CDVI

Security to Access

ATRIUM

Software Version 7.0

www.cdvigroup.com

1] PRODUCT PRESENTATION 3

2] NOTES AND RECOMMENDATIONS 4

3] PACKAGE CONTENTS 5

4] INSTALLING/UPDATING THE ATRIUM SOFTWARE 5

5] PROGRAMMING 6

Starting the ATRIUM Software 6
Adding a Controller 7
Adding a Sub-Controller 9
Understanding the ATRIUM Software 11
Users 16
Cards 24
Holidays 31
Schedules 34
Areas 39
Access Levels 42
Operator Programming Rights 44
Doors 46
Relays 55
Inputs 57
Outputs 62
Events 64
Reports 66
System Overview 70
Locks 85
Bells 87
Tamper switch 90
Readers 91
Macros 93
Advanced Macros 97
Email Notifications 103
Cameras 105
DESFire Application ID and Readers 109
Global Settings 115
Intrusion (Alarm) Integration 119
Elevator Integration 126
Lockdown 140
IEVO Biometric Integration 158
Accounts 165
OFFLINE Configuration 170

6] WARRANTY - TERMS & CONDITIONS 175

1] PRODUCT PRESENTATION

The ATRIUM software is an advanced and powerful access control management tool. It allows an operator to monitor and manage the system by accessing the ATRIUM controller using a network connection. The ATRIUM USB includes the ATRIUM software and the reference manual. The reference manuals for ATRIUM hardware components are also available on the ATRIUM USB.

This chapter contains important information concerning the installation and use of this software.

Manage up to:

- **500 Doors**
- **10,000 users**
- **10,000 cards**
- **1,000 Access Levels**
- **250 Schedules each supporting 100 time periods**
- **100 Holidays**
- **256 Floors (Elevator Integration)**

2] NOTES AND RECOMMENDATIONS

This section describes how to install the ATRIUM software on a computer, start the application, register your product and add a controller.

COMPUTER REQUIREMENTS

The ATRIUM interface is designed to operate with computers running a suitable Windows operating system as detailed in the "Operating System Requirements".

- Intel i5 Processor 4.2 GHz or better
- 8GB RAM (16Gb recommended for superior performance)
- 500GB of Hard Disk (SSD recommended for superior performance)
- Ethernet access either through physical 10/100 Mbps Ethernet port or WIFI

OPERATING SYSTEM REQUIREMENTS

The ATRIUM interface has been tested on the following operating systems:

- Windows 11
- Windows 10
- Windows 8, 8.1,
- Windows 7 Service Pack 1
- Windows Server 20016 R2 Service Pack 2,
- Windows Server 2012 R2
- Windows Vista Service Pack 2

OTHER SOFTWARE REQUIREMENTS (AVAILABLE ON THE USB):

- Windows Installer 4.5
- .NET Framework 4.6.1
- .NET Framework 4.8
- VC++ 2017 Redistributable
- VC++ 2019 Redistributable
- SQL Server Express 2012, SP4
- SQL Server Express 2019

FREE TECHNICAL SUPPORT

For technical support in North America, dial 1-866-610-0102 Monday to Friday from 8:00 a.m. to 8:00 p.m. EST. For other locations, please refer to last page of this document or visit our website: www.cdvigroup.com.

3] PACKAGE CONTENTS

- One USB key

4] INSTALLING/UPDATING THE ATRIUM SOFTWARE

To install the ATRIUM software on Windows, you must be logged on with an administrator account.

Ensure the computer has the latest Windows Update installed before installing ATRIUM software. Failing to do so may cause software installation malfunction. The tolerance of your antivirus may also cause a malfunction of the software ATRIUM. It is recommended to add both paths in your antivirus exceptions: C: \ Program Files (x86) \ CDVI Group \ * and C: \ Program Files \ Microsoft SQL Server \ MSSQL11.CDVI_ATRIUM \ *. These paths are created by default when installing the ATRIUM software.

1. Start the ATRIUM setup either from the supplied USB key or from the hard drive when downloaded from the web.
   a) To install from the USB, insert the ATRIUM software USB key into the computer's USB port. If the auto run feature is enabled, go to the step 2. Otherwise, use Windows Explorer to locate and start ATRIUM-Setup.exe.
   b) To install from the hard drive, first download the application from www.cdvi.ca then use Windows Explorer to locate and start ATRIUM-Setup.exe.
2. Select the installation language from the list then click on OK.
3. Click Next.
4. The License Agreement window will appear. To install the ATRIUM software, select "I agree to these terms and conditions" check box and click Next.
5. If you wish to select a different folder destination for the ATRIUM software, click the Browse button, choose the folder destination and click Install.

The ATRIUM software is installed by default to C:\Program Files (x86)\CDVI Group and the database is in C:\Program Files\Microsoft SQL Server\MSSQL11.CDVI_ATRIUM

6. Click Finish to complete the installation. If required, restart your computer to complete the installation.

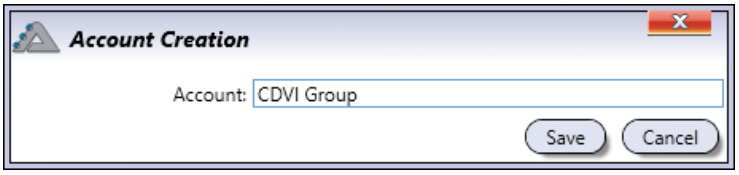
An ATRIUM icon is automatically added to your computer desktop.

5] PROGRAMMING

STARTING THE ATRIUM SOFTWARE

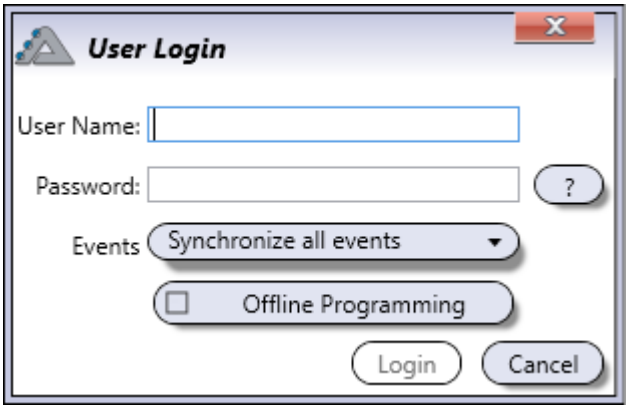
This section describes how to start the ATRIUM software.

1. Double-click the ATRIUM icon on your desktop or click Start >Programs >CDVI Group >ATRIUM >ATRIUM. The first time you start the ATRIUM software, the "Account Creation" window will be displayed.



2. Type the name of the new account and click "Save".

3. The ATRIUM software "User Login" window will be displayed. Type the Login ID and password for the selected account. The default login ID and password is ***"admin"***. You can also choose to synchronize the events from the A22 or A22K controller or not to. Events do not hold any database configuration.



Once you have created your account with the default login ID and password. It is strongly recommended you change the Login ID and password for security reasons. Refer to the "Accounts" chapter for account and password management.

4. Click on "Login".

ADDING A CONTROLLER

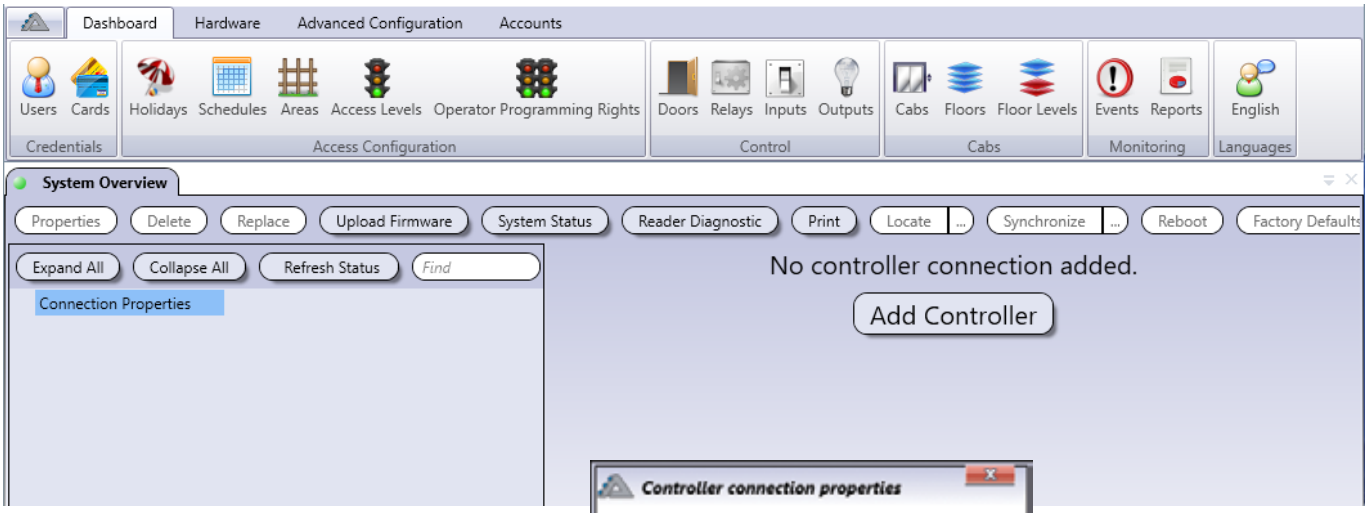
For each new account, the following screen is displayed to indicate that a controller needs to be associated with the account. To add a controller, proceed with the following steps.

It is recommended to choose as the first controller of a site, one that will be designated as ***"Master"*** controller and to which the doors are connected will be the LEAST busy (less activity).

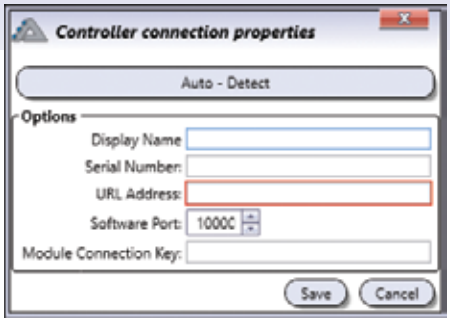
Out of the box ATRIUM controller is ready for IP connectivity, fifty (50) controller maximum per account. If you have more than one ATRIUM controller per account, one must be set as the ***"Master"*** controller to manage the other forty-nine (49) IP controllers, defined as ***"Sub-Controllers"***.

It is HIGHLY recommended that you reserve an IP address in the DHCP server for each ATRIUM controller. Consult the IT specialist in charge of the network so that he can reserve an IP address for the ATRIUM controller.

1. Click on ***Add Controller***. The Controller Connection pop up will be displayed.

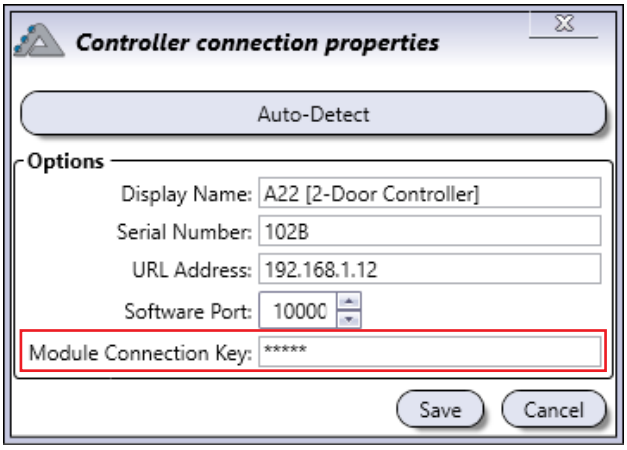


2. Click the ***Auto-Detect*** button to find the ATRIUM controller(s) on the network.



3. Select the controller from the list and click ***Select***.

The Serial Number, IP Address and Software Port information will be inserted automatically.



4. Enter "Module Connection Key" password. The default password is "admin". Click ***OK***.

The ATRIUM system includes two users, "Installer" and "Administrator". The default login ID and password for "Installer" are "admin". The default login ID and password for "Administrator" are "admin1". Additional users may be added to the system and assigned user rights accordingly. In addition, the system offers four software "User rights" levels. See below.

SOFTWARE USER RIGHTS

User Rights	Can do firmware update	Can configure the system	Can add/delete/modify users, cards and PIN	View only
1. Installer	