Door Entry Systems

Smart Doorphones BVBA
Hodn Fasttel
Klipsenstraat 18A
9160 Lokeren
+32 9 244 65 20
info@fasttel.com

FT9002/4A
Door Access System Controller

Manual
Even called Fasttel DAS

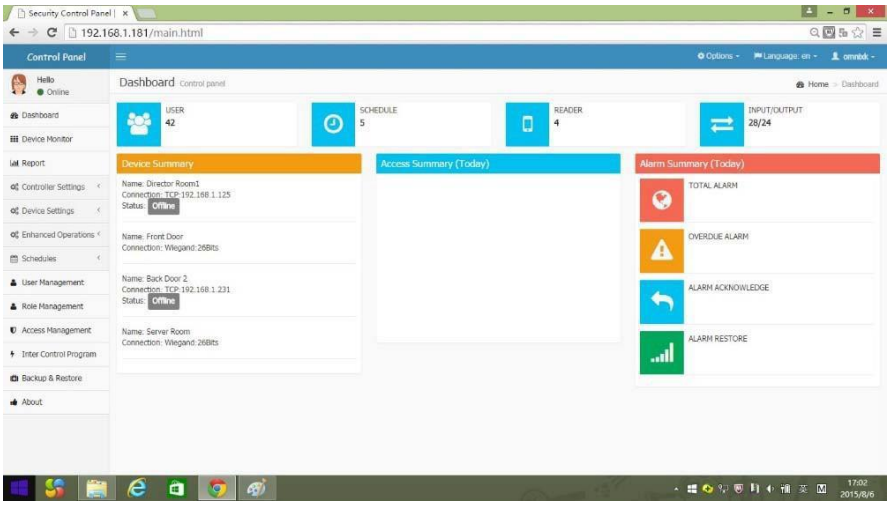
Version 1.01

Content

Dashboard

The Dashboard Page

After login to DAS will lead you to a Dashboard page. This page provides a summary of the controller configurations.



The Dashboard top row shows the nos. of the controller respective database configuration.
In above example the User is 42, it means there are 42 users records in the controller user database.
Schedule is 5 means there are 5 schedules setting in the schedule database.
Likewise for Reader and Input/Output records.

When move the mouse to click on the respective box it will bring you to the respective menu to see the details.

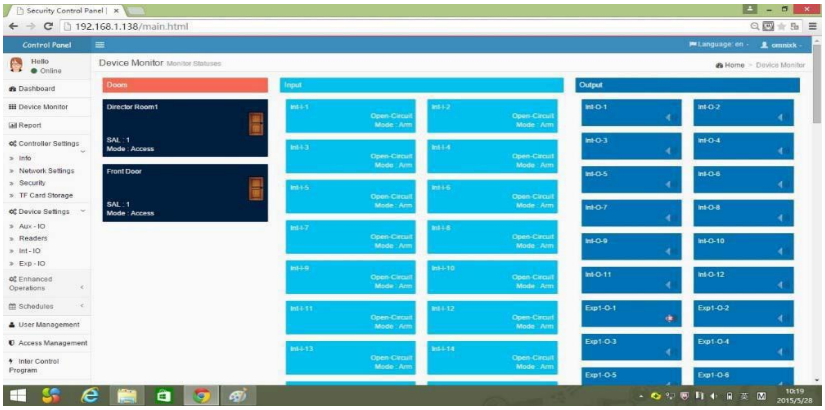
The Door Summary shows the configure door[card reader] name, it connection type, and the status. The Access Summary(Today) shows the access nos. of the door[card reader] in this controller. The Alarm Summary(Today) indicates the alarm occurred in today,

Device Monitor

The Device Monitor Page

In Device Monitor Page, authorized administrator will be able to perform manual operations to Door, input and output to change their operation mode.

In this page you can see 3 column groups.
1st column is the Door [which is also known as card reader],
2nd & 3rd column is Input point and
4th & 5th column is Output point.



Depends on the controller type, the Device Monitor page are different.
In above example it show the FT9002A-IO controller page which is a FT9002A integrated controller. The FT9002A-IO can support 2 doors plus 14 input points and 12 output points.

If it is FT9002A controller then you can only see 1st column with 2 door ICON. If it is a FT9004A controller then you will see 4 Door ICON box. However if the FT9002A or FT9004A or FT9002A-IO is connected with EXP-IO board you will see a whole list of Inputs and Outputs according to the nos. of EXP-IO board.

When move the mouse to the respective ICON box and right click, you can change the operation mode of the respective device.

Operate on Door ICON

Below example illustrate the Door right click menu:

The right click menu will give you control of the following:

Unlocking a Door Temporarily

Via the [Remote Unlock] menu, user can remote unlock the door for a pre-define seconds define under the Door lock properties. After the pre-define seconds the door will back to its lock condition.

Locking a Door Manually

Via the [Locked] menu, user can change the Door[Card reader] mode to Lock mode, this will make the door into lock condition and not allow any authorize user access.

Unlocking a Door Manually

Via the [Free Access] menu, user can change the Door[Card reader] mode to Free Access and it remain unlock until:

- An operator manually change the Door mode;
- The next change of mode via the schedule;
- The event action designated in Inter-Control Program definition;

Change to Access Mode

Via the [Access] menu, user can change the Door[Card reader] mode to Access mode and make the card reader to accept using only One verifying source either by Card or Fingerprint.

Change to Secure Mode

Via the [Secure] menu, user can change the Door[Card reader] mode to Secure mode and make the card reader to accept 2-factor authentication, either by Card+PIN or Card+Fingerprint or Fingerprint+PIN.

Change to Supervised Mode

Via the [Supervised] menu, user can change the Door[Card reader] mode to Supervised mode and make the card reader to accept 2 user cards or 2 user fingerprints to verifying the authorization. The criteria of 2 user cards or 2 user fingerprints will depends on the setting.

Change to Increase SAL Security

Via the [Increase SAL] menu, user can instant raise the Door[Card reader] security level and only accept user with access level rights equal or higher than it before verifying it authorisation. The highest SAL is 16.

Change to Decrease SAL Security

Via the [Decrease SAL] menu, user can instant downgrade the Door[Card reader] security level and accept user with access level rights equal or higher than it before verifying it authorisation. The minimum SAL is 1.

Restore of DOTL

Via the [DOTL Restore] menu, user can instant restore the DOTL alarm to silent the reader's buzzer beeping sound.

Operate on Input
ICON

Below example illustrate the Input right click menu:

Change to Arm mode

Via the [Arm] menu, user can instant modify the input point into arm mode. An arm mode is putting the input into monitoring condition.

Change to Disarm mode

Via the [Disarm] menu, user can instant modify the input point into disarm mode.

A disarm mode is putting the input into ignore condition.

Restore Alarm

Via the [Alarm Restore] menu, user can instant silent the alarm event and restore it to normal condition if the alarm condition is rectify.

.

