Smart Access Manager

Version 3.0

User Guide

Smart Access Manager

User Guide

Version 3.0

Contents

1 Introduction

Thank you for purchasing **SmartKey** *Access Control System*. The system contains the Master Controller and the Smart Access Manager (SAM) software. Integrating with door controllers and smart cards, it forms security system which protects buildings or premises by controlling door access by authorized persons only. The system can operate either online and offline. In offline mode, the standalone Main Controller can operate without connecting with the computer.

SAM provides a user friendly interface for the installation of Main Controllers and Door Control Units. The software detects connected devices and presents them clearly in the form of a tree structure in the window to facilitate installation. This powerful feature is also useful for troubleshooting and allows users to identify defected devices lying on the security network.

The powerful software comes with a multi-language support. It supports English, Traditional Chinese and Simplified Chinese language interface. Users can switch from one language interface to another easily with included translation software. Other languages are also supported upon request by calling our hotline.

SAM provides reporting function to generate a report to show the transaction log recorded in the Main Controllers. The **First In Last Out report** shows the first time and last time a person accesses to a particular door. Both reports are useful for human resources management and time attendance. The reports can also be exported as *Excel CSV files* and imported to external systems for other purposes.

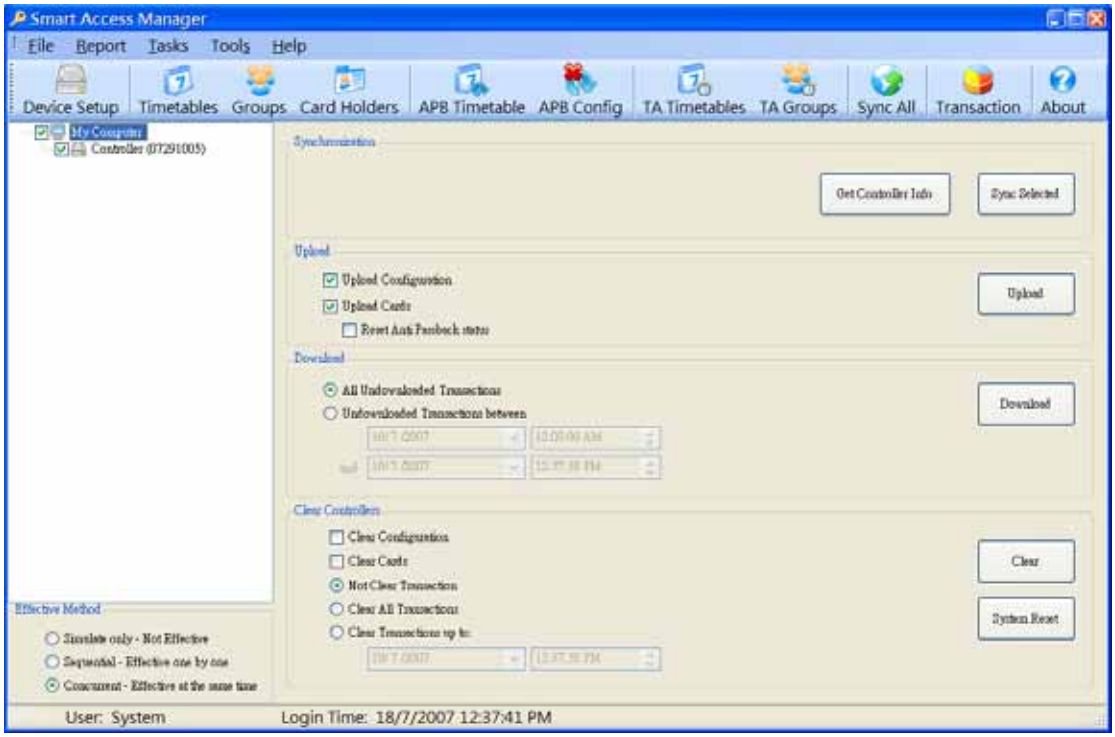
2 Configuration in SAM

This chapter gives a general description of setting up the hardware in SAM and provides instructions for the fundamental data setup which is necessary for the system to operate.

Before doing any configuration in SAM, you should go through the *Installation Guide* and complete the installation.

2.1 Main Menu

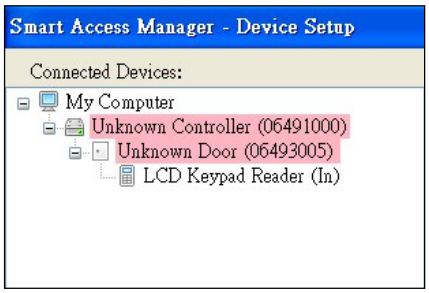
Start SAM by clicking the icon on the desktop. The Main Menu is displayed as below. You can navigate to other functions from the Main Menu.



2.2 Device Setup

Clicking the **Device Setup** button on the menu bar in the **Main Menu** will bring you to the **Device Setup** function. The function provides a user friendly interface for the setup of the Main Controllers and Door Control Units as describe below.

1. Click the **Scan Devices** button.



2. The system automatically explores all the Master Controllers and Door Control Units connected. The default come with Door 1, Door 2, you can change the SN for Door 1⁄2 for faster input.

3. If devices are found, they are displayed as “Unknown Controller” and “Unknown Door” on the left panel under **My Computer** icon.

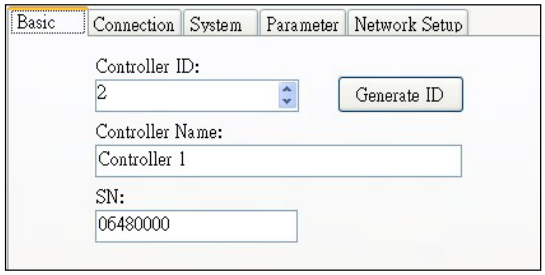
2.2.1 Set up Master Controller

1. Move the cursor to the “Unknown Controller” and left click.

2. Click the right mouse button and a window pops up.

3. Select **Add Controller** and the Controller will be automatically added as shown on the right panel.

4. On the **Basic** tag page, leave the default value on the **Controller ID** or enter a number to identify the controller. It should be a unique number among all controllers found. Alternately, you can click the **Generate ID** button to let the system automatically generate the ID.

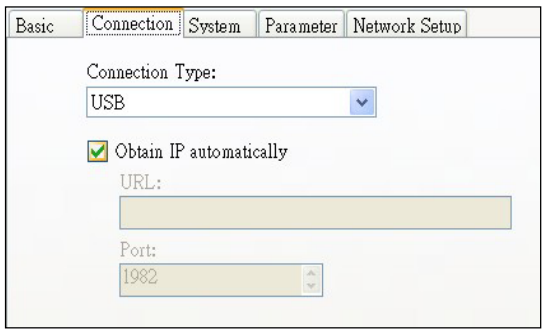


5. Enter a name on the **Controller Name** to describe the controller.

6. Use the default serial number **SN** or enter the serial number of the controller.

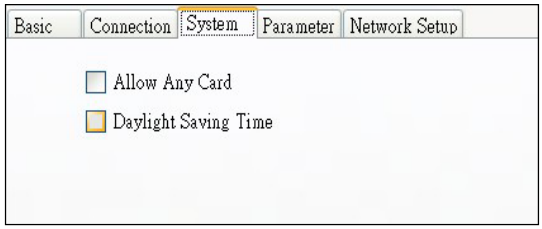
You can find the serial number on the cover of the package. Alternatively, you can find the serial number next to the controller icon on the left panel.

7. On the **Connection** tag page, select **USB** or **NETWORK** from the drop down list of **Connection Type**. By default, the system automatically detects the appropriate **Connection Type**.



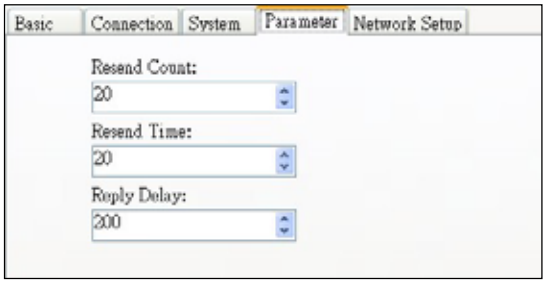
8. If the **Connection Type** is **NETWORK**, i.e. via Ethernet, uncheck **Obtain IP automatically** and enter the IP address and port number of the Master Controller; otherwise use the default and the system uses DHCP to automatically assign the IP address with port number 1982.

9. On the **System** tag page, under normal circumstances, leave the box **Allow Any Card** unchecked. Check the box only if you want to allow all card holders to gain access to the doors connected to the controller irrespective of the setting of the card holders in the system.

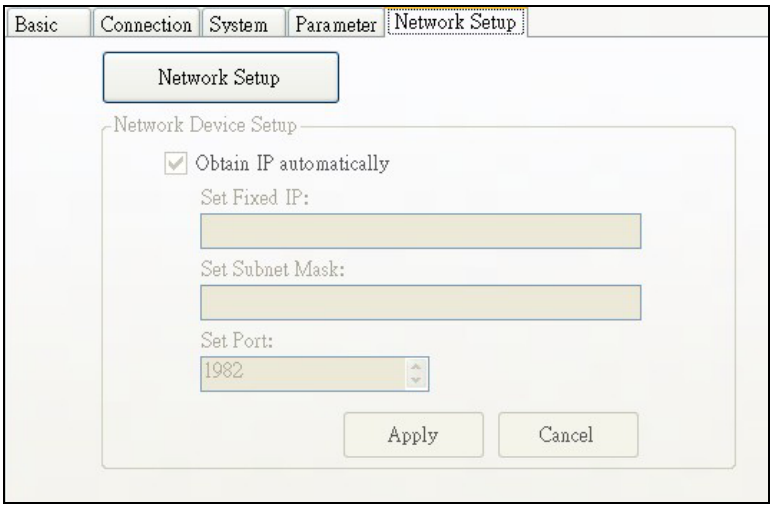


10. Check the box **Daylight Saving Time** (DST) if your country adopts DST; otherwise leave it unchecked by default.

11. On the **Parameter** tag page, the default values, which controls the throughout of the communication between the Master Controller and the computer, work fine under normal circumstances. Adjust the parameters only if you get connection problems.



12. On the **Network Setup** tag page, make any necessary changes if the connection is via Ethernet.



The system allows the setup of SAM on the computer remotely connected to the Master Controller via Ethernet. For more information about the setup of the controller under this circumstance, please visit our website or call our support.

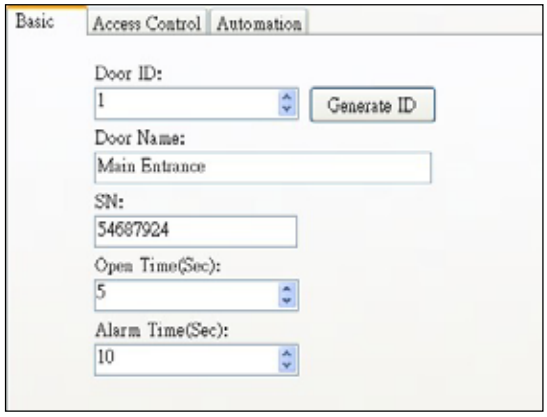
2.2.2 Set up Door Control Unit

1. Move the cursor to the "Unknown Door" and left click.

2. Click the right button of the mouse and a window pops up.

3. Select **Add Door** and the Door will be automatically added as shown on the right panel.

4. On the **Basic** tag page, leave the default **Door ID** or enter a number to identify the Door Control Unit. It should be a unique number among all Door Control Units found. Alternately, you can click the **Generate ID** button to let the system automatically generate the ID.



5. Enter a name on the **Door Name** to describe the door attached to the Door Control Unit.

6. Leave the serial number **SN** or enter the serial number of the Door Control Unit.

You can find the serial number on the cover of the package. Alternative, the system discovers the connected device and displays the serial number next to the door icon on the left panel.

7. Change the **Open Time** in second of which the door remains unlocked after a card holder opens the door.

8. Change the **Alarm Time** in second. If a card holder opens the door and does not close it for a period as specified in the **Alarm Time**, the alarm will be triggered

*The parameters **Open Time** and **Alarm Time** depend on the type of door and the door installation. Please consult your vendor providing the doors if they support these features. The typical value of **Open Time** is 1 second for **Drop Bolt** type electric lock and the magnetic lock is 5 second. If you have any further queries, please visit our website or call our support.*

9. On the **Access Control** tag page, check the box **Enable Door PIN** and enter a four-digit **Door PIN**. Select the **Door PIN Timetable** in which the PIN setting is effective. As a result, anyone can gain access to the door by entering the **Door PIN** without using the smart card. Uncheck it if it is not necessary.

Check the box **Enable Fire Alarm** if you want this door open during fire alarm occurs. Note that this feature is available if the Master controller connected to Fire Alarm system. For further queries, please contact your installation contractor.

It should be noted that the PIN is different from that of the card holders as described in the later section.

