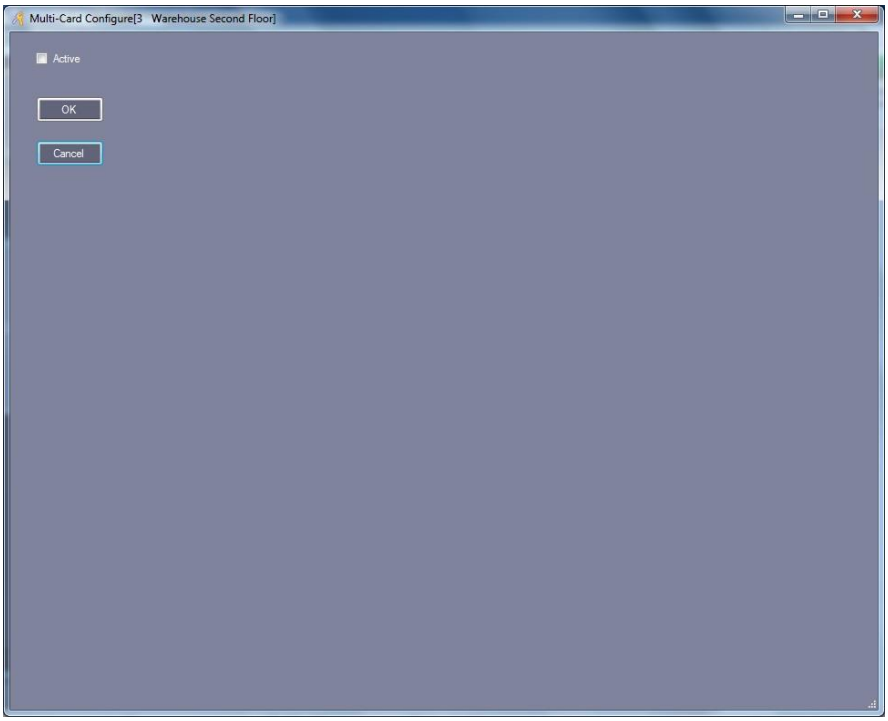


Figure 66 - Multi-Card Dialog when Multi-Card is Inactive

When the Active checkbox is checked all of the Multi-Card configuration elements display.

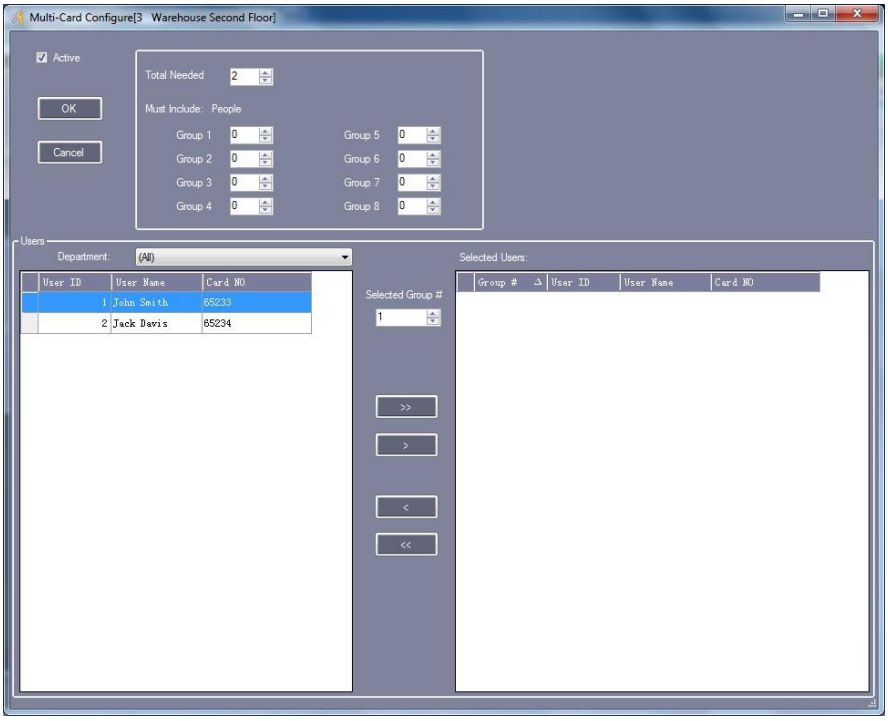


Figure 67 - Multi-Card Configuration Dialog when Active is checked

The “Total Needed” field specifies the number of different valid cards that are required to gain access. In addition, if entry requires users form different departments are present, you can enforce that by putting the users in different groups here and setting the number required from each group. The group definitions are door specific which means user ‘John Smith’ can be in group 1 for one door and in group 8 for another.