Operate on Output ICON

Below example illustrate the Output right click menu:

Change to Trigger On

Via the [Trigger On] menu, user can instant trigger ON the relay output, the triggering duration or mode will depends on the output properties setting.

Change to Trigger Off

Via the [Trigger Off] menu, user can instant trigger OFF the relay output, the triggering duration or mode will depends on the output properties setting.

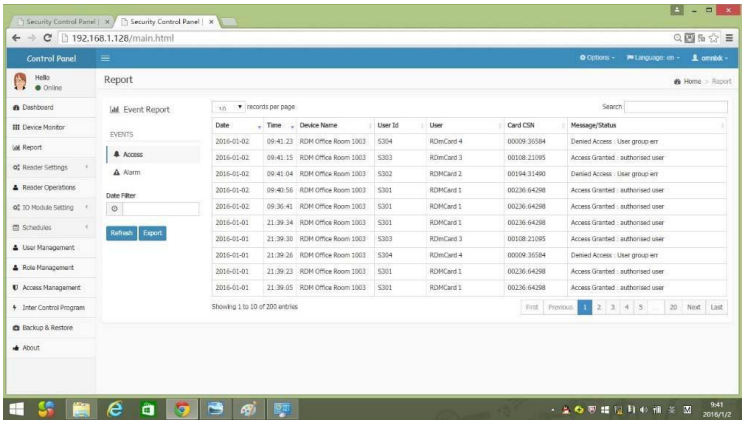
Report

DAS provides simple report and allow it to export in excel format or pdf format. There are 2 types of reports: Access and Alarm.

To get a comprehensive report and better analyzing result, it is advise to use Cloud platform software.

Access Report

DAS Access Report is also known as event report. It record the timestamp of each access event occurred in this controller. Such event includes access granted, access denied, etc…



1. Schedules

1.1 Schedules Definition

Schedule is configure to enabling the system to execute desire operations such as permitting time access to employee, automatic lock or unlocking doors, zone arming or disarming, change of reader operating mode, etc. The Schedule is also use to determine when to arm or disarm an input or activate a relay output controlling a special function (such as motor, liftcar).

DAS provide 2048 weekly schedules for different devices/user and you can create different schedule for each application for easy assigning and modifying to a particular schedule. These devices/user includes:

1) Reader
2) Input
3) Output
4) Elevator
5) User
6) System

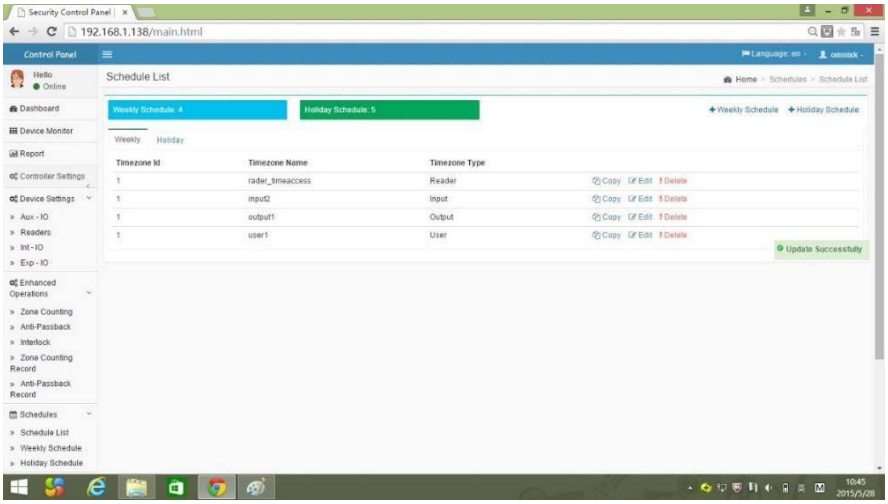
DAS already factory default each devices/user with a 24 hour schedule. You can modify it as well as create more of different schedule to these devices/user. At the moment, System is not in used.

Each weekly schedule is composed of six intervals with a starting and ending time and seven days of the week. Each of these intervals can be individually configure for the desire mode. Each weekly schedule includes 2 holidays know as Public holiday and Special Holiday.

Defining a Schedule

Click on the [SCHEDULE] menu and you can see the page below. It consists of 2 tabs, the weekly schedule list & the holiday list.

Click on the top right “+ Weekly Schedule” to add schedule or click on the “+ Holiday schedule” to add hoiday definition.



Copy a Schedule

If you want to add a new schedule is quite similar or the same as one of the schedule in the listing, just click on the “Copy” icon and it will show the schedule for you to enter a new schedule name, save it and it will become new listing.

Edit a Schedule

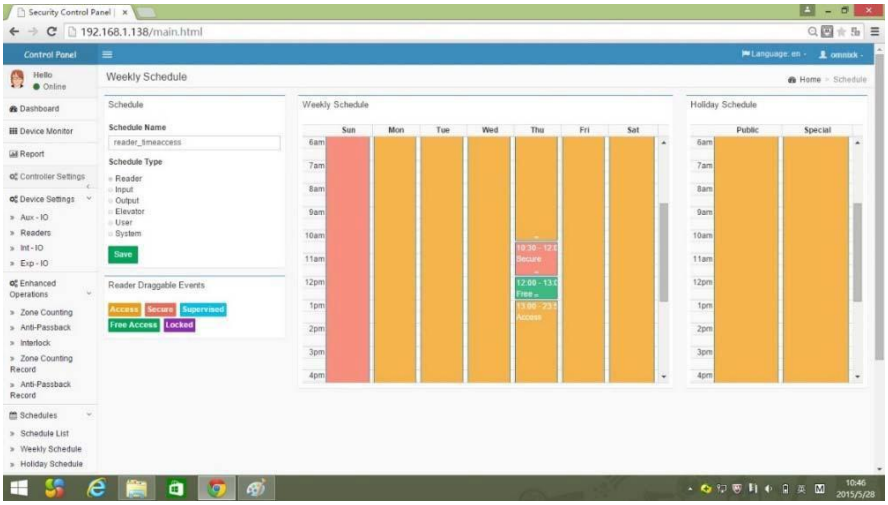
To edit an existing schedule just click on the “Edit” icon and it will show the schedule for you to edit, save it and it will successful change.

Delete a Schedule

To delete an existing schedule just click on the “Delete” icon and it will remove from the schedule list, note that once this schedule is deleted, and users or devices using this schedule will be diverted to its respective 24hour schedule.

Add a Schedule

Click on the top right “+ Weekly Schedule” and you can see this page below.



1. Enter a Schedule Name.
2. Select the schedule type.
3. From the Draggable Events box select the mode function, drag the function box to the desire day column and expand to the desire time hours. Repeat from Sun to Sat column.
4. Repeat to the Holiday Schedule for Public and Special holiday column.
5. Press Save button. It will save the setting and back to the listing UI.