10. On the **Automation** tag page, check the box **Enable Always Open Timetable** and select the corresponding **Timetable** so that the

door remains open during the selected period. Normally, leave it unchecked by default.

*The parameter **Enable Always Open Timetable** depends on the type of door and the door installation. Please consult your vendor providing the doors if they support the feature. If you have any further queries, please visit our website or call our support.*

11. Finally, click the **Apply** button to make the changes.

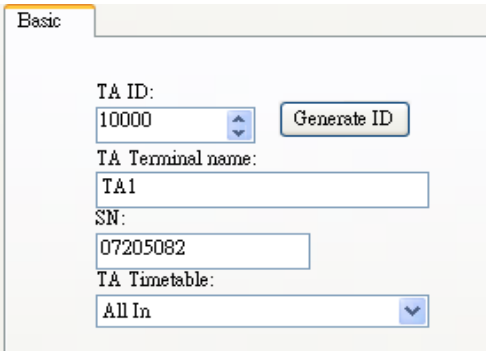
2.2.3 Set up TA Terminals

1. Move the cursor to the “Unknown TA” and left click.

2. Click the right button of the mouse and a window pops up.

3. Select **Add TA Terminal** and the TA will be automatically added as shown on the right panel.

4. On the **Basic** tag page, leave the default **TA ID** or enter a number to identify the TA Terminal. It should be a unique number among all TA Terminal found. Alternately, you can click the **Generate ID** button to let the system automatically generate the ID.



5. Enter a name on the **TA Terminal Name** to describe the TA attached to the Master controller.

12. Leave the serial number **SN** or enter the serial number of the TA Terminal. You can find the serial number on the cover of the package or the back of TA Terminal. Alternative, the system discovers the connected device and displays the serial number next to the TA Terminal icon ( ) on the left panel.

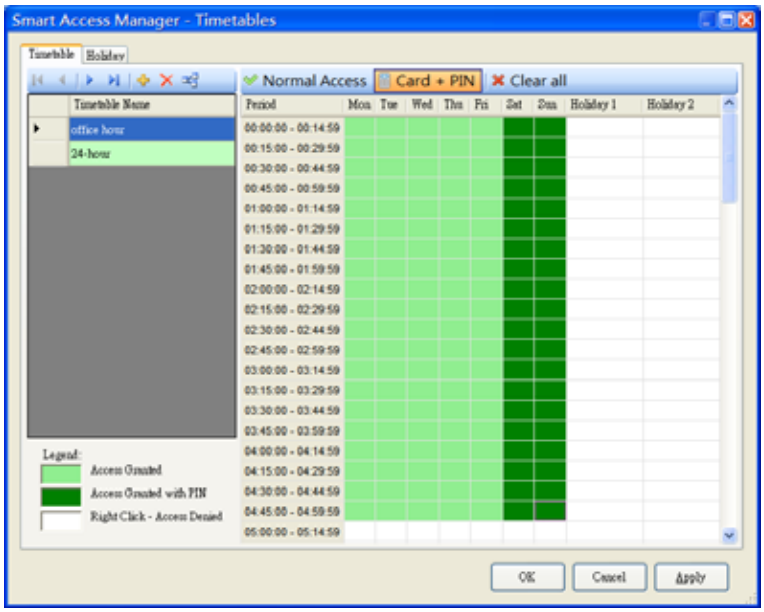
13. Change the **TA Timetable** for Automatic change In/Out period for that Terminal. You must create new TA Timetable before set this setting.

2.3 Timetables

The **Timetables** menu provides two functions, namely **Timetable** and **Holidays**.

2.3.1 Timetable

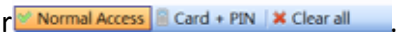
The **Timetable** function allows you to define the time zones of door access on business days and holidays. You can create different timetables for different groups of people. In this way, you can control the door access of different groups of people in different time zones.



To create a new **Timetable Name**:

1. Click the **Add** button .

2. Enter the name of the new blank record created at the bottom.

3. Click the Access mode on the tool bar 

. *Normal Access* is card only while *Card + PIN* is required the Indivual User PIN after present card.

4. On the right panel, move the cursor to the desired time slot.

5. Click the left mouse button and the time slot is changed from white to

green/light green which indicates the door access is granted.

6. To select a range of time slots, hold the left mouse button and drag the mouse and release the button. The selected time slots will be changed to green/light green.

7. To change the selected timeslot to access denied, follow the procedure 4-6 but click the right mouse button.

8. Click the **Apply** button to make the changes.

To remove an existing **Timetable Name:**

1. Position the cursor to the Timetable Name which is to be deleted.

2. Make sure that no existing Card Holders use the selected Timetable Name. Use **Related Settings** to check.

3. Click the **Delete** button  .

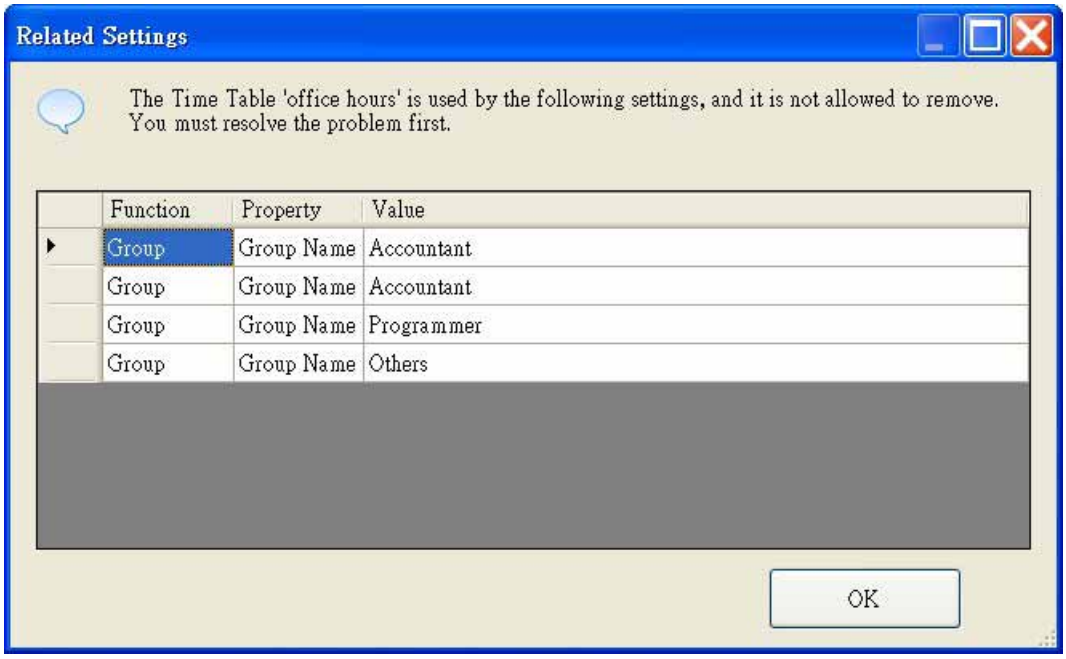
4. Click the **Apply** button to make the changes.

To check which existing Card Holders are associated with the Timetables:

1. Position the cursor to the **Timetable Name** to be checked.

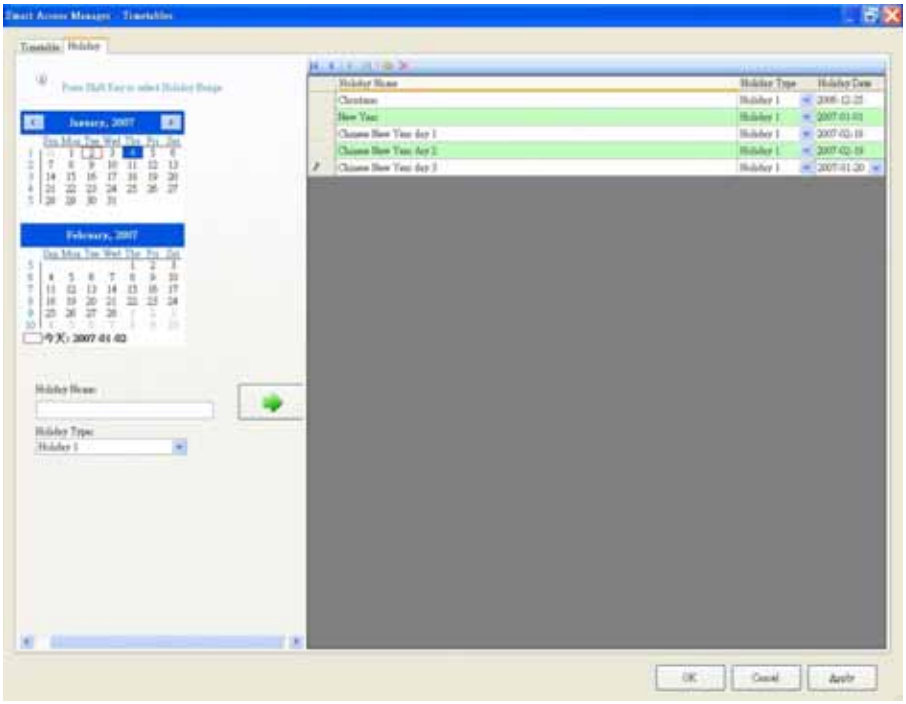
2. Click the **Related Settings** button  .

3. The results are displayed as shown below.



2.3.2 Holiday

The **Holiday** function allows you to define the holidays in the system. There are two types of holidays available in the system, namely Holiday 1 and Holiday 2. In some countries, there is more than one kind of holidays, e.g. in Hong Kong there are public holidays and labor holidays. You can define different timetables for the two types of holidays.



To create a new **Holiday** – Method 1:

1. Move the cursor on the desired date on the calendar on the left panel and click to select.

2. Enter the **Holiday Name**.

3. Select the **Holiday Type** from the drop down list.

4. Click the **Add** button  and the record will be added.

5. Click the **Apply** button to make the changes.

To create a new **Holiday** – Method 2:

1. Click the **Add** button  .

2. Enter the **Holiday Name** of the new record created at the bottom.

3. Select the **Holiday Type** from the drop down list.

4. Enter the **Holiday Date** or select from the drop down list.

5. Click the **Apply** button to make the changes.

To remove an existing **Holiday:**

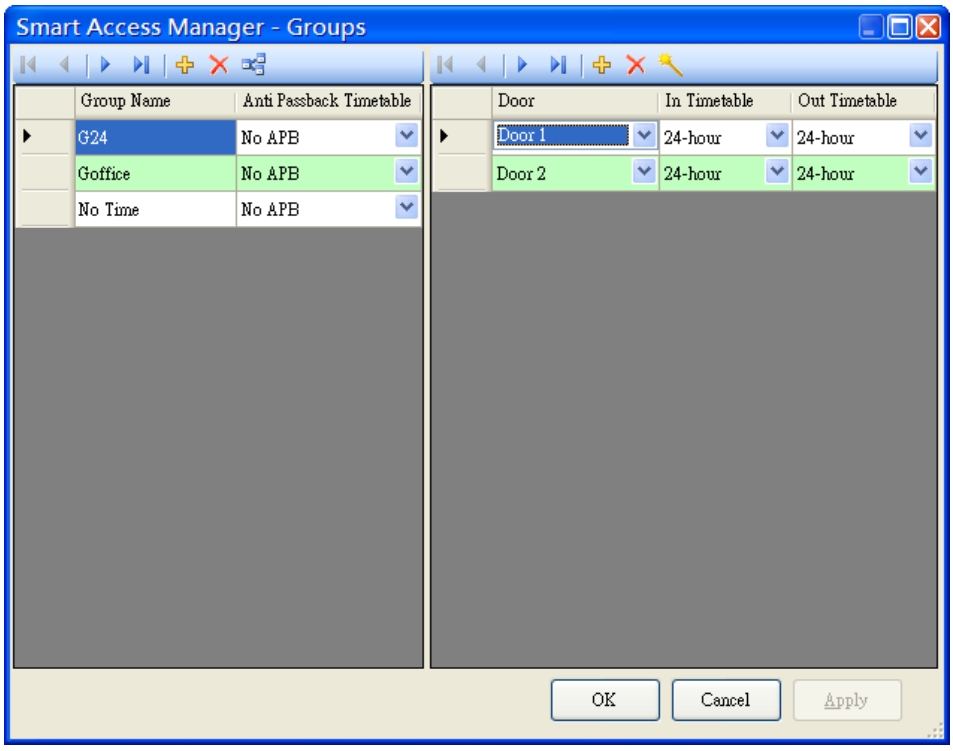
1. Position the cursor to the **Holiday** which is to be deleted.

2. Click the **Delete** button  .

3. Click the **Apply** button to make the changes.

2.4 Groups

The **Groups** function allows you to define the door access right and the corresponding timetable of a group of people.