To add a user or users to a group, highlight the user(s) in the left list box, change the “Selected Group #” to the desired group number, then click  . The definition will appear in the “Selected Users:” list box on the right. Use  to move all of the users in the left list box to the right list box for the group specified.

To remove a user from a group, highlight the user in the “Selected Users:” list box and click  . To move all of the users in the “Selected Users:” list box, click  .

Once you are satisfied with the multi-card configuration, click “OK”. It will be saved. “Cancel” will exit without saving.

Close the “Multi-Card” dialog to save all of the changes.

To upload the configuration to the controllers, you must use the “Upload” button in **Base Operate** mode.

Multi-Card can be combined with Swipe+Key for added security.

First Card Open

Consider the following. The main entrance to a building is open Monday through Friday from

7:00 am to 8:00 pm. But if the door shouldn't open until there is someone there, how do you handle that? Simple, configure the door to unlock on the first valid card read.

Select the "First Card Open" button on the **Access Control** screen. If the button is not visible, you may need to right-click on the button header to find the hidden options.

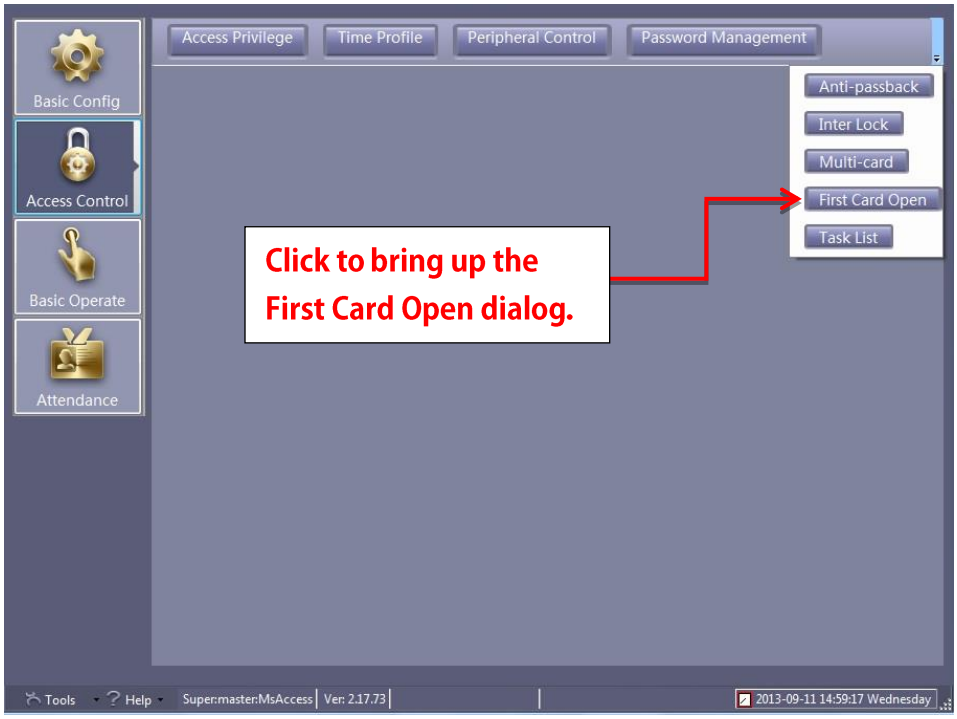


Figure 68 - First Card Open Button on the Access Control Screen

The "First Card Open" dialog appears listing all of the active doors in your system.

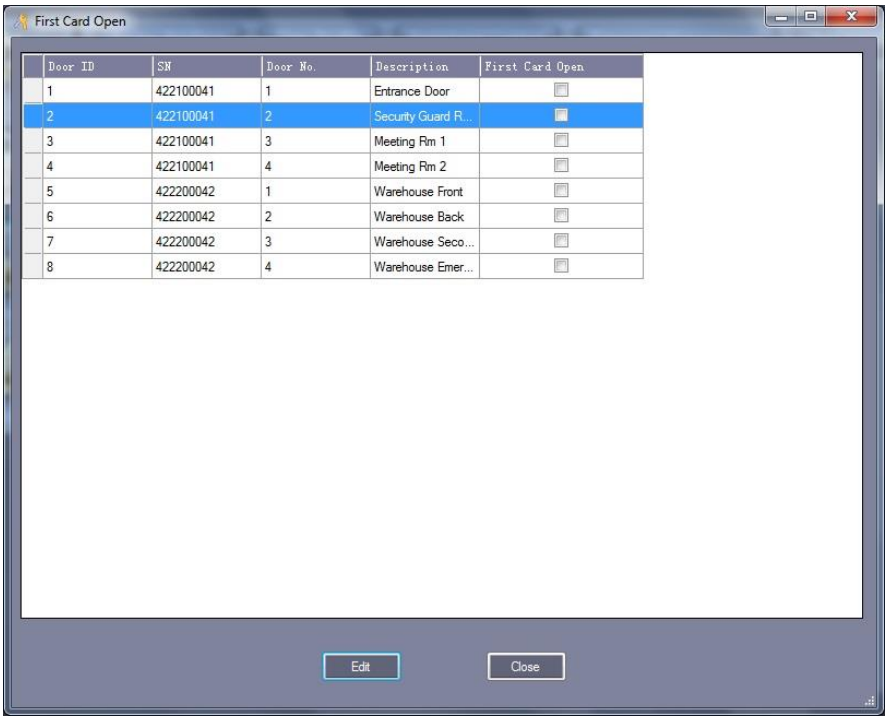


Figure 69 - First Card Open Dialog

Highlight a door to configure the “First Card Open” feature then click “Edit” at the bottom of the dialog. If the feature is not active for this door, the “First-Card Open” configuration dialog appears with only the Active field which is unchecked and the “OK” and “Cancel” buttons.

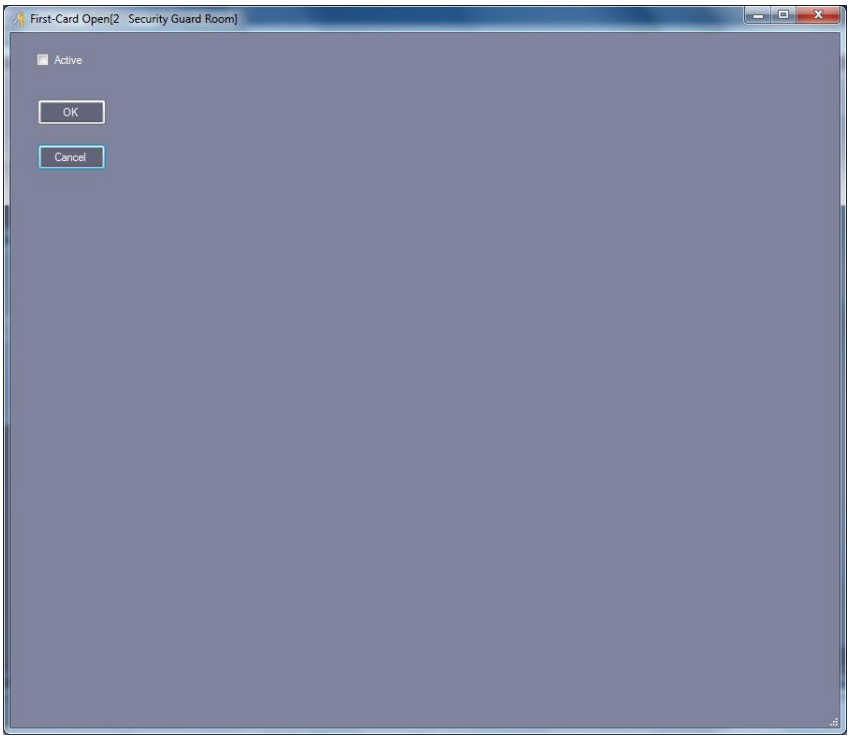


Figure 70 - First-Card Open configuration dialog when Active is unchecked

When Active is checked, the configuration options will appear.

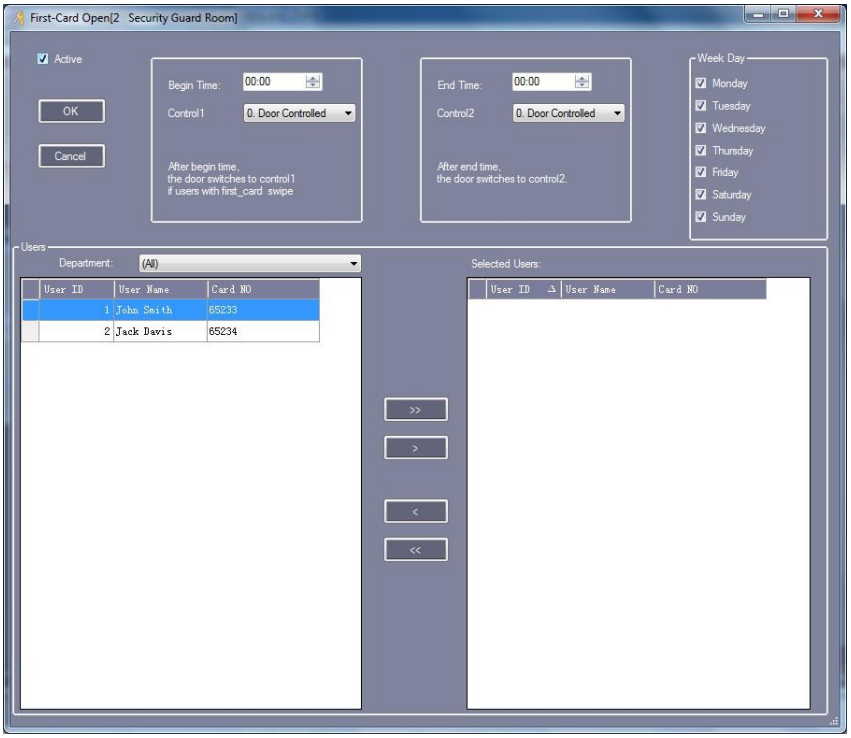


Figure 71 - First-Card Open configuration dialog when Active is checked

In the “Begin Time” field, put the start time for the “First Card” configuration. Put the end time in

the “End Time” field. All times are 24-hour times also known as military time. For example, 1:00pm is 13:00.

The Control1 and Control2 fields are drop down menus with multiple options. By selecting “Door Open” for Control1, the door will open when an appropriate card read occurs after the begin time. If “Door Closed” is selected for Control1, then the door would lock instead.

For Control2, select the option that defines the desired behavior for the door after the end time. Usually you would choose option “0:Door Controlled” so that standard behavior applies.

Check the days of the week to which this applies.

You will need to define which cards will open/close the door. This is done in the same way as all of the other User selection processes in ReadyAXS. The “Department” drop down menu allows you to select users by a particular department. After selecting a particular “Department” the users that are in that department will populate the “Users” box.

In the “Users” list box, highlight the user or users. Click 

and move them to the “Selected Users” list box to the right. To move all of the users, click 

. To remove a user from the “Selected Users” list box, click 

. The highlighted user will be moved back to the “Users” list box on the left. To move all of the users out of the “Selected Users” list box click 

.

Once you are satisfied with the First Card configuration, click “OK”. It will be saved. “Cancel” will exit without saving.

Close the “First Card Open” dialog to save all of the changes.

To upload the configuration to the controllers, you must use the “Upload” button in **Base Operate** mode.

These settings override all other settings for the door. If you need to lock a door before the “End Time” specified, you will have to deactivate the configuration by bringing up the “First Card Open” dialog and clicking on the Active checkbox to clear it and then upload it to the controller.

There is only one “First Card” setting per door which means, you cannot have a Monday - Friday configuration and a Saturday - Sunday configuration. You can only have one or the other.

All First Card Open settings go into effect immediately upon uploading to the controller. Therefore, if the upload occurs at a time in the middle of the interval specified the door will lock/unlock until a correct card read occurs.

Task List

Door operations can be scheduled using the Task List. This is where you would define all of the different normal operations for your system such as the week day schedule, the week night schedule, and the weekend schedule.

Select the “Task List” button on the **Access Control** screen. If the button is not visible, you may need to right-click on the button header to find the hidden options.

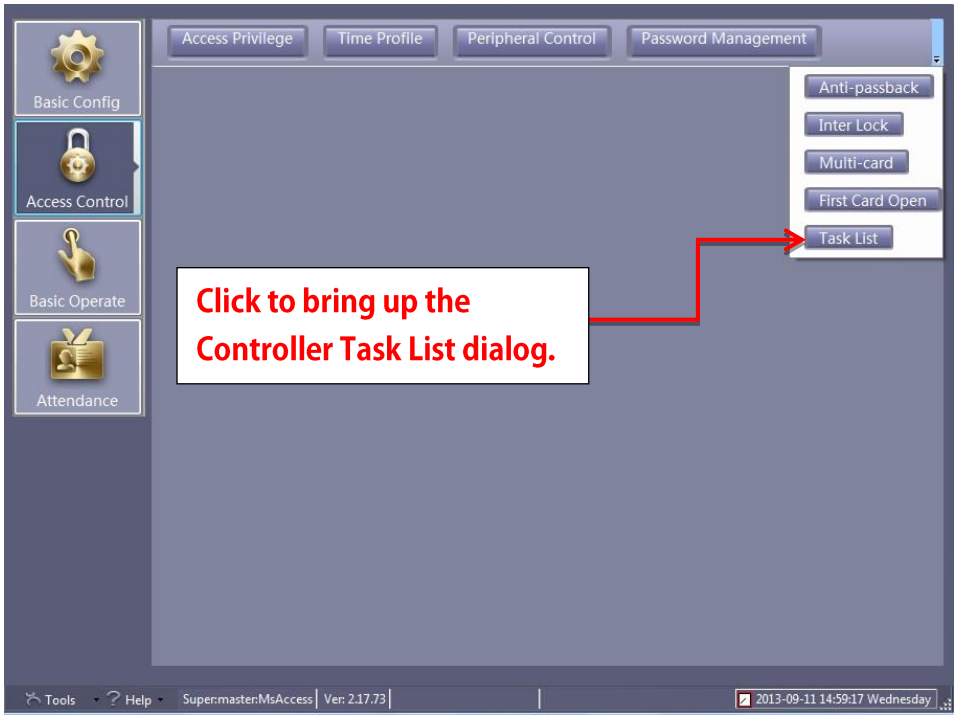


Figure 72 - Task List Button of the Access Control Screen

The “Controller Task List” dialog appears. Here you will define tasks for each controller. A task stays in effect until the next task begins.

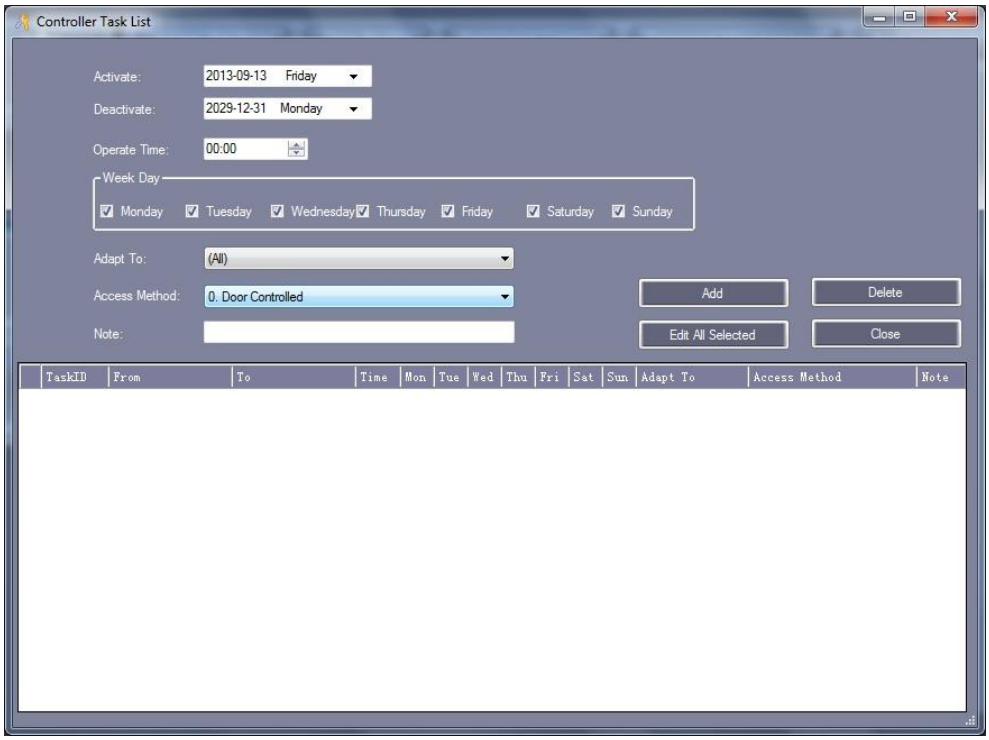


Figure 73 - Controller Task List Dialog

On this dialog, you may configure the following for each task:

- Activate – The date when this task begins
- Deactivate – The date when this task is no longer valid
- Operate Time – How long this task runs
- Week Day – The days of the week on which this task is active
- Adapt To: - Which door(s) this task affects
- Access Method
    - Door Controlled
    - Door Open
    - Door Closed
    - Disable Time Profile
    - Enable Time Profile
    - Card – NoPassword
    - (In) Card + Password
    - (In – Out) Card + Password
    - *MoreCard Disabled - unavailable*
    - *MoreCard Enable - unavailable*
    - *Trigger Once (V3.9) - unavailable*
- Note – Describe the purpose of this task

Basic Operate

Once the system is configured, **Basic Operate** mode is where you spend the majority of your time. Here you can monitor all the configured doors, upload any changes, check the status of any controller, adjust the time on a controller, download swipe records from a controller, and even discover who is currently inside your facility.

To switch to **Basic Operate** mode, click the “Basic Operate” button in the mode menu on the left.

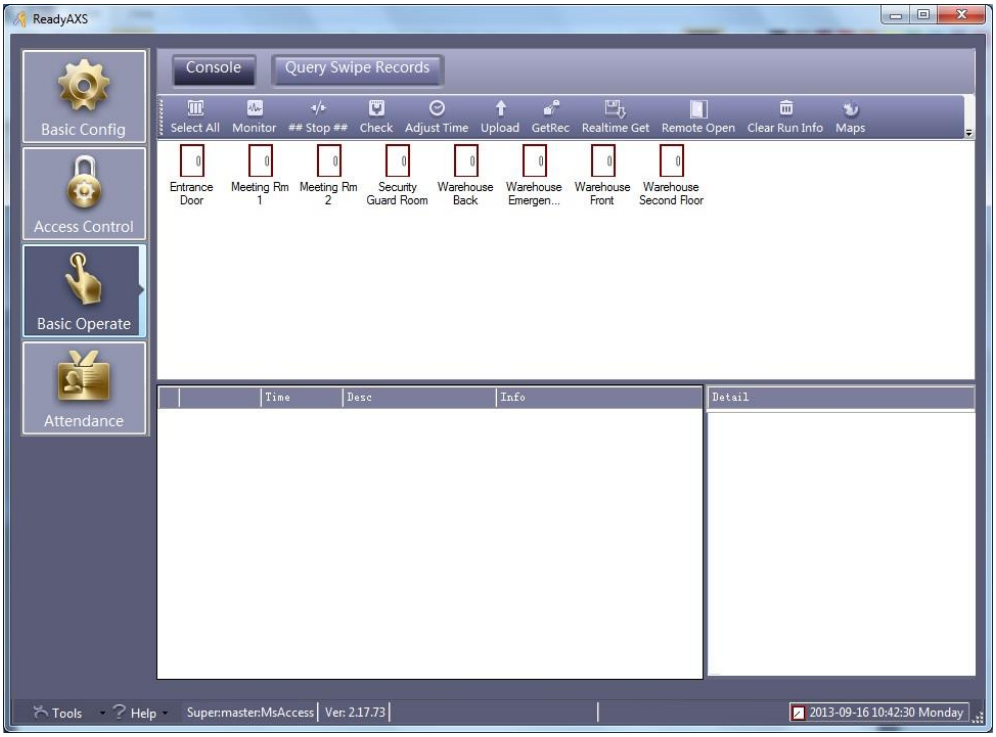


Figure 74 - Basic Operate Mode

Console

The **Basic Operate** "Console" screen displays the doors and their last known state. The console is displayed by default when entering **Basic Operate** mode. To return to the "Console" screen, click the "Console" button at the top of the screen.

Under the toolbar is the Doors display box. Here the available doors are displayed as well as their last known state. Which doors are displayed is controlled by the Zone tool.

Beneath the Doors display box are the activity list box and the Details list box. The activity list box contains all the events for the selected door(s) that you are actively monitoring. The details of the highlighted event appear in the Details list box.

Toolbar controls all the basic operations for this mode.

Figure 75 - Basic Operate Console Toolbar

Let us examine the toolbar.

Display Zones

You can display all doors or the doors in a specific zone by using the drop down control found in the toolbar. If the dropdown control isn't visible, you can locate it by right-clicking on the toolbar or clicking on the indicator on the extreme right of the tool bar.

Select All

In the Doors display box, you can select a door by clicking on it. The standard Windows multiple selection behavior is observed when selecting multiple doors. Shift+Click selects all doors between the selected ones, Ctrl+Click only selects the doors that were clicked. But to easily select all of the doors in the Doors box, click the "Select All" tool in the toolbar.

Monitor

To monitor the activity of any door, highlight it and then click the "Monitor" tool. The events for the selected door or doors will appear in the activity list box.

To see the details of an event, click on it. The information for that event appears in the "Details" list box.

##Stop##

The ##Stop## tool causes all monitoring to cease.

Check

The "Check" tool allows you to check the status and information residing in a particular controller (e.g. firmware version, time and date, door delay time, etc…) ReadyAXS queries the selected door(s) and writes the results in the activity list box. To see the details, highlight the appropriate event. The information appears in the "Details" list box.

Adjust Time

Use the "Adjust Time" tool to send the current date and time from the computer to the selected doors.

Upload

This is one of the most important tools. This tool must be used whenever a change is made. Changes can be made in **Basic Config** and **Access Control** modes but to get those changes to the controllers, you must use the "Upload" tool.

Highlight the doors that must be updated. Quite often the changes affect all of them, so you can just click “Select All” then click “Upload”. ReadyAXS will send the changes to the appropriate doors

GetRec

The “GetRec” tool retrieves the records from the controller for the selected door and saves those records.

Realtime Get

The “Realtime Get” tool retrieves the records from the controller for the selected door and saves those records and begins to monitor the selected doors, storing the records while monitoring.

Remote Open

The “Remote Open” tool will pulse the selected door(s) allowing the door to be opened without swiping a card.

Clear Run Info

The “Clear Run Info” tool clears all displayed activity in the monitoring console.

Maps

This tool allows you to add map files to your system, place the doors appropriately and display them. **This is a work in progress.**

Warn Existed. Click to Confirm

This tool appears during monitoring when an alarm is occurs for a door being monitored. It will flash until it is clicked. The events will be confirmed and the tool will disappear again.

The events in yellow are the alarms that caused the “Warn Existed.” tool to display. The “Details” list box contains the information about the 12th event in the list.

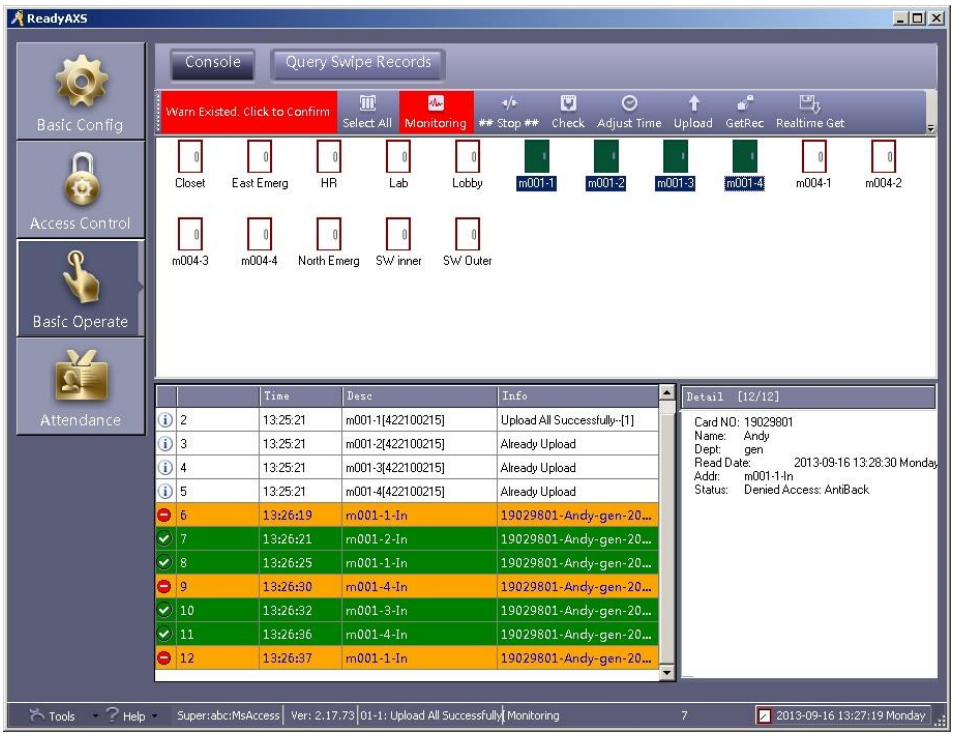


Figure 76 - Console Screen with Alarms in the Activity List Box

Query Swipe Records

All card swipes are recorded in the ReadyAXS database. To search and display the database, click the “Query Swipe Records” button on the **Basic Operate** screen.

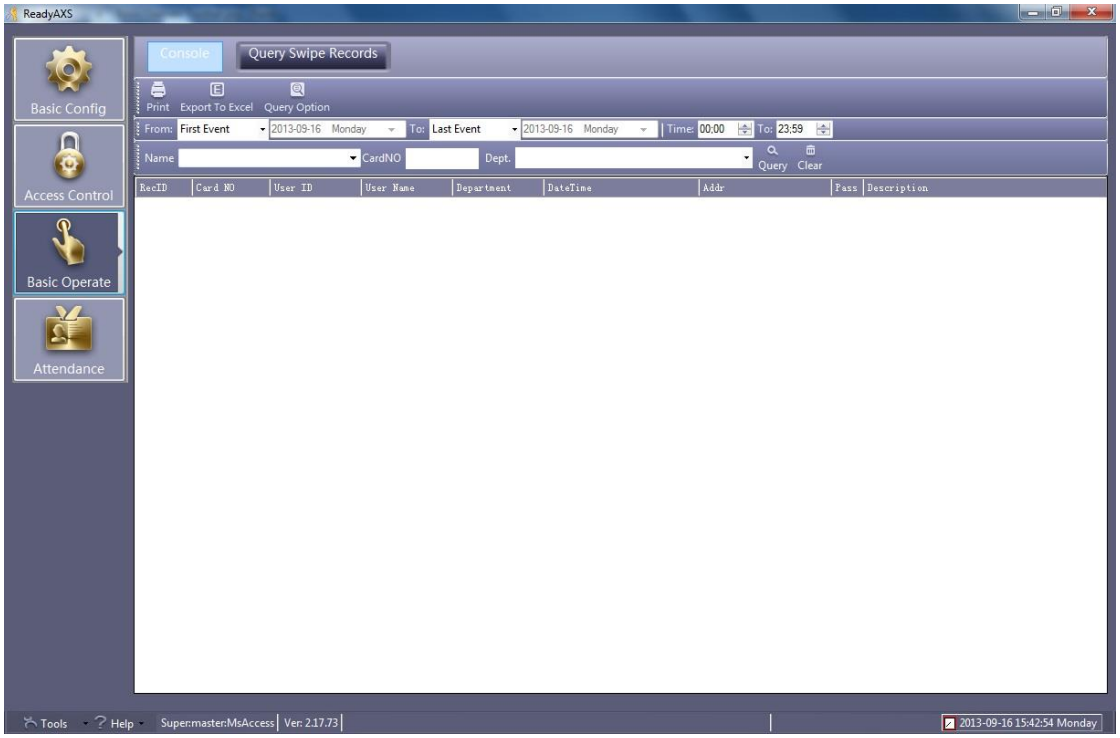


Figure 77 - Query Swipe Record Dialog

Use the Query toolbars to define your search criteria.

Figure 78 - Query Toolbars

The query elements are:

- From – Either the first event on the date or based on the time
- To – Either the last event on the date or based on the time
- Time – Start and end time
- Name – User name
- CardNO – Card number
- Department

A query can be done specifying one element, all elements, or any combination thereof. When the query is defined, click the “Query” tool. The database is searched and all records matching the query are displayed in the table.

To clear the table, click “Clear” in the toobar.