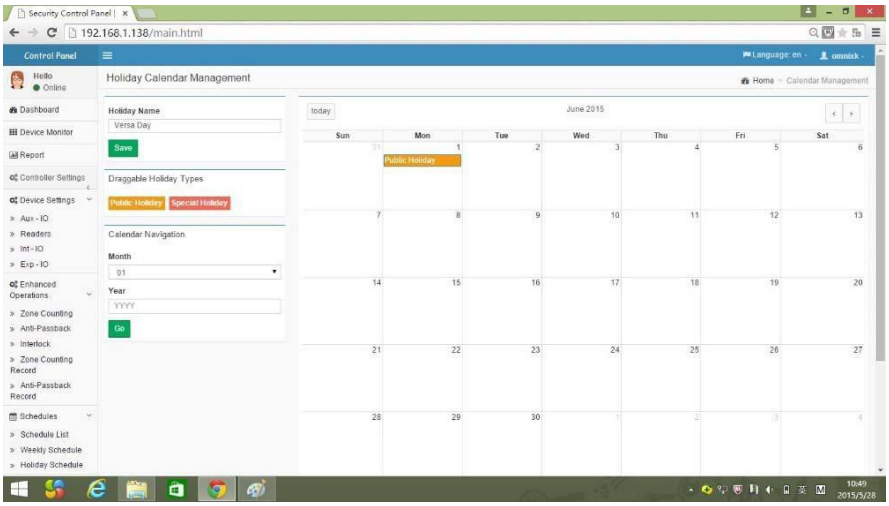
NOTE 1: *DAS Schedule supports drag and drop operations and for simplicity it is only precise in 30 minutes timeslot. If you need to define more specify time, eg. 0810-1220, please use the Cloud software to define and download.*

NOTE 2: *DAS Holiday Schedule will override the operation of the day schedule if the day is define as Holiday. But You need to define the holiday date in "Weekly Holiday"..*

Holiday Definition

You are recommended to define Holiday date at the beginning of the current year in the "+Holiday Schedule". The Holiday is use to override the normal calendar days when come to access control function.

Holiday is classify into 2 types: Public Holiday which is known as national designated holiday and Special Holiday is known as exception event rest day, eg. Company anniversary day or extra off-day.



Add a Holiday Date

Click on the top right "+ Holiday Schedule" and you can see this page below.

1. Enter a Holiday Name.
2. From the Draggable Holiday Type box, select the holiday to the cablendar date. If it is more than 1 day, drag the box to the desire date.
3. Press Save button. It will save the holiday setting and back to the listing UI.

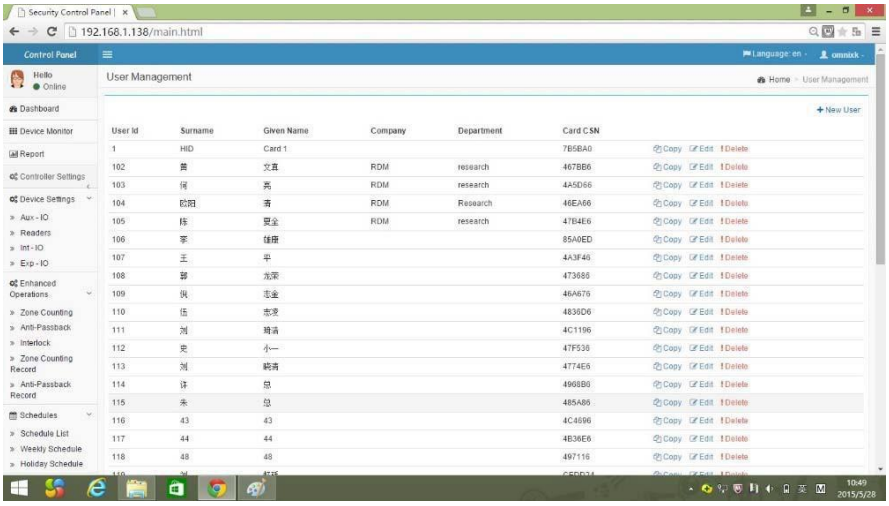
NOTE 1: *DAS Holiday page is to define only ONE holiday name. You need to add more holiday for different date.*
You will also need to separate the public holiday with special holiday.

NOTE 2: *DAS Holiday Schedule allows you to set more than ONE year calendar, you can set for the current year, current year+1, current year+N, etc.*

User Management

The Users Management Menu

Click on the User Management will first see the listing page showing the available user register in this controller.



Note that if you are using Cloud software you should enter these data in Cloud and it will download to the controller. If Cloud already downloaded you should see a complete User listing.

Add New Users

Click on the [+New Users] at the top right hand will allow you to register new user It will give a user multiTab frame for you to enter.

NOTE 1: *DAS user multiTab frame provides comprehensive data field for you to fill in, most of these fields are options and may not require to fill in. However, below are mandatory field you need to fill in:*

- User ID
- Surname
- Given name
- Alias
- Card info
- Access Rights:

Copy User

Click on the [Copy] icon at the user list will allow you to copy some of the existing user properties for use in a new User data, you will need to enter the new user name, issue new card and validity and change the user personnel record, etc.

Edit User

Click on the [Edit] icon at the user list will allow you to edit the selected user prop erties, such as company info, role, SAL, card issue, etc.

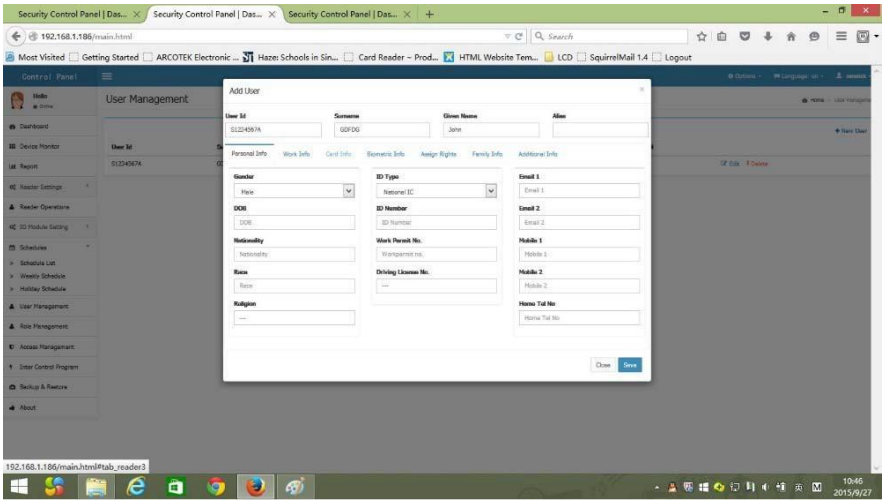
Delete User

Click on the [Delete] icon at the selected user list will allow you to delete the user record from the controller.