To create a new **Group**:

1. Click the **Add** button on the left hand tool bar.

2. Enter the **Group Name** of the new record created at the bottom on the left panel.

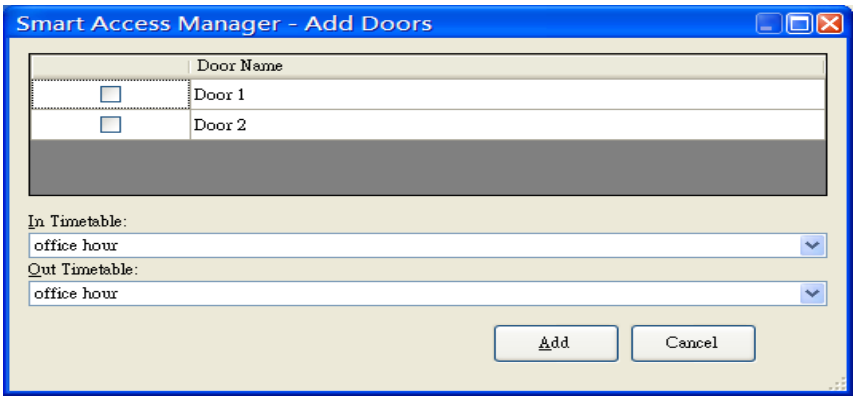
3. Select the **Door** from the drop down list on the right panel.

4. Select **In Timetable** from the drop down list.

5. Select **Out Timetable** from the drop down list.

6. Note that if the door has a *keypad reader* and **Timetable** has set **Card + PIN**, the group will be required **indivual user PIN** to access the door.

7. For faster input the doors, you can click  on the right hand tool bar. Then a dialog will show as

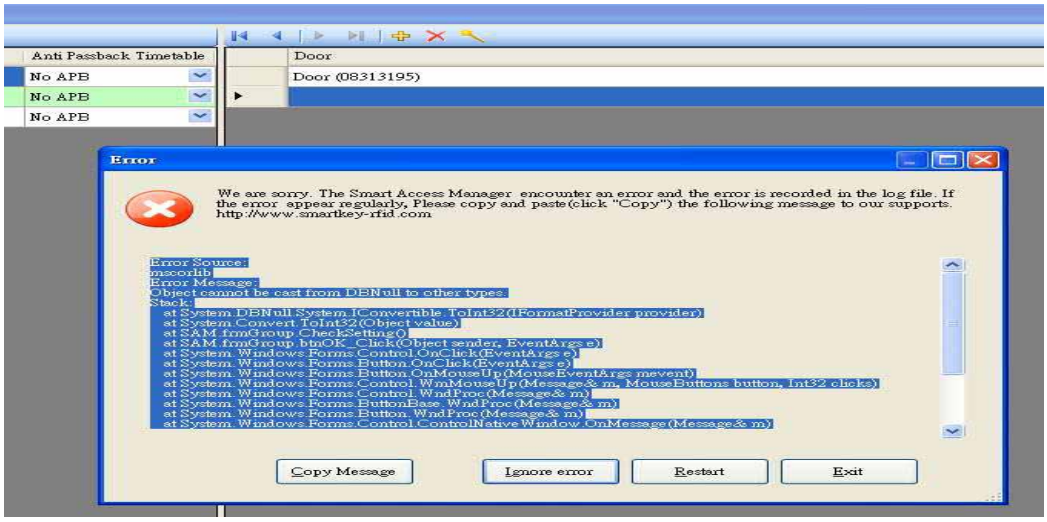


Simplify click the door(s) and select the default In, out timetable, then click **Add**

8. Click the **Apply** button to make the changes.

Remarks :

Added a Blank Door Row will cause error message as below when click "Apply" or "OK"



click "ignore error" then click delete button  *to delete the blank door row to solve it .*

To remove an existing **Group**:

1. Position the cursor to the **Group** which is to be deleted.
2. Click the **Delete** button  .
3. Click the **Apply** button to make the changes.

Each door can only link to only one Timetable; otherwise an error will be displayed.

2.5 Department

The **Department** function allows you to group card holders in terms of department. Select the main menu, Task\Department:

To create a new **Department Code**:

1. Click the **Add** button .
2. Enter the **Department Code** of the new record created at the bottom.
3. Enter the name of the **Department**.

4. Click the **Apply** button to make the changes.

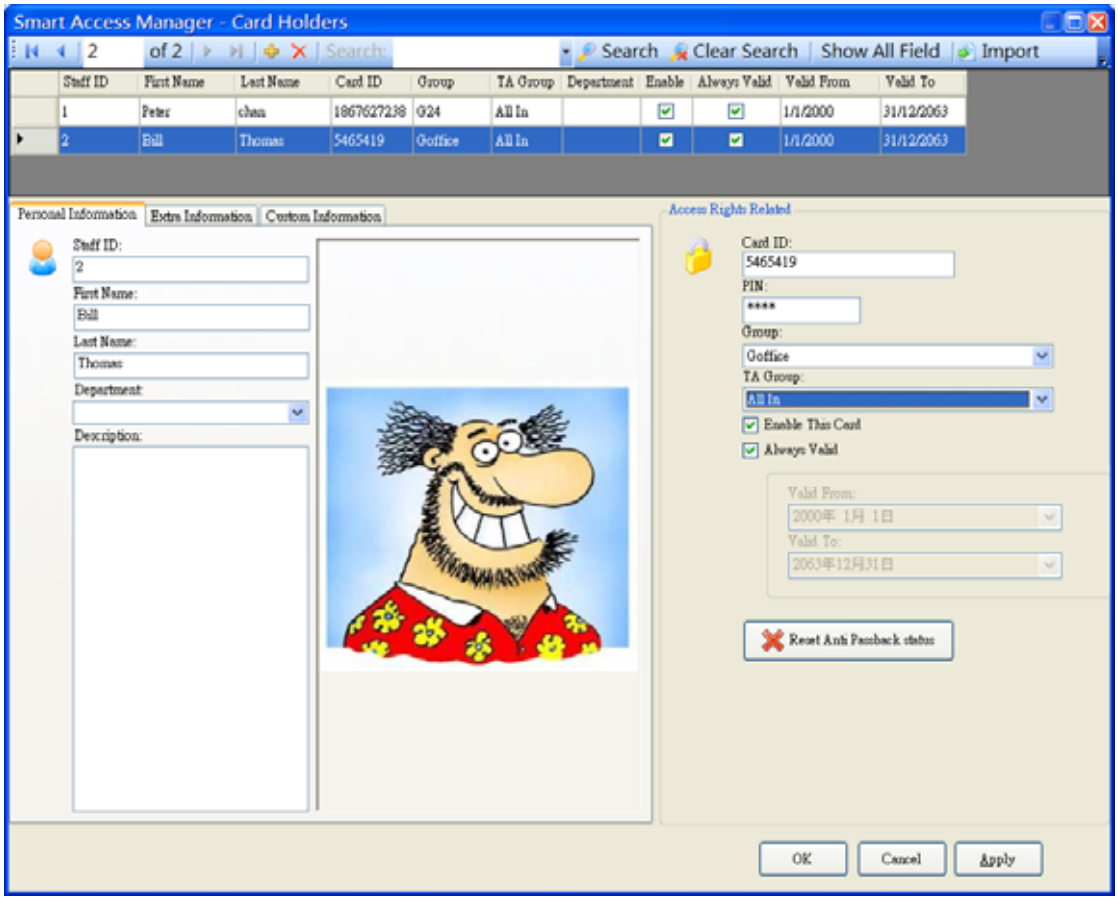
To remove an existing **Department Code**:

1. Position the cursor to the **Group** which is to be deleted.
2. Click the **Delete** button .
3. Click the **Apply** button to make the changes.

Department Code is not allowed to repeat.

2.6 Card Holders

The **Card Holders** function allows you to define the door access right of an individual. Personal details and photographs of the card holders can be maintained for additional identification.



To create a new **Card Holder**:

1. Click the **Add** button .

2. Enter the **Staff ID**, **First Name** and **Last Name** of the Card Holder.

3. Select the **Department** from the drop down list. (Refer to previous section for the creation of Department).

4. Enter the **Description** of the Card Holder as necessary.

5. Enter the **Card ID** of the smart card.

<u>Remarks : How to get the card ID</u>

Method [A]

Read the card ID by another stand alone reader and drop down the card ID

Method [B]

make sure all the readers already connected with the Door units & controllers and the SAM software is installed properly

Go to main menu → transaction → real time scan  ***(icon)***

Then put the card on any reader to read

A long beep will be heard and an invalid card message will be show on the transaction.Double click on the invalid transaction column .

The screen will switch to card holders menu and the card ID will be shown on the field automatically.

6. Enter the **PIN** if a PIN is required to gain access to the door; otherwise leave it blank. (valid for the reader with keypad version only)

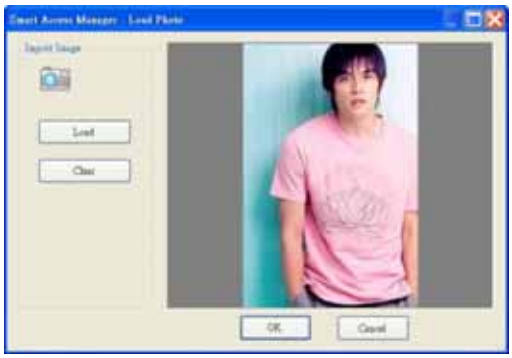
7. Select the **Group** as defined in the previous section from the drop down list.

8. Select the **TA Group** as defined in the previous section from the drop down list.

9. Check the box **Enable This Card** to make the setting the card to take immediate effect. Uncheck the box will disable the card.

10. Check the box **Always Valid** to enable the card with no expiry date. Uncheck the box and input the valid period of the card.

11. Optionally, you can upload an photograph of the Card Holder by clicking the button in the middle white box. A window will pop up to guide to import the image.



12. On the **Extra Information** tab page, enter personal details of the Card Holder as necessary.

13. On the **Custom Information** tab page, enter additional information as necessary.

14. Click the **Apply** button to make the changes.

To remove an existing **Card Holder**:

1. Position the cursor to the **Card Holder** which is to be deleted.

2. Click the **Delete** button  .

3. Click the **Apply** button to make the changes.

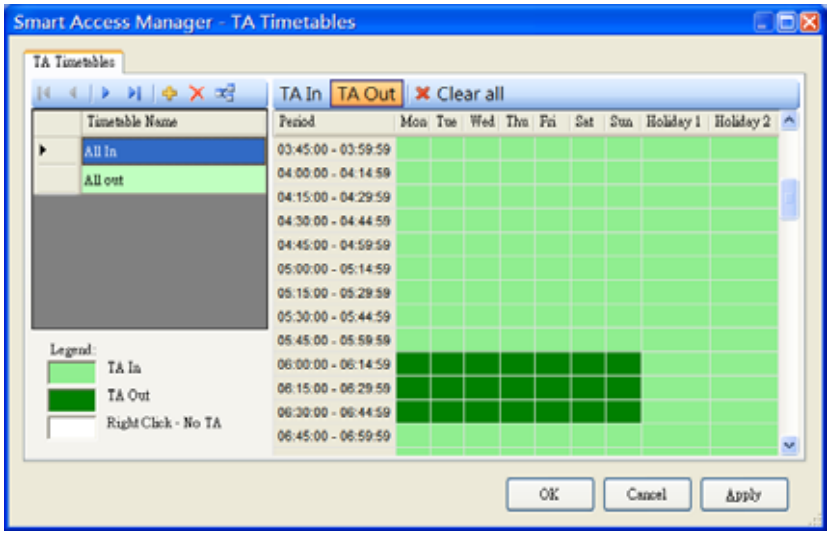
- *A search function is provided to allow you to easily locate the Card Holders. You can enter the Staff ID, First Name, Last Name or Card ID and click **Search** Button. A list of card holders with details matching the criteria will be displayed. To reset the list, click the **Clear Search** button.*

- *Staff ID is a unique indentify the person and his/her transaction. Once enter, please don't change otherwise you can't view the person's transaction.*

2.7 TA Timetables

2.7.1 TA Timetable

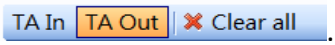
The **TA Timetable** function allows you to define the time zones of TA access on business days and holidays. You can create different timetables for different groups of people. In this way, you can control the TA access of different groups of people in different time zones.



To create a new **TA Timetable Name**:

1. Click the **Add** button  .

2. Enter the name of the new blank record created at the bottom.

3. Click the Access mode on the tool bar 

.

4. On the right panel, move the cursor to the desired time slot.

5. Click the left mouse button and the time slot is changed from white to green/light green which indicates the In/Out.

6. To select a range of time slots, hold the left mouse button and drag the mouse and release the button. The selected time slots will be changed to green/light green.

7. To change the selected timeslot to access denied, follow the procedure 4-6 but click the right mouse button.

8. Click the **Apply** button to make the changes.

To remove an existing **TA Timetable Name:**

1. Position the cursor to the Timetable Name which is to be deleted.

2. Make sure that no existing Card Holders use the selected TA Timetable Name. Use **Related Settings** to check.

3. Click the **Delete** button  .

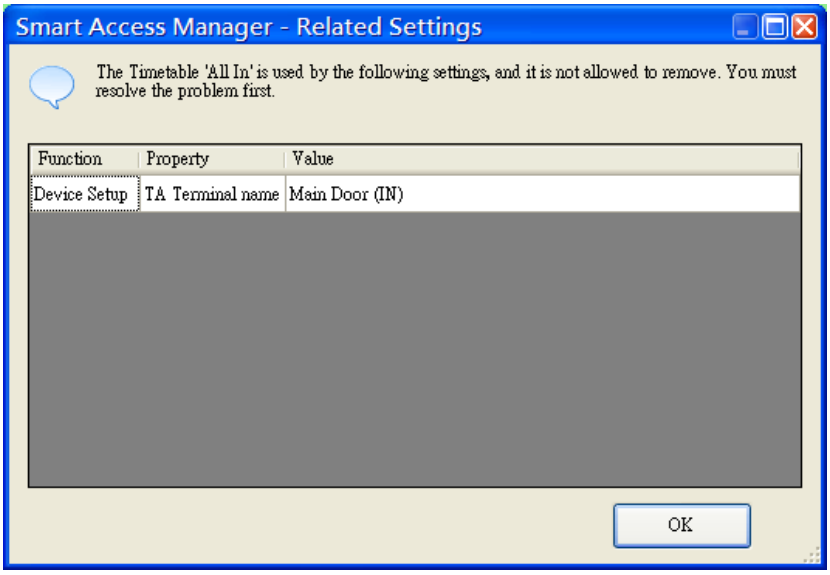
4. Click the **Apply** button to make the changes.

To check which existing Card Holders are associated with the TA Timetables:

1. Position the cursor to the **TA Timetable Name** to be checked.

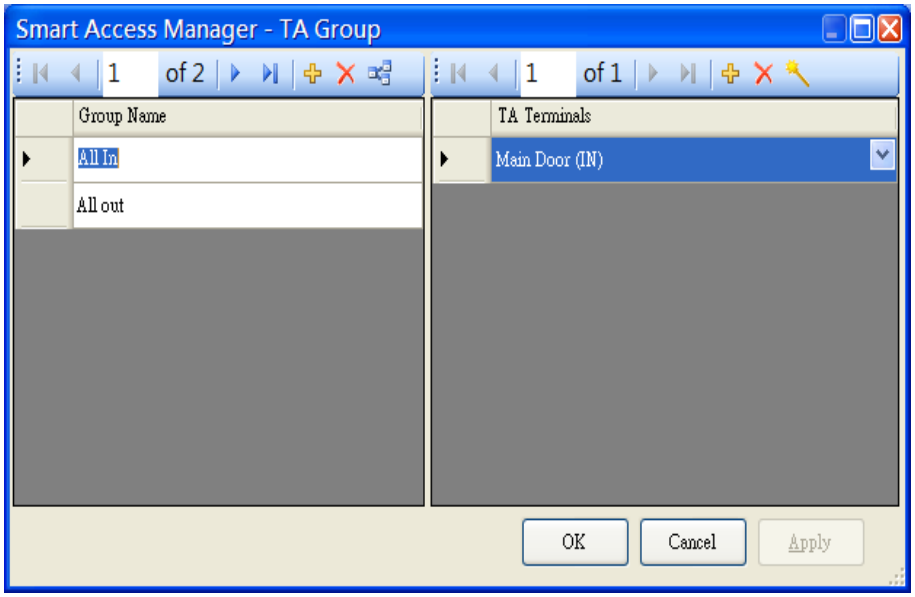
2. Click the **Related Settings** button  .

3. The results are displayed as shown below.



2.8 TA Groups

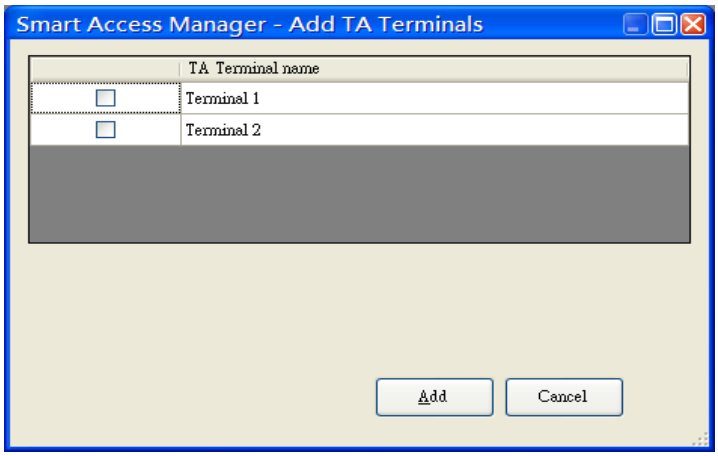
The **TA Groups** function allows you to define the groups of TA Terminals



To create a new **TA Group**:

9. Enter the **Group Name** of the new record created at the bottom on the left panel.

10. click  on the right hand tool bar. Then a dialog will show as

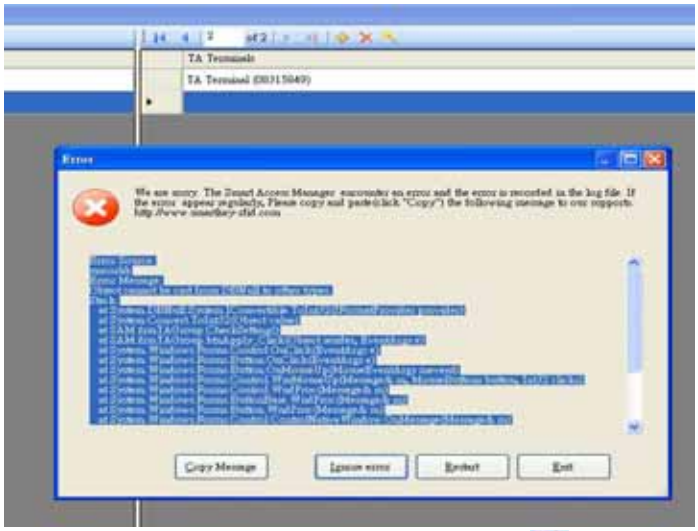


11. Simplify click the Terminal(s) then click **Add**
12. Click the **Apply** button to make the changes.

Remark :

 *is Nil function under TA selection menu , pls use*  *to add a TA group*

Added a Blank TA row will cause error message as below when click "Apply" or "OK"



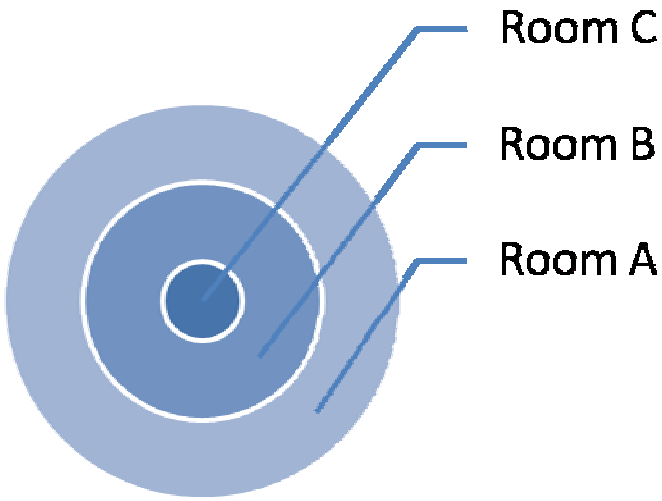
click "ignore error" then click delete button  *to delete the blank TA row to solve it .*

To remove an existing **TA Group**:

4. Position the cursor to the **TA Group** which is to be deleted.
5. Click the **Delete** button  .
6. Click the **Apply** button to make the changes.

2.9 Anti Passback

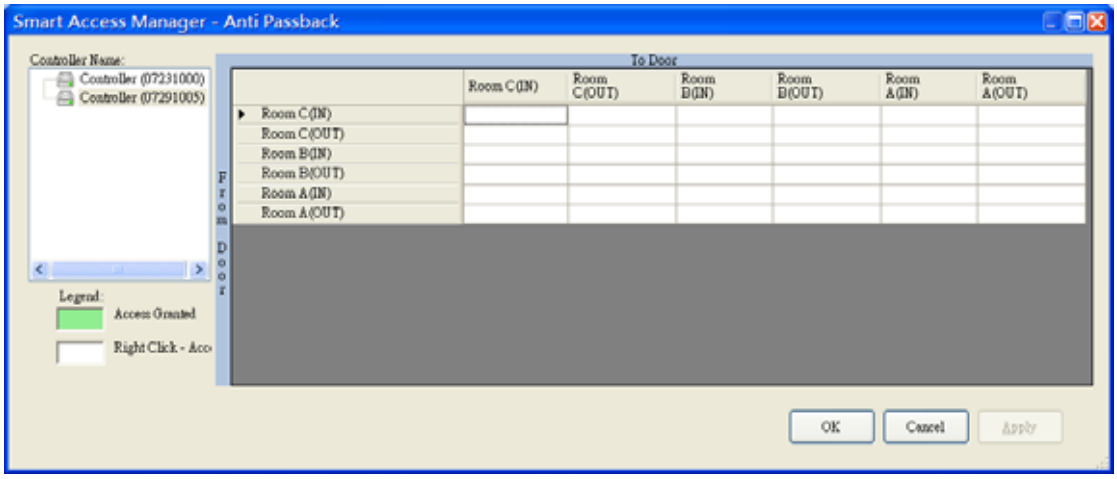
Anti-Passback (APB) is a direction control mechanism in access control. For example, Peter enters Room A and he can not enter Room A again if he doesn't exit from Room A. Furthermore, APB can set a desired path for human. Refer to the following figure, a possible path is Room A → Room B → Room C →Room B, etc. APB can block the path for Room A → Room C.



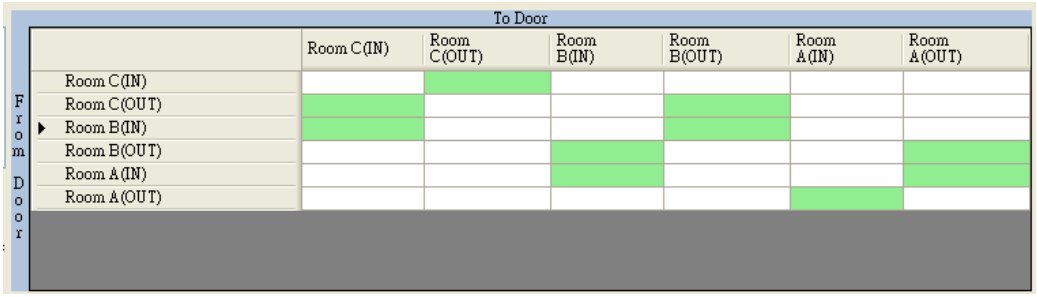
2.9.1 Setup Anti Passback Config

Click **Tools\Anti Passback config** in main screen menu.

In Anti Passback config screen, click the desired Master Controller on the left hand side, as shown



The Horizontal is *To Door* and vertical is *From Door*, now we are set the path Room A → Room B → Room C → Room B → Room A, **left click** the box to select the path or right click to clear the box as shown in the following figure:

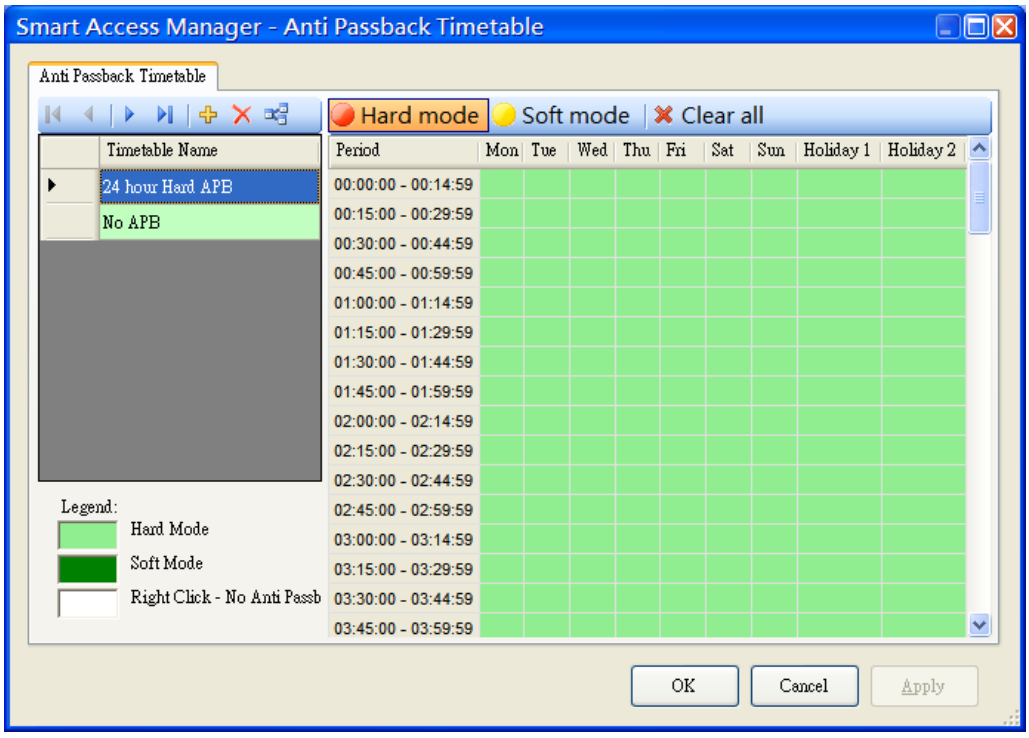


2.9.2 Setup Anti Passback Timetables

1. Click Tools\Anti Passback Timetables in main screen menu.

2. A Anti Passback Timetables screen will appear, the left hand side is Timetable name and right hand side is timetable setting, APB has two modes: Hard and Soft.

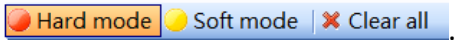
   - Hard mode – The Cardholder must follow the path
   - Soft mode – The Cardholder can follow the path, but the system will block one time if he break the APB rule, that is need to present card twice.



To create a new **Timetable Name**:

1. Click the **Add** button .

2. Enter the name of the new blank record created at the bottom.

3. Click the Access mode on the tool bar 

. *Hard mode* is no exception on APB while Soft mode can bypass the rule(need present card twice.

4. On the right panel, move the cursor to the desired time slot.

5. Click the left mouse button and the time slot is changed from white to green/light green which indicates the mode.

6. To select a range of time slots, hold the left mouse button and drag the mouse and release the button. The selected time slots will be changed to green/light green.

7. To change the selected timeslot to No Anti Passback, follow the procedure 4-6 but click the right mouse button.

8. Click the **Apply** button to make the changes.

To remove an existing **Anti Passback Timetable Name:**

1. Position the cursor to the Timetable Name which is to be deleted.

2. Make sure that no Group(s) uses the selected Timetable Name. Use **Related Settings** to check.

3. Click the **Delete** button .

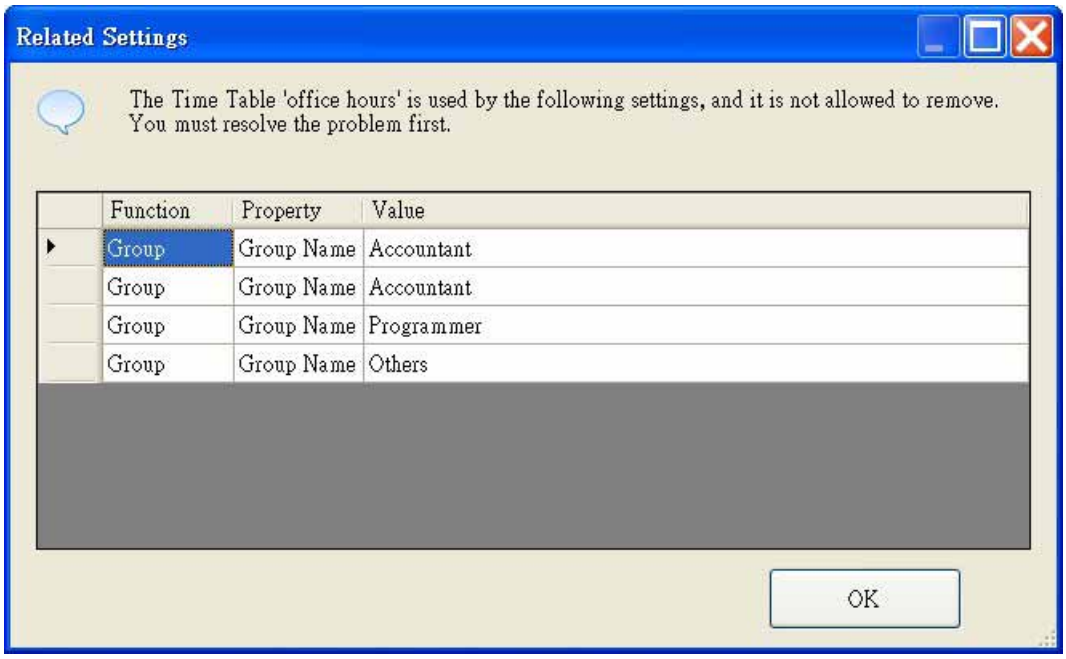
4. Click the **Apply** button to make the changes.

To check which existing Groups are associated with the Timetables:

1. Position the cursor to the **Timetable Name** to be checked.

2. Click the **Related Settings** button .

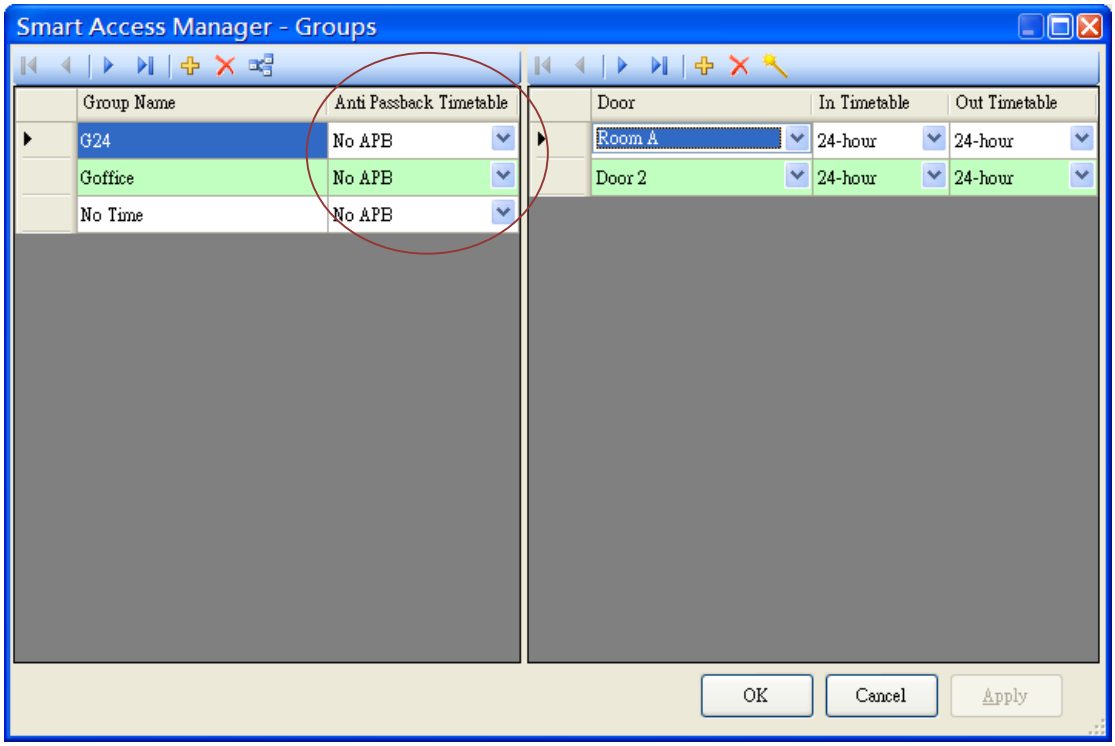
3. The results are displayed as shown below.



2.9.3 Setup Anti Passback in groups

1. In the Main screen, click the Groups button.

2. On the left hand side, Choose the desired Anti Passback timetable for each groups:

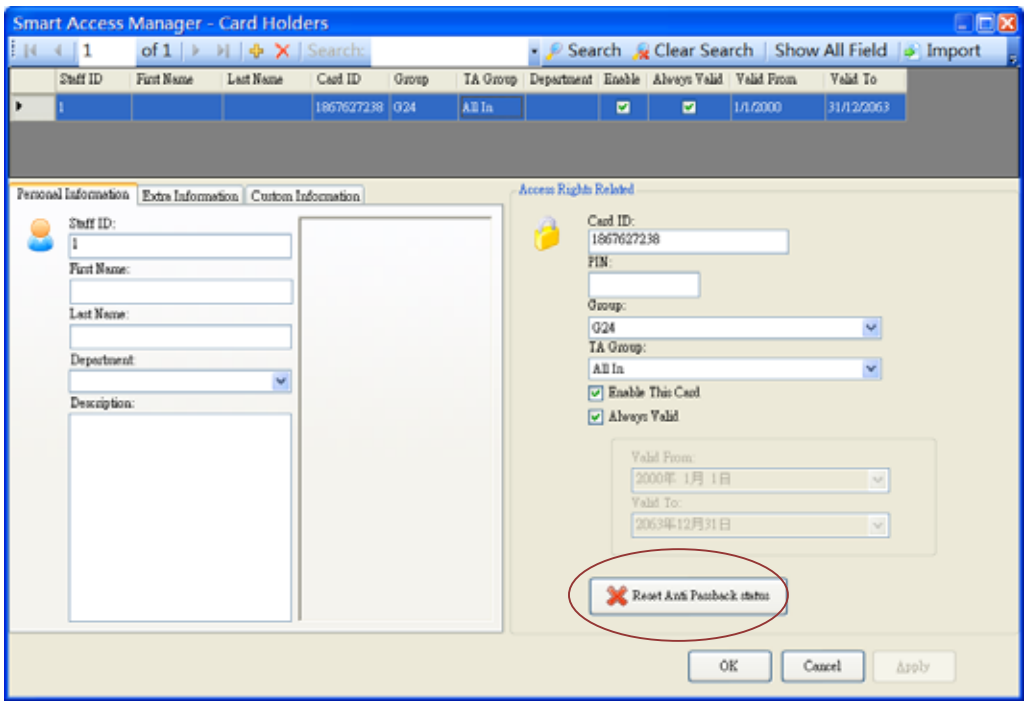


3. Click the **Apply** button to make the changes.

2.9.4 Reset Anti Passback status for one Cardholder

1. Click **Tasks\Cardholder** in main screen's menu

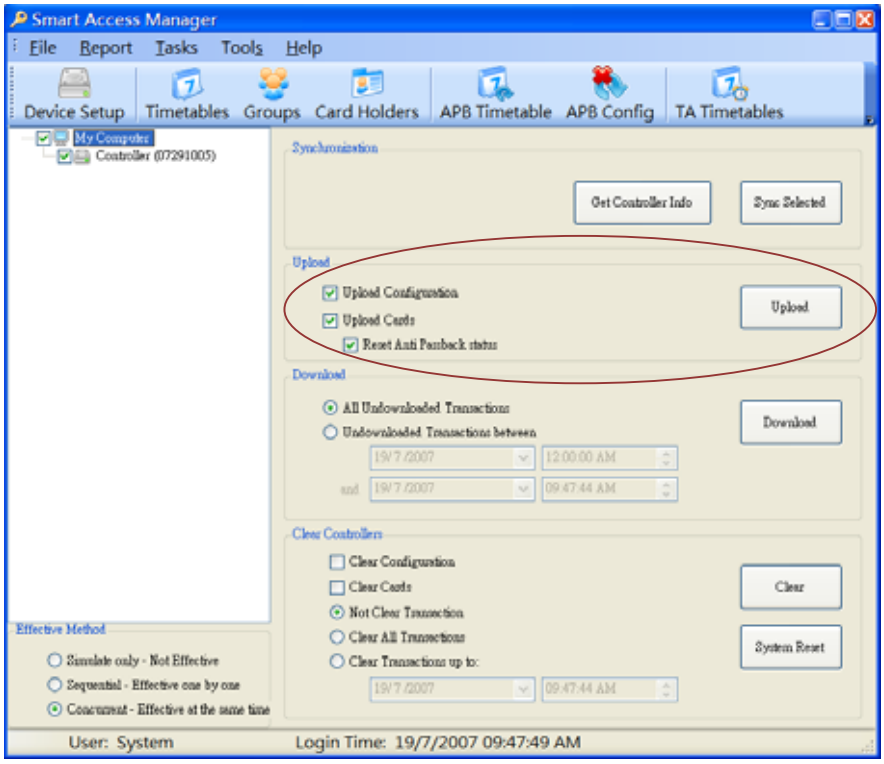
2. Select a **cardholder**, click the **Reset Anti Passback status** button on the right bottom side of screen.



2.9.5 Reset Anti Passback status for one Cardholder

1. Check the checkbox **Reset Anti Passback status** in the main screen

2. Click **Upload** button



2.9.6 Anti Passback Limitations

Local scope – The APB information is store in each controller and doesn't share information between Master Controllers. For Example, you can't control the sequence when *Room A* in *Master Controller A* and *Room B* in *Master Controller B*.

2.10 Emergency Card

The Access Right and Cardholders information is store in Master Controller while Emergency Card is store in Door Control Unit(DCU). When the Emergency Card was stored in the DCU, any of the following situations can be open the door:

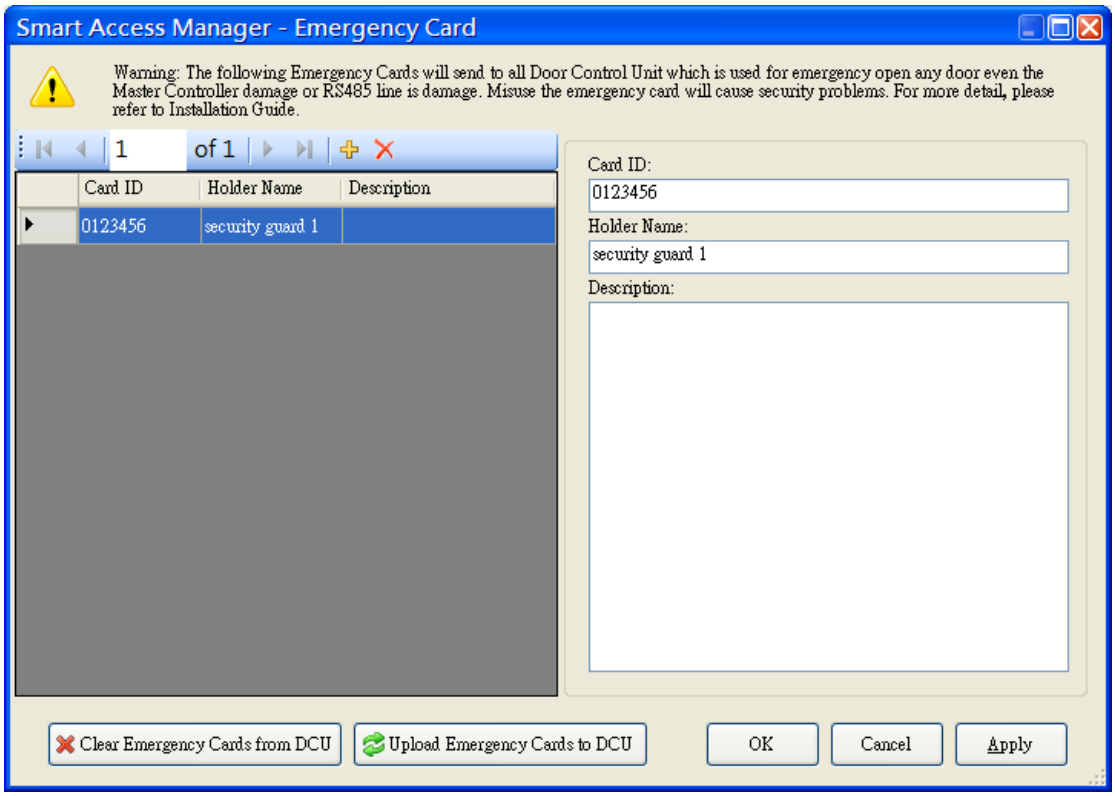
1. Master Controller was damaged
2. Master Controller has no power
3. The cable between Master Controller and Door Control Unit was damaged

However, the following condition must meet:

1. Door lock has backup battery
2. DCU has backup battery
3. Reader has backup battery
4. Cables between DCU and Reader is no damage
5. Cables between DCU and Door lock is no damage

Setup Emergency Card

1. Click **Tools\Emergency Card** in main screen's menu
2. Click the **Add** button  on the left hand side tool bar.
3. Enter the **Card ID, Holder Name** in the right hand side
4. Repeat step 2-3 for another card
5. Click the **Apply** button to make the changes to Database only.
6. Click the **Clear Emergency card from DCU** button
7. Click the **Upload Emergency card to DCU** button



Clear Emergency cards from DCU means no emergency card in DCU but database has the card.

The maximum number of Emergency cards for the DCU is 10, while database is unlimited.

Upload and Clear Emergency card function will apply to ALL the doors.

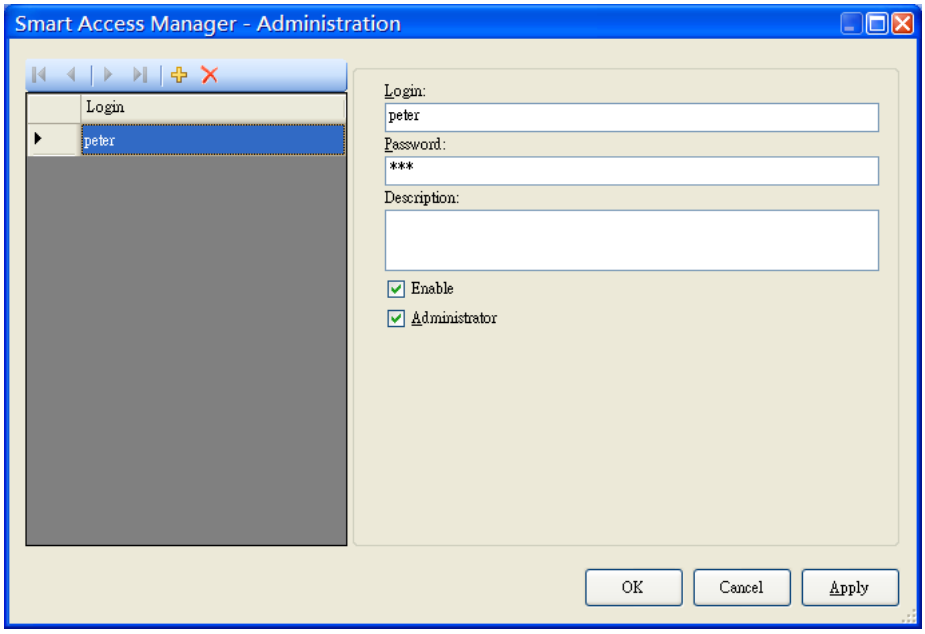
If the DCU was replaced, it is required to click the ***Upload Emergency card to DCU*** *button After the Device Setup*

2.11 Administration

Smart Access Manger allows multi-user administration. For example, Manager is allowing to full access (Administrator) in SAM while accountant is allow to view *First In, Last Out Report* (User) only.

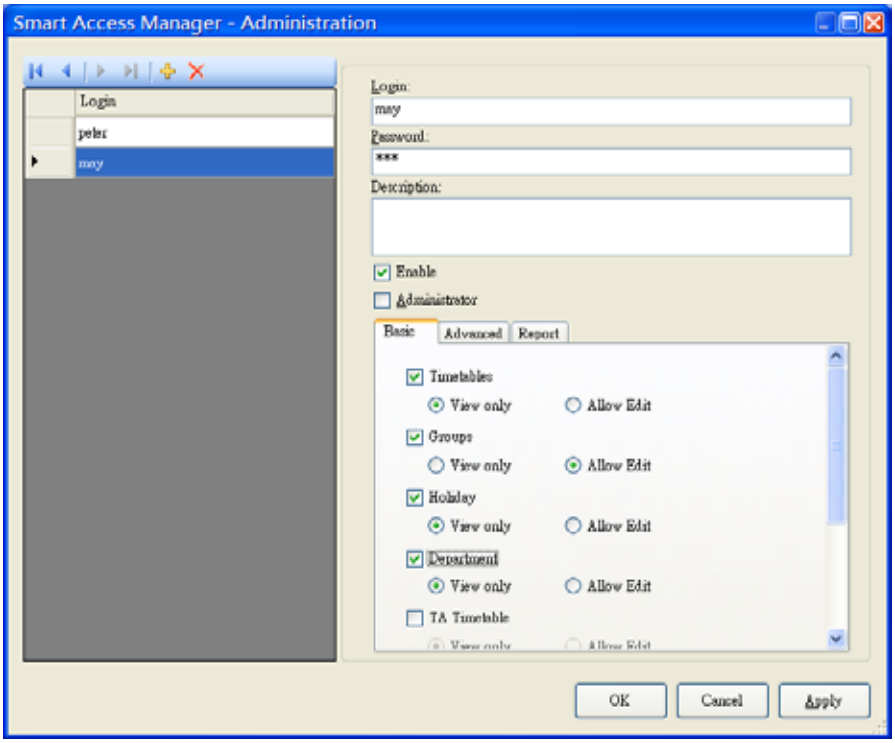
2.11.1 Create Administrators

1. Click Tools\Administration on the main screen's menu
2. Click the **Add** button  on the left hand side tool bar.
3. Enter the **Login, Password** in the right hand side
4. Check the checkbox Administrator
5. Repeat step 2-4 for another user
6. Click the **Apply** button to make the changes



2.11.2 Create Users

1. Click Tools\Administration on the main screen's menu
2. Click the **Add** button  on the left hand side tool bar.
3. Enter the **Login, Password** in the right hand side
4. Un-Check the checkbox Administrator
5. Select the Access right for Smart Access Manager for the user on the right bottom side.
6. Repeat step 2-5 for another user
7. Click the **Apply** button to make the changes



Only Administrator has a right to access the Administration.
SAM must have at lease one Administrator.
Login screen will not appear If no Administrator and user.

2.12 Sync All/Sync Selected

After the setup has been completed in the computer, the settings have to be uploaded to the Master Controllers. You can run synchronization with all or selected controllers. The configuration and card holder information will be populated to the controllers. After the synchronization, the Access Control System is ready to use.

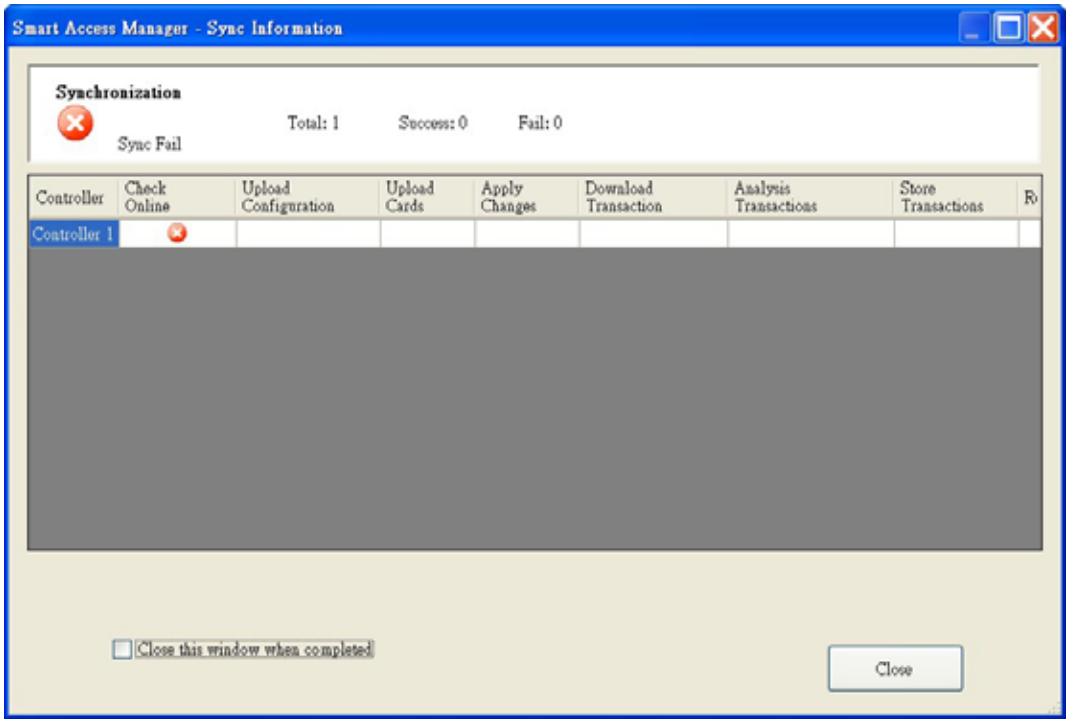
The time of the computer and the Main Controllers gets synchronized during this process.

2.12.1 Sync All

1. In the Main Menu, click the **Sync All** button so that the configuration and card information of all the Controllers will be synchronized.

2. The synchronization starts immediately and a window pops up to show the progress.

3. Upon completion, the window closes automatically.



2.12.2 Sync Selected

1. On the left panel of the Main Menu, check the box of the controllers to be synchronized.

2. Click the Sync Selected button.

3. The synchronization starts immediately and a window pops up to show the progress.

4. Upon completion, the window closes automatically.

At the left hand corner of the Main Menu, there are three **Effective Methods** which affect the Synchronization process.

Simulate only – Not effective
The synchronization runs without actually uploading the data to the Main Controllers. This is used to check the connection between the PC and Controllers before actual upload takes place.

Sequential – Effective one by one
When there is more than one Main Controller connected, the same set of data is uploaded to the Controllers one after the other. When this method is selected, the data in a Controller is effective right after the synchronization of that Controller is completed. As a result, there is a time during which the data in all the Controllers are not in line during the synchronization of all the Controllers.

Concurrent – Effective at the same time (default setting)
When there is more than one Main Controller connected, the data in all of the Main Controllers will get effective at the same time after the synchronization of all the Controllers is completed. In other words, all the Controllers have the same set of information at all of the time.

3 Miscellaneous Functions

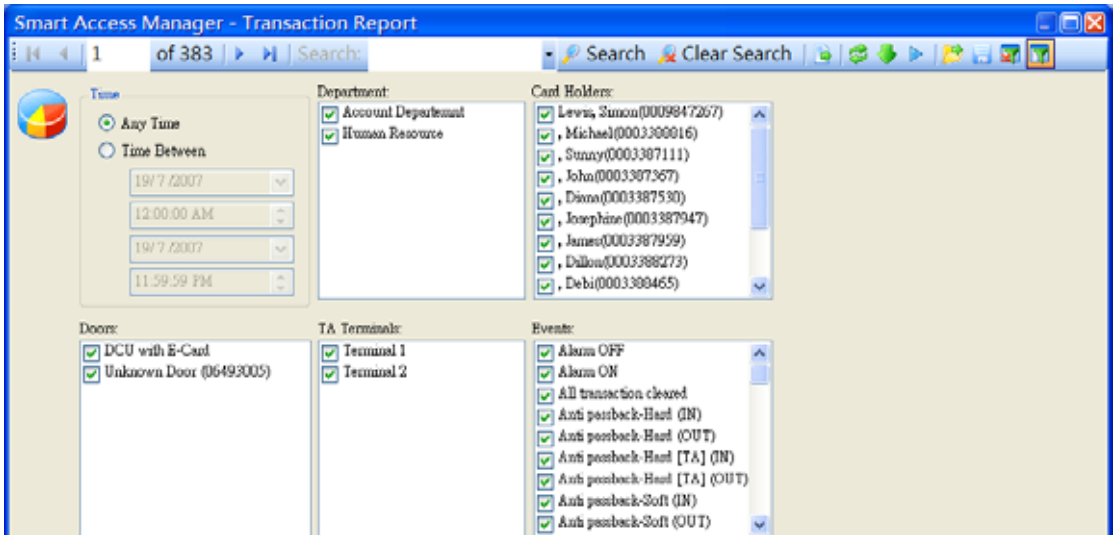
This chapter describes the miscellaneous functions available in SAM. The functions include reporting, upload/download and customization of the system.

3.1 Report

After the data are downloaded from the Main Controllers to the computer, you can generate two reports, namely *Transaction Report* and *First In, Last Out Report*, to review the transaction log in the Controllers.

3.1.1 Transaction Report

The report shows the complete set of transactions logged in the Controllers. It provides details of the transactions such as Controllers, Card Holders, Doors, Events and Time. The report is useful to track who and when has entered a particular door in case of investigation.

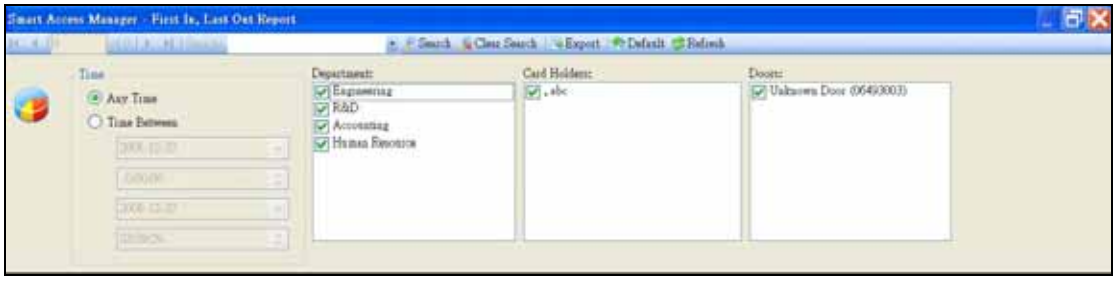


To create the report:

1. In the Main Menu, click **Transaction Report** under the **Report Menu**.
2. In the Transaction Report function, click filter button  . select **Time**, **Department**, **Card Holders**, **Doors** and **Events**.
3. Click **Refresh** and the transactions meeting the selection criteria are generated on the screen.
4. Enter the keyword in the **Search field** and press the **Search** button. Only records containing the keyword will be displayed.
5. To export the results to a CSV file, click the **Export** button on the top menu bar.
6. Select the fields to be exported and click the button.
7. Enter the destination file.
8. Press the **Export** button to generate the output file.

3.1.2 First In Last Out Report

The report provides tracking records of card holders the first and last time accessing the doors within the requested period.



To create the report:

1. In the Main Menu, click **First In Last Out Report** under the **Report Menu**.

2. Enter the **Time**, **Department**, **Card Holders** and **Doors**.

3. Click Refresh and the transactions meeting the selection criteria are generated on the screen.

4. Enter the keyword in the Search field and press the Search button. Only records containing the keyword will be displayed.

5. To export the results to a CSV file, click the **Export** button on the top menu bar.

6. Select the fields to be exported and click the  button.

7. Enter the filename and the destination directory.

8. Press the **Export** button to generate the output file.

3.1.3 Report Template

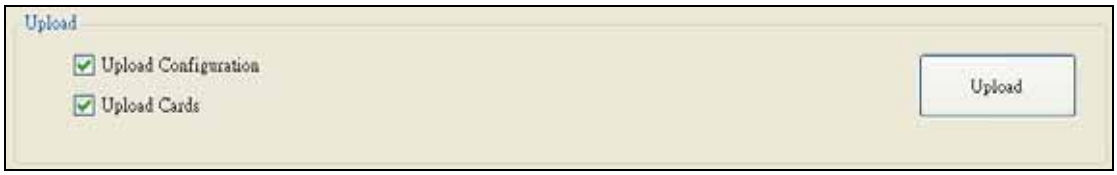
In report, the filter can be saving as a template file and load the template later.

1. For save template, click  on tool bar

2. For save template, click  on tool bar

3.2 Upload Function

In the Main Menu, the **Upload** function allows you to transfer the configuration and/or Card Holders data defined in SAM from the computer to the Controllers. If both configuration and Card Holders are selected, the results are the same as Synchronization as described in the previous sections.



1. In the left panel of the Main Menu, select the Controllers to which the data will be uploaded.

2. In the Upload section, check the box **Upload Configuration** to if you want to upload the configuration.

3. Check the box **Upload Cards** to if you want to upload the Card Holder information.

4. Click **Upload** button to start the upload process.

5. Click the **Close** button upon completion of the process.

3.3 Download Function

In the Main Menu, the **Download** function allows you to download the transactions logged in the Controllers to the computer.

1. In the left panel of the Main Menu, select the Controllers from which the data

will be downloaded.

2. In the Download section, select **All Undownloaded Transactions** if you want to download the transactions which have not been downloaded before since the last download.

3. Select **Undownloaded transactions between** and enter From/To Data/Time to download the transactions within a particular period.

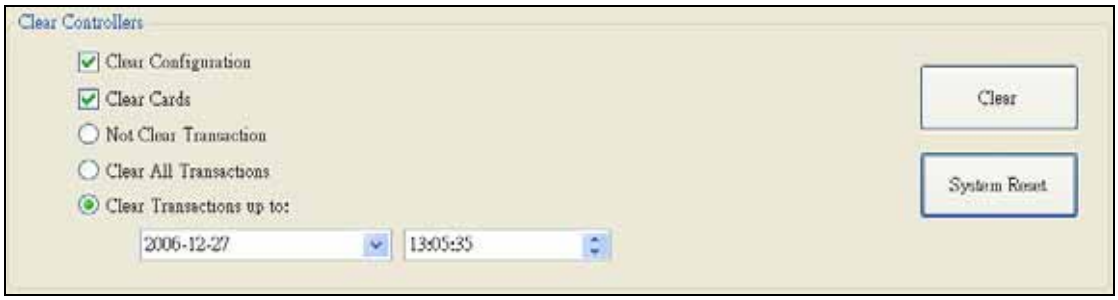
4. Click the **Download Transaction** button to start the download process.

5. Click the **Close** button upon completion of the process.

If transactions already exist in the SAM database, download the same set of transactions to the database will not overwrite the existing data. As a result, duplicated transactions will be kept in the database.

3.4 Clear Controllers

In the Main Menu, the **Clear Controllers** function resets the configuration and/or card holder information and allows you to remove the transaction log in the controllers.



1. In the left panel of the Main Menu, select the Controllers in which the data will be cleared.

2. Check the box **Clear Configuration** if you want to clear the configuration setting.

3. Check the box **Clear Cards** if you want to remove the card holder information.

4. Select **Not Clear Transaction** if you do not want to remove the transaction log

5. Select **Clear All Transaction** if you want to remove the entire transaction log.

6. Select **Clear Transaction up to** and enter the Date/Time if you want to remove transaction log from the beginning to the specified date.

7. Click the **Clear** button to move to the System Reset Screen.

8. Click the **Reset Now** button to start the process.

9. Close the window upon completion of the process.

10. Alternative, you can click the **System Reset** button to clear configuration, card holder information and all the transactions in one go.

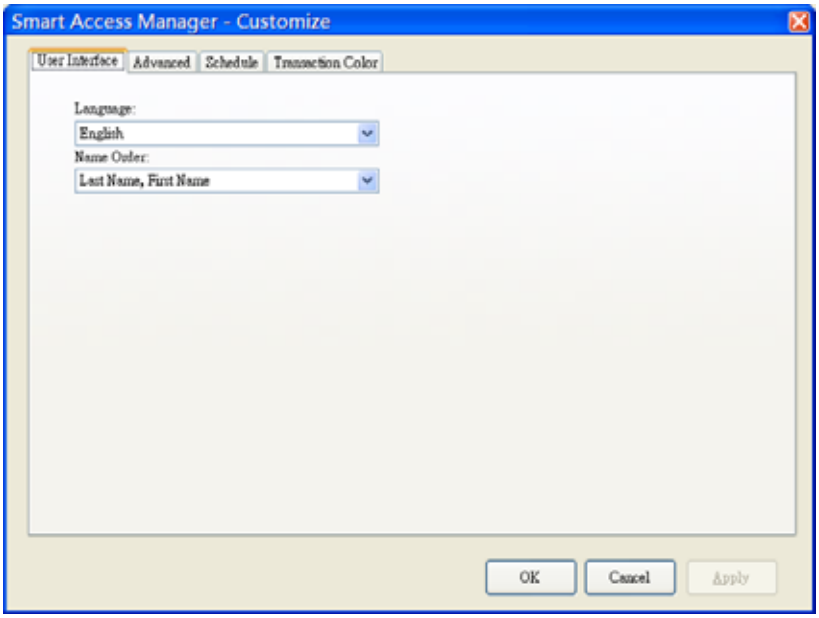
3.5 Remove Transaction

The **Remove Transaction** function allows you to permanently remove the downloaded transactions stored in the database. You can either remove all the transactions or transactions within a particular period. In general, it is not advised to remove transactions in the database. If you come across any database problem and need to run the process, please consult your database administrator or call our support.

3.6 Customize

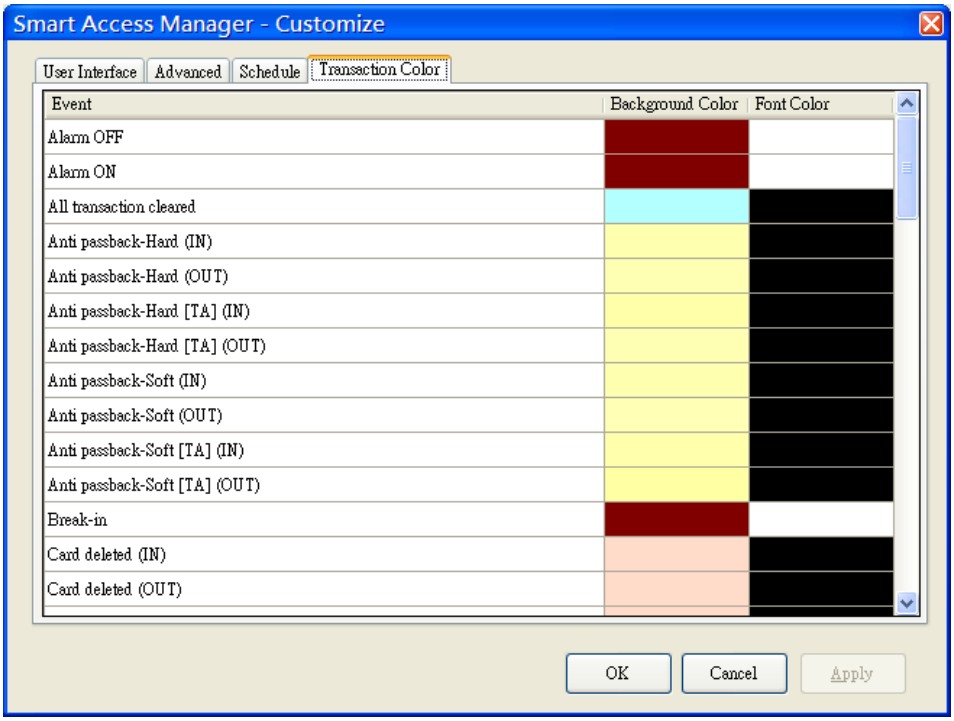
3.6.1 User Interface

SAM provides an option to allow you to select the preferred language interface. The software comes with three languages, namely English, Simplified Chinese and Traditional Chinese. The default is English. If you need other language interfaces than English and Chinese, please call our hotline for further details.



3.6.2 Transaction Color

SAM allows showing the transaction as desired color. For example, a break-in event will show as Red for easier discriminate. Click the Background/Font color on the desired event as show in the following figure:



4 Tools

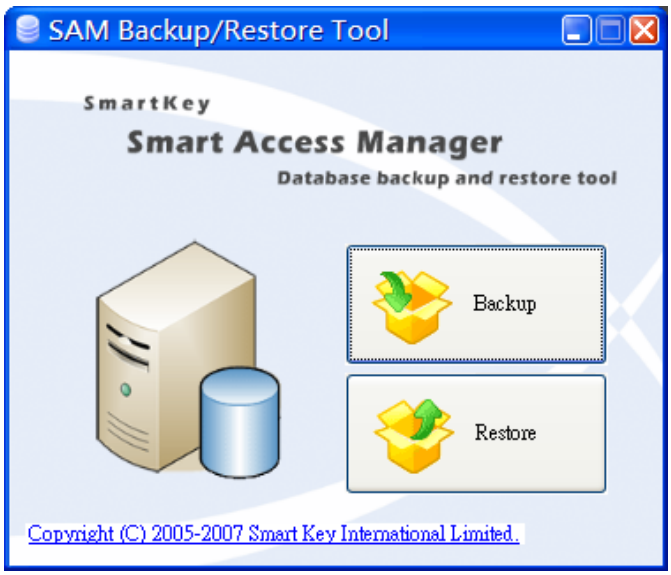
4.1 Backup and Restore Tool


This tool is used to backup the whole database into one file or restore from one file. If you are using MSDE or SQL 2000, you must install the SQL Client and SQL XMO from CD.

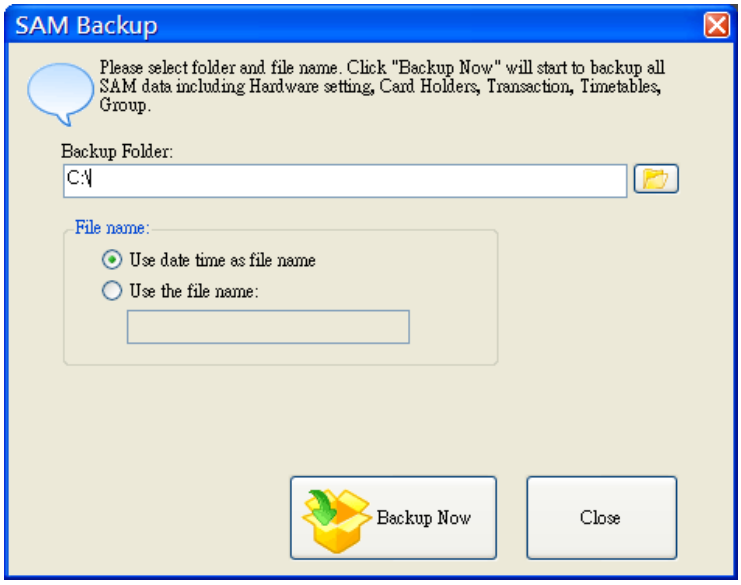
4.1.1 Backup database

1. Execute **Start\Program Files\Smart Access Manager\Backup and Restore Tool**

2. Click Backup button



3. Click  button to select the target folder



4. Click Backup Now button

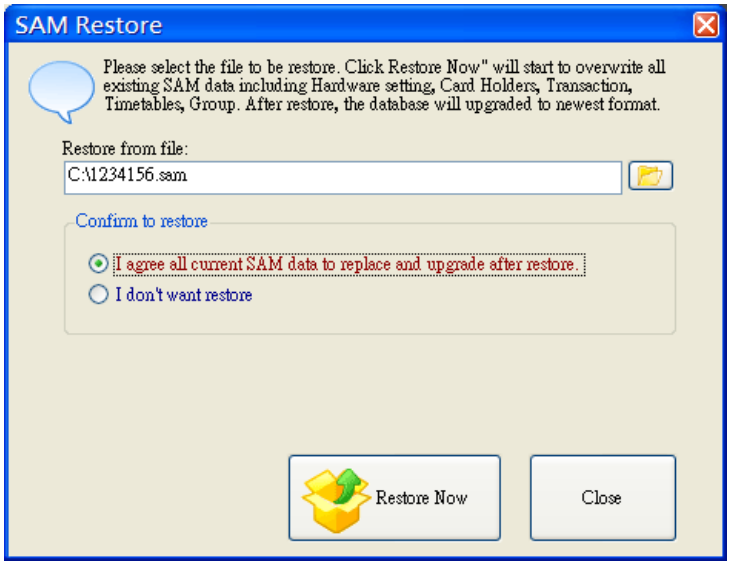
5. When finish, a message will appear

Restore database

1. Execute **Start\Program Files\Smart Access Manager\Backup and Restore Tool**

2. Click **Restore** button

3. Click  button to select the source folder



4. Click “I agree” button

5. Click **Restore Now** button to begin the restore

6. When finish, a message will appear

4.2 Language Translation Tool

This Tool is used to translate the language.

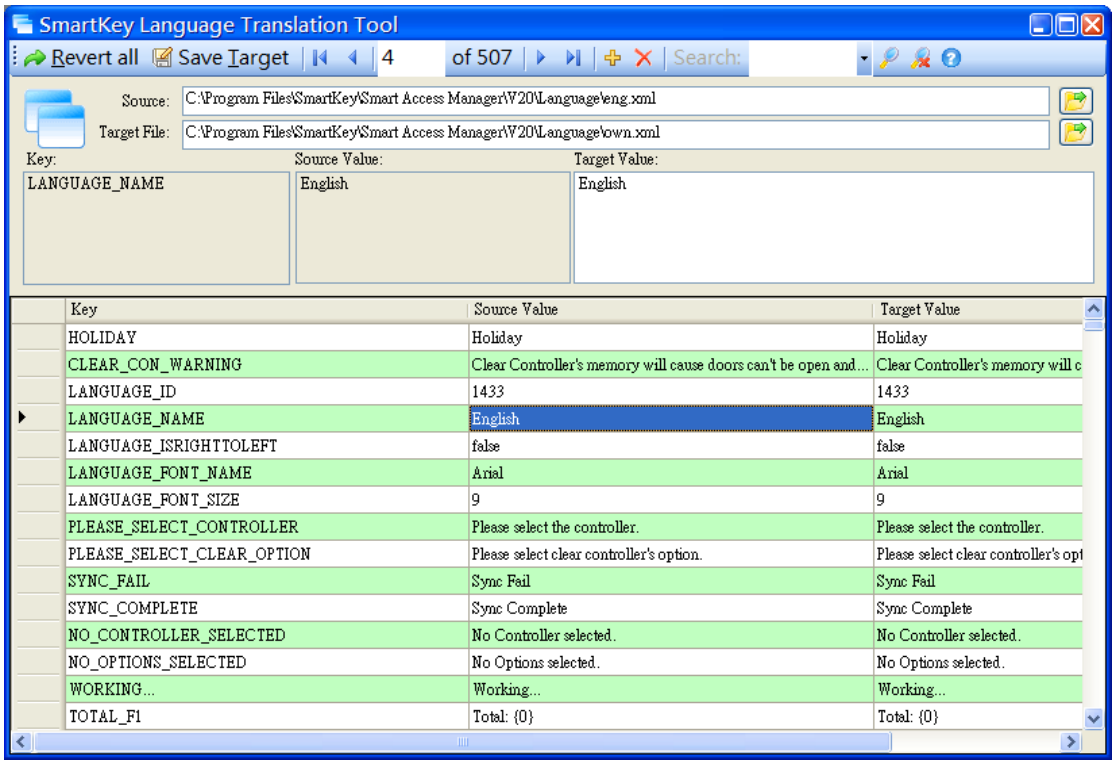
4.2.1 Create Target language file

1. In Windows Explorer, Open the SAM directory at **C:\Program Files\SmartKey\Smart Access Manager\V20\Language**

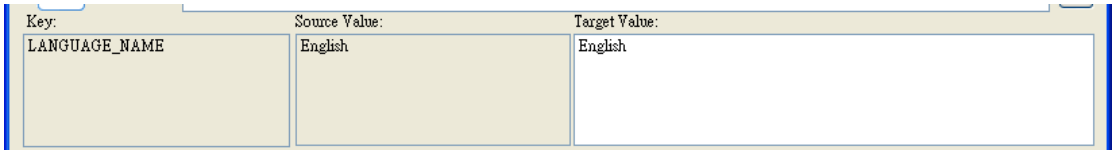
2. Copy a the eng.xml(or other language file) into own.xml(or other name)

3. Execute **Start\Program Files\Smart Access Manager\Language Translation Tool**

4. Click  to select the source and target file as the following



5. Select the row and change the value of Target Value in the box



6. Click **Save Target** button to save the translated file or click **Revert all** to restore the last saved file.

Some field must change:

- *LANGUAGE_ID*
- *LANGUAGE_NAME*
- *LANGUAGE_ISRIGHTTOLEFT*
- *LANGUAGE_FONT_NAME*
- *LANGUAGE_FONT_SIZE*

For the LANGUAGE_ID and LANGUAGE_NAME, it is required to be unique in exist language. The following is the ISO standard language ID:

LANGUAGE_ID	LANGUAGE_NAME
1	Arabic
4	Chinese
9	English
1025	Arabic – Saudi Arabia
1026	Bulgarian
1027	Catalan
1028	Chinese – Taiwan
1029	Czech
1030	Danish
1031	German – Germany
1032	Greek
1033	English – United States
1034	Spanish – Traditional Sort
1035	Finnish
1036	French – France
1037	Hebrew
1038	Hungarian
1039	Icelandic
1040	Italian – Italy
1041	Japanese
1042	Korean
1043	Dutch – Netherlands
1044	Norwegian – Bokmal

1045	Polish
1046	Portuguese – Brazil
1047	Rhaeto-Romanic
1048	Romanian
1049	Russian
1050	Croatian
1051	Slovak
1052	Albanian
1053	Swedish
1054	Thai
1055	Turkish
1056	Urdu
1057	Indonesian
1058	Ukrainian
1059	Belarusian
1060	Slovenian
1061	Estonian
1062	Latvian
1063	Lithuanian
1065	Persion
1066	Vietnamese
1069	Basque
1070	Serbian
1071	Macedonian (FYROM)
1072	Sutu
1073	Tsonga
1074	Tswana
1076	Xhosa
1077	Zulu
1078	Afrikaans
1080	Faeroese
1081	Hindi
1082	Maltese
1084	Gaelic
1085	Yiddish
1086	Malay – Malaysia
2049	Arabic – Iraq
2052	Chinese – PRC

2055	German – Switzerland
2057	English – United Kingdom
2058	Spanish – Mexico
2060	French – Belgium
2064	Italian – Switzerland
2067	Dutch – Belgium
2068	Norwegian – Nynorsk
2070	Portuguese – Portugal
2072	Romanian – Moldova
2073	Russian – Moldova
2074	Serbian – Latin
2077	Swedish – Finland
3073	Arabic – Egypt
3076	Chinese – Hong Kong SAR
3079	German – Austria
3081	English – Australia
3082	Spanish – International Sort
3084	French – Canada
3098	Serbian – Cyrillic
4097	Arabic – Libya
4100	Chinese – Singapore
4103	German – Luxembourg
4105	English – Canada
4106	Spanish – Guatemala
4108	French – Switzerland
5121	Arabic – Algeria
5127	German – Liechtenstein
5129	English – New Zealand
5130	Spanish – Costa Rica
5132	French – Luxembourg
6145	Arabic – Morocco
6153	English – Ireland
6154	Spanish – Panama
7169	Arabic – Tunisia
7177	English – South Africa
7178	Spanish – Dominican Republic
8193	Arabic – Oman
8201	English – Jamaica

8202	Spanish – Venezuela
9217	Arabic – Yemen
9226	Spanish – Colombia
10241	Arabic – Syria
10249	English – Belize
10250	Spanish – Peru
11265	Arabic – Jordan
11273	English – Trinidad
11274	Spanish – Argentina
12289	Arabic – Lebanon
12298	Spanish – Ecuador
13313	Arabic – Kuwait
13322	Spanish – Chile
14337	Arabic – U.A.E.
14346	Spanish – Uruguay
15361	Arabic – Bahrain
15370	Spanish – Paraguay
16385	Arabic – Qatar
16394	Spanish – Bolivia
17418	Spanish – El Salvador
18442	Spanish – Honduras
19466	Spanish – Nicaragua
20490	Spanish – Puerto Rico