NOTE 1: *When a user deleted it will no longer resided in the controller, you will need to re-enter the user particular if wrongly deleted.*

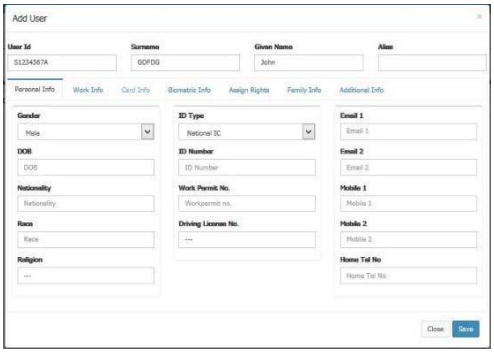
Users Data

Below is the user multiTab frame screenshot. You can see there are 7 tabs to fill inn.
regardless of which tab you select, the top portion is remain as User ID and Use r name.



Personal Info Tab

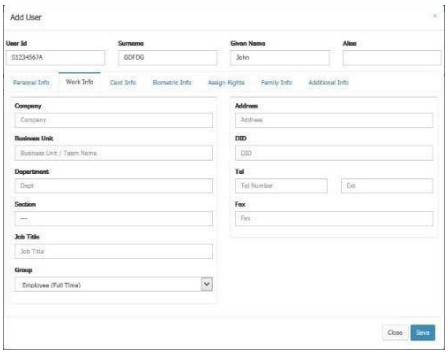
The fields inside this tab is optional.



If you have Cloud it should already fill in these fields. However if you are direct access via DAS you can ignore these fields but it is good practice to enter it as your office personnel record.

Work Info Tab

The fields inside this tab is optional.

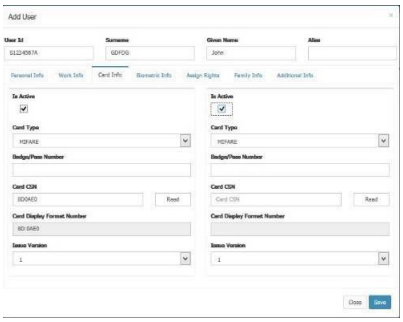


If you have Cloud it should already fill in these fields. However if you are direct access via EzPass you can ignore these fields but it is good practice to enter it as your office personnel record.

The work info is particular useful if the building is occupy with multi-tenants of a co rporation or different companies and these employee are giving an access cards to access the main door, Flapgate or Liftcar, so with the work info data it can easily identify the cardholder is employ in which company or business unit.

Card Info Tab

The fields inside this tab has to fill in if the user is issue card for access to door.



If you have Cloud it should already fill in these fields. However if you are direct access via DAS you need to tick on the Card 1 or Card 2 to assign a card to user and fill in the mandatory fields.

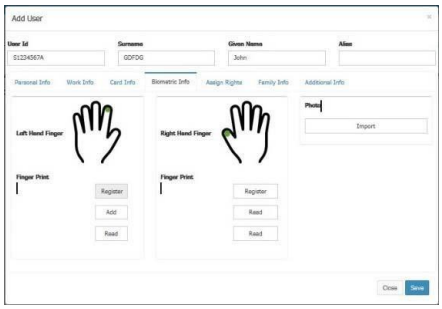
DAS allow each user to hold 2 cards so give convenience to the user to enter premises where in some cases the building is equipped with old format card reader and new card readers. For example, one card can be 13.56MHz (Type A/B) card and the other can be 125KHz (prox) card.

DAS also provides a quick card detection method, instead of key-in the card CSN, when click on "Read" button, place a card to the reader, it will auto-read the card CSN and fill in.

NOTE 1: *Card CSN is unique to a card and sometimes is not display on card surface, so using "Read" button is the quickest way to read out the card CSN.*

Bio Info Tab (version 2023)

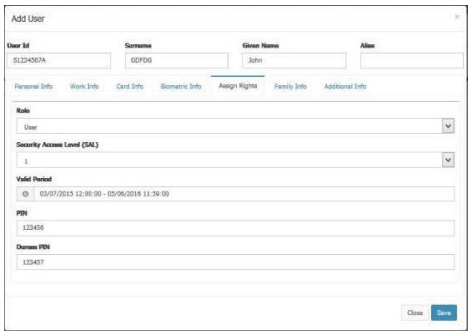
The fields inside this tab has to fill in if the user is using Fingerprint card reader for access the door.



If you are using Type D card reader which is also a TCPIP card reader, Cloud can directly download the fingerprint template into Type D reader. However, if you are using RS485 card reader in OSDP protocol connect to FT9002A/FT9002A-IO/FT9004A controller, then these fingerprint template will download to the controller, and later via OSDP protocol download to fingerprint card reader.

Type D reader allows direct enrollment to user fingerprint template.

Access Rights Tab

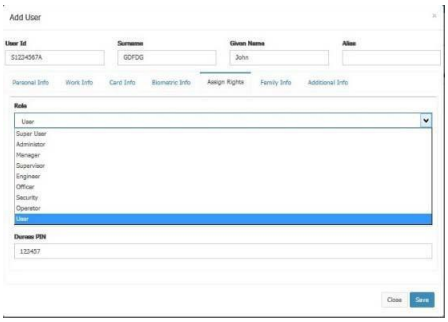


The fields inside this tab has to fill in so that the user will have common access rights criteria regardless if he or she is issue card or fingerprint for access to door.

The Access Rights is to define the user Role functions, Security Access Level, Valid Period, PIN and Duress PIN.

If you have Cloud it should already fill in these fields. However if you are direct access via EzPass then you need to fill in all the fields.

Access Rights - ROLE



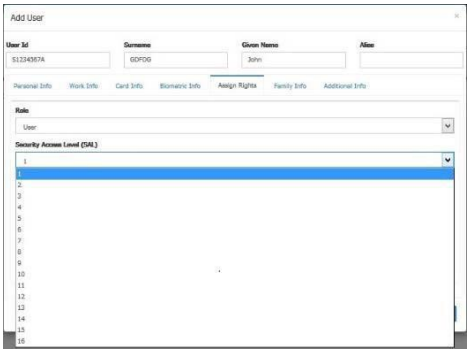
This role is useful to the Admin to assign each user a role. EzPass designed 9 roles

- Super User
- Administrator
- Manager
- Supervisor
- Engineer
- Officer
- Security
- Operator
- User

For typical user (or known as cardholder) you can assign them as [User] role just to access the door and not authorize to login to control the system or controller. For user that authorized to operate or control the system or controller you can assign the other role to them.

DAS provides a simple Role Management menu to allow configure of user Role to the system function. Details please refer to Role Management menu.

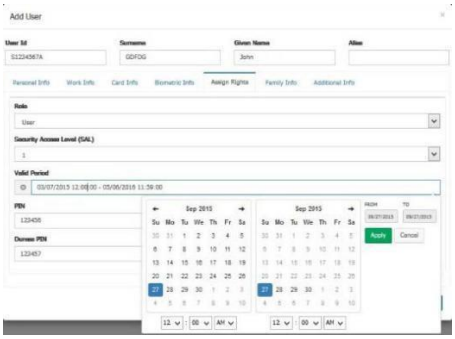
Access Rights - SAL



The SAL is known as Security Access Level and define from 1 to 16 level. Each user is to assign a SAL level. This SAL is to use in door access where the door reader will verify if the user SAL is equal or higher before granting access into the door.

Note that the SAL is a very useful feature since it can easily modify the security criteria to a particular door or door group during critical period. For example, if a door reader is define as SAL=1, and user is SAL=1 for normal operation, however in some occasion when the door is to block access to some users, you can increase the door SAL=2 via [Reader] properties page, or via Device Monitor [Door] reader icon. Once change, those user with SAL=1 will denied access to this door.

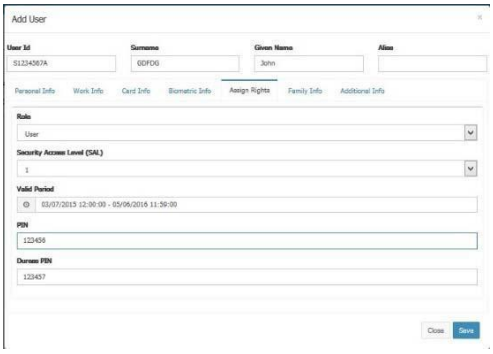
Access Rights – Valid Period



Each user should give a time period known as validity period. This is to define the user card or user fingerprint is valid from [Start date:Start Time] to

[End date:End Time]. Please ensure you enter the correct validity period to avoid denied access to the user.

Access Rights – PIN & Duress PIN



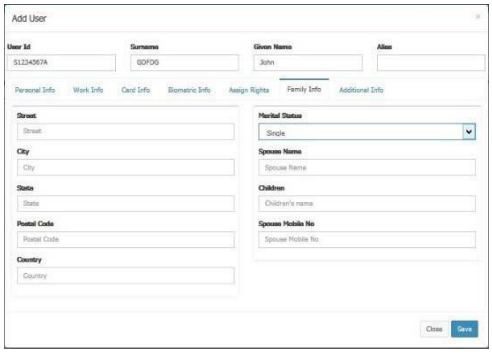
Each user should give a 4-digit PIN & Duress PIN, both PIN should not be identical. It is also advise to have different PIN for different user.

The PIN or Duress PIN will be used when door reader is define as [Secure] mode.

NOTE 1: *If Duress PIN is press and activated, it will still grant access to the user with a Duress Message send to Cloud. If the controller is connected with IO to siren (in the security control room), it can also activate the siren to alert the security officer.*

Family Info Tab

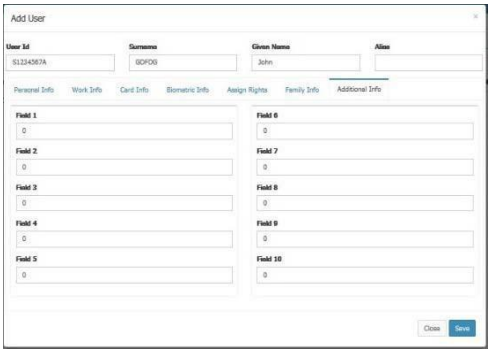
The fields inside this tab is optional.



If you have Cloud it may already fill in these fields. However if you are direct access via DAS you can ignore these fields but it is good practice to enter it as your office personnel record. For example a tel contact nrs for next of kind during emergency.

Additional Info Tab

The fields inside this tab is optional.

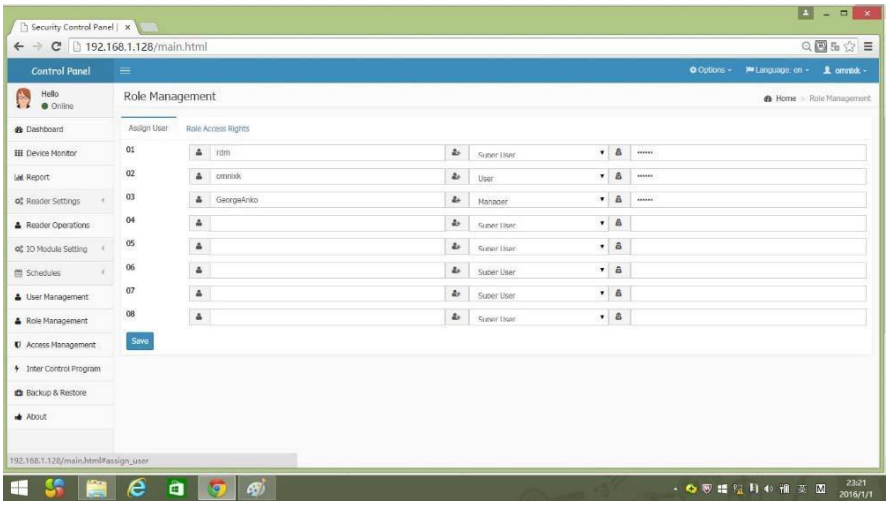


If you have Cloud it may already fill in these fields. However if you are direct access via DAS you can ignore these fields but it is good practice to enter it as your office personnel record. The additional field allow you to enter particular info such as user's car type, car plate license, interest, etc.

Role Management

Role Management Menu

Click on the Role Management will first see the [Assign User] tab as shown below.

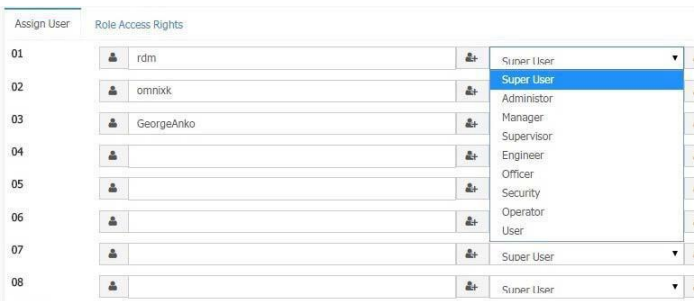


Assign User
You can enter a user name, password and his/her role A confirm role user can then use his/her username, password to log in DAS directly via browser.

Note that if you are using Cloud software you should perform the role assigning in Fine Cloud and it will download to the Controller or Reader. For simple installation without Cloud and only direct access via browser the role assigning is limited to 8 operating user only.

NOTE 1: *Since DAS is accessing via browser and only to One controller or One reader at any one time, so it is only limited to 8 operating users and the assigning rights is much simpler. If you need more complex user rights assigning would have to use Cloud.*

Assign User - Role

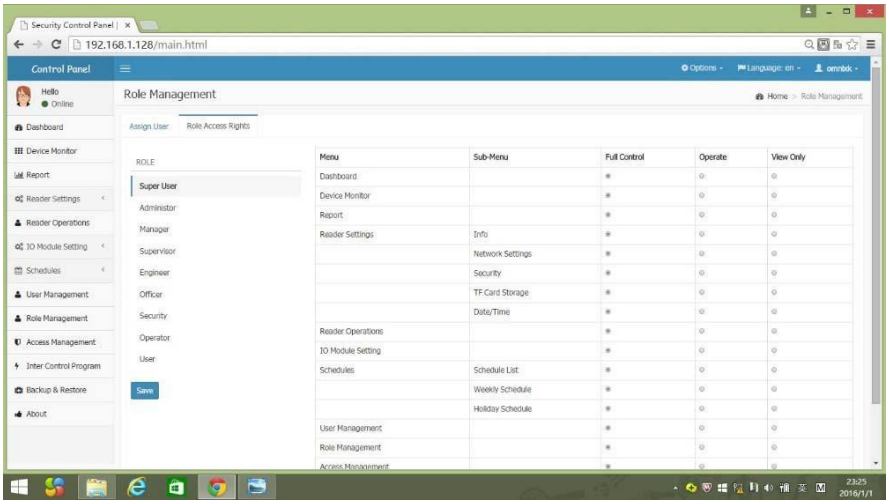


The role pull down choice is similar to the User Management defining a user on his/her role. DAS provides 9 roles

- Super User
- Administrator
- Manager
- Supervisor
- Engineer
- Officer
- Security
- Operator
- User

Role Access Rights

After giving a user role, Click on the "Role Access Rights" will show you the authorize functions assign to user role.



This page show the controller or reader menu & sub-menu with 3 choices

- Full Control
- Operate
- View Only

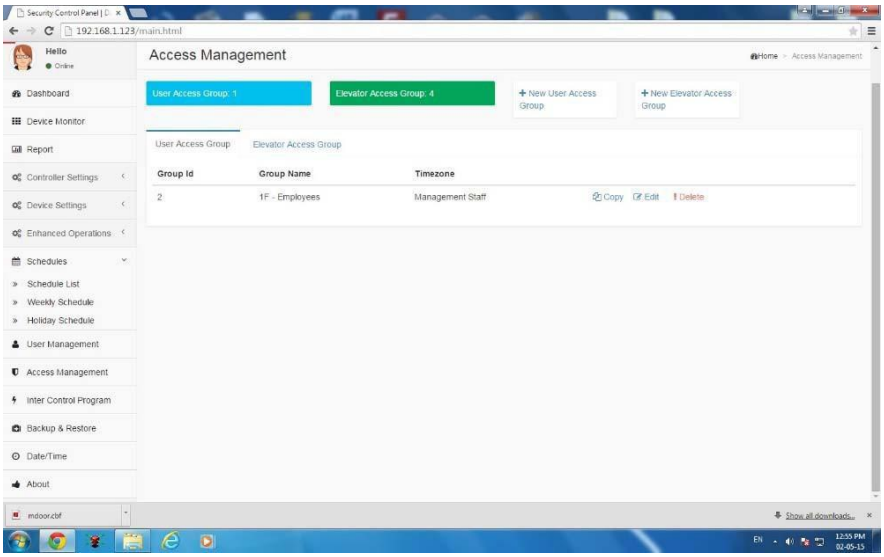
You can select the correct operating choice to the user role.

Access Management

Access Management Menu

Click on the Access Management menu will see the page as shown below. This menu is for you to assign the user authorization to access the door or elevator floor level. User Access Group is to assign user to doors, and Elevator Access Group is to assign user to Elevator floor.

Before you continue on this access management, please ensure you have already configure the Door[reader], schedule and user.

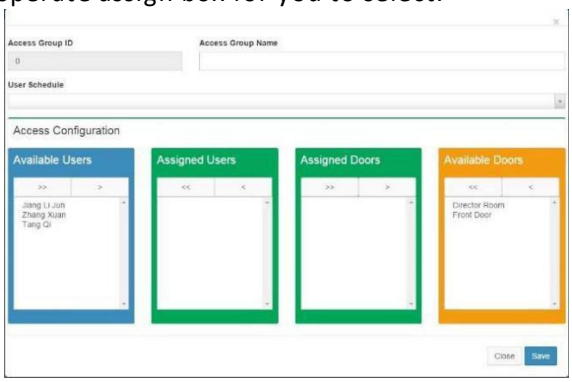


User Access Group

This show the list of user access groups (UAG).

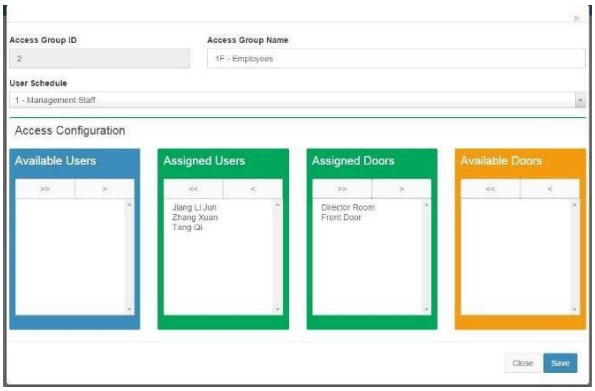
Add New User Access Group

Click on the [+New User Access Group] will allow you to register new user access group. It will give an easy operate assign box for you to select.



Available Users refer to registered user in the controller or reader. Available Doors is refer to the Door[readers] connected to this controller or the reader itself.

1. Enter an Access Group Name, it is advise to give a meaningful name example like Office Staff {08:30-17:30}, Management Staff {24hr}, 3rd Production Group {13:00-21:00}, R&D section {09:00-19:00}, etc.
2. Select a suitable schedule, the schedule will be a complete list configure as Reader schedule.
3. Select the user from the Available User Box, click on [>] to move to Assigned Users Box. Repeat till user assigned complete. If require to move all users just click on [>>] to move all.
4. Select the Door from the Available Doors Box, click on [<] to move to Assigned Doors Box. Repeat till doors assigned complete. If require to move all doors just click on [<<] to move all.
5. The result should be as follow.



6. Press Save button. It will save the setting and back to the listing UI.

Copy User Access Group

Click on the [Copy] icon at the UAG list allow you to copy the existing user access group, you will need to enter the new user access group name, schedule and save it.

Edit User Access Group

Click on the [Edit] icon at the UAG list allow you to edit the selected user access group, etc.

Delete User Access Group

Click on the [Delete] icon at the UAG list allow you to delete the user access group record from the controller or reader.

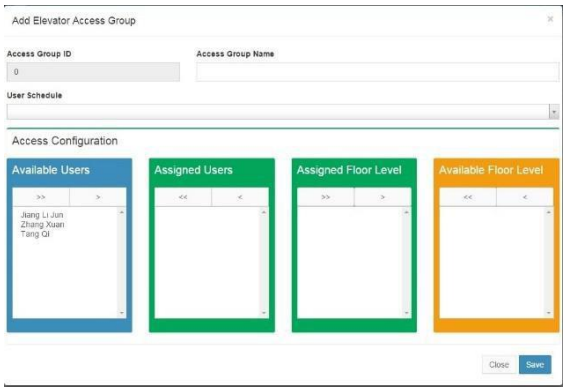
NOTE 1: *When a user access group deleted it will no longer resided in the controller, you will need to re-enter the user access group if wrongly deleted.*

Elevator Access Group

This show the list of elevator access groups.

Add New Elevator Access Group

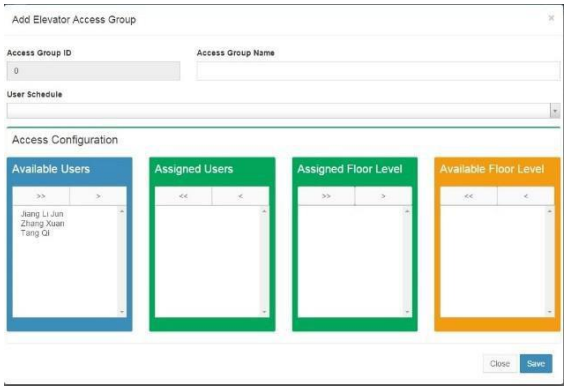
Click on the [+New Elevator Access Group] will allow you to register new elevator acc ess group. It will give an easy operate assign box for you to select.



Available Users refer to registered user in the controller or reader. Available Floor Level is refer to the either the INT-IO board or EXP-IO board Output point connected to this control ler.

Also to note is if this controller is use for Elevator control, it is best to have it connected to ONE reader and define in Reader 1.

1. Enter an Access Group Name for Elevator Access Group, it is advise to give a meaningful name example like Office Staff {08:30-17:30}, Management Staff {24hr}, 3rd Production Group {13:00-21:00}, R&D section {09:00-19:00}, etc.
2. Select a suitable schedule, the schedule will be a complete list configure as Elevator schedule.
3. Select the user from the Available User Box, click on [>] to move to Assigned Users Box. Repeat till user assigned complete. If require to move all users just click on [>>] to move all.
4. Select the Door from the Available Floor Level Box, click on [<] to move to Assigned Floor Level Box. Repeat till doors assigned complete. If require to move all Levels just click on [<<] to move all.
5. The result should be as follow.



6. Press Save button. It will save the setting and back to the Access Management listing UI.

Copy Elevator Access Group

Click on the [Copy] icon at the UAG list allow you to copy the existing elevator access group,you will need to enter the new user elevator access group name, schedule and save it.

Edit Elevator Access Group

Click on the [Edit] icon at the UAG list allow you to edit the selected elevator access group, etc.

Delete Elevator Access Group

Click on the [Delete] icon at the UAG list allow you to delete the elevator access group record from the controller or reader.

NOTE 1: *If FT9002A/FT9002A-IO/FT9004A is use for elevator controller, the elevator reader will connect to reader port 1, and do not connect the extra reader port for door access. It should be dedicated to elevator controller only.*

Inter-Control Program

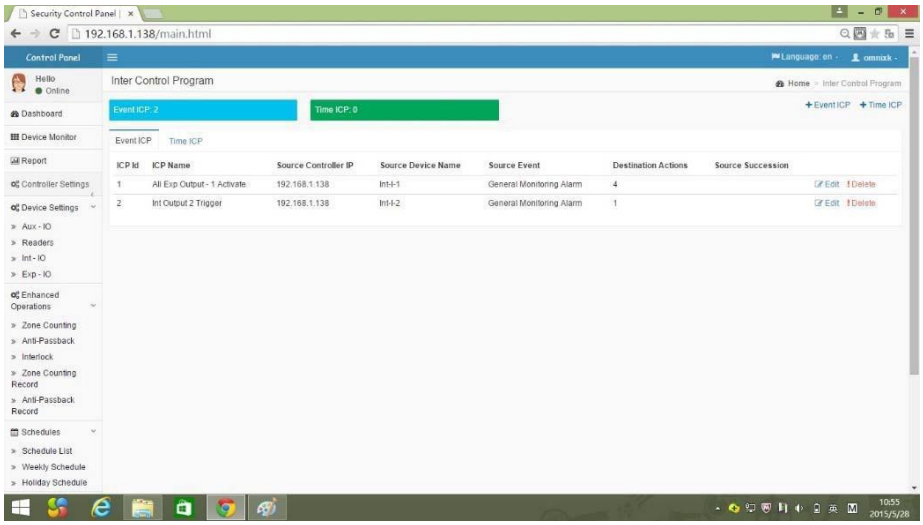
Inter-Control Program Menu

Inter-Control Program (or known as ICP) is a unique logic function to match source and destination function. It is a useful and powerful function to cater for small to large installation needs.

DAS allows you to define any available source event and activate a set of destination for actions. Not only it can define within its own controller actions, it can also provide peer-to-peer control to another controller or group of controllers without intervention of Cloud.

Note that Each ICP, regardless of Event ICP or Time ICP is allowing to configure upto 8 destination action. However, it can use Succession to extend to another 8 actions making it a total 16 actions for one event ICP or one time ICP.

When click on the Inter-Control Program menu, it will show a listing page and there are 2 tabs, Event ICP & Time ICP.



Event ICP

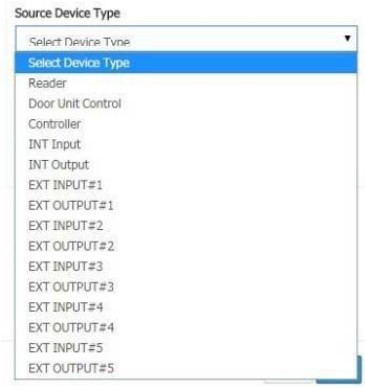
This show the list of event ICP. Above UI show that there are 2 event ICP. Press “Edit” to make changes to existing ICP, press “Delete” to delete the ICP.

Add New Event ICP

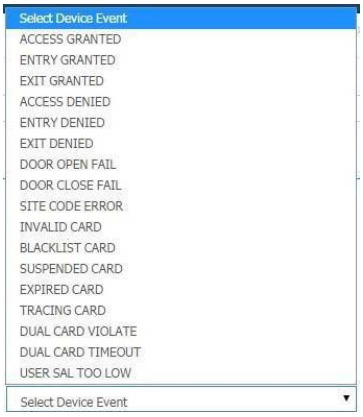
Click on the [+ Event ICP] will allow you to configure the event to action task.

In this example we illustrate how to configure a source event cause by Reader when the user card is Access Denied at the Front Door.

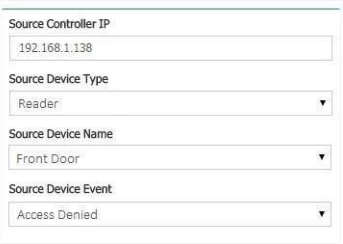
1. The ICP ID is auto generated.
2. Enter an ICP name, it is advised to give a meaningful name example like Access Denied switch on 3rd level Siren, etc.
3. Source Controller IP should be similar to existing controller IP.
4. Source device type is to select the device that are to cause the event, a pull down list show there are Reader, Door Unit Control, Controller, Input & Output, etc. In this example we choose Reader



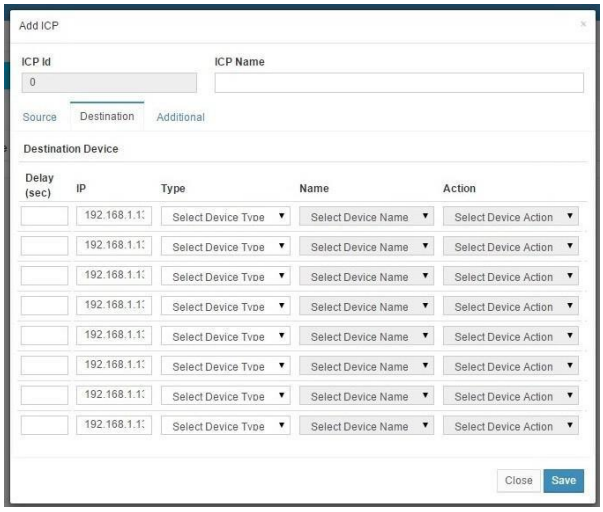
5. After select the Reader, on the Source Device Name pull down list to select the desire door.
6. After select the door, from the Source Device Event, select an event for the ICP, as follow:



7. The result should be as follow.

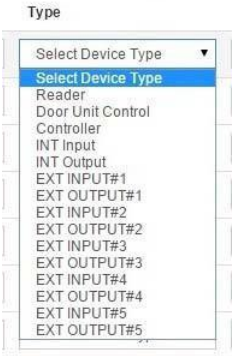


After configure the event, we now configure the Destination which is known as defining the action.

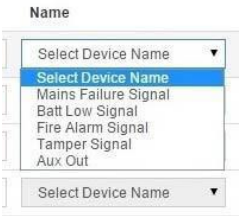


1. Enter an IP address.

2. At the Type, select the Device Type, note that the INT-Input & INT-Output are only available if the FT9002A-IO is in use, and Ext-Input & Ext-Output are only appear if FT9000EXP-IO module in use, in here we select the Controller.

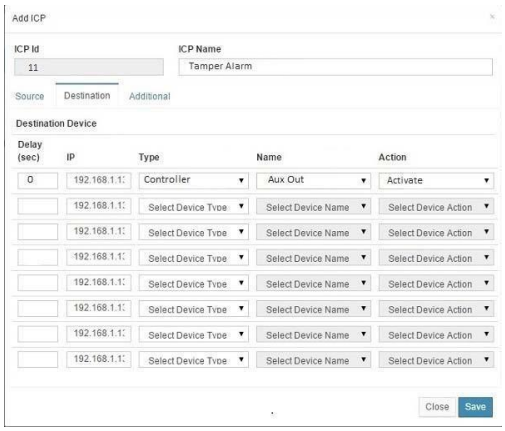


3. At the Select Device Name select the desire output action device, in this example we select the Aux Out:



4. Destination Action field is to select the desire action of the select devices.

Since device is selected as Aux Out, then the action can only be Activate or Deactivate.



5. The final result as shown above.

From above ICP screen shot, it is easy to configure to define any event to cause an action.

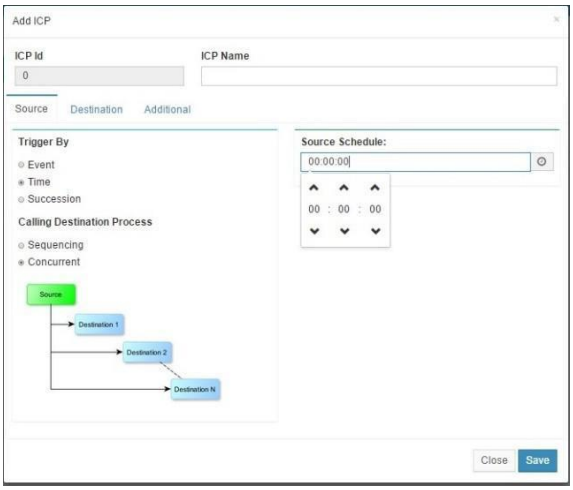
Note that once the ICP event-action occurred, one need to reset manually to change to normal status. You can do it via the Device Monitor panel, or via another ICP to deactivate it, or via the respective device parameter.

Time ICP

The Time ICP is quite similar to the event ICP except it occur base on time setting.

Add New Time ICP

Click on the [+ Time ICP] will allow you to configure the Time to action task.

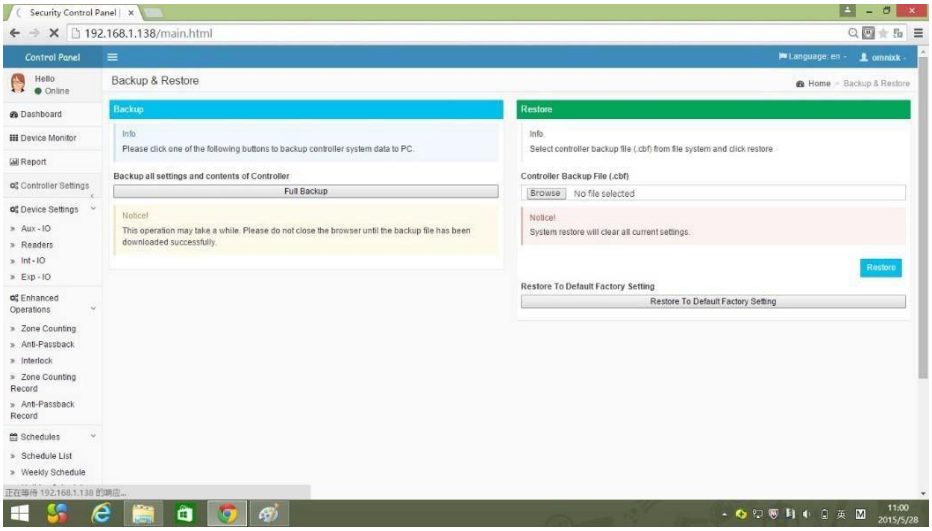


After the time set, go to Destination and configure the device type and desire actions.

Backup & Restore

Backup Menu

Click on the Backup menu you can see below page. This menu allow you to backup the database and restore it. For example, if you have 2 or more controllers and you have configure controller IP:192.168.1.11, then you can backup the database, and when you goto controller IP: 192.168.1.12, you can restore the same file (backup from 192.168.1.11) to the 192.168.1.12 controller so it can be the same setting.



Once you press Backup, please note that the prompt notice is appear at the bottom left bar, the backup will also take some time before it can fully backup.

A backup file is known as “*.cbf”, when you wanted to Restore to its own controller or another controller, at the Restore column, browse and select this “*.cbf” file, then press Restore button.

If you want to return the controller to factory default setting, press the “Restore to Factory Default Setting” button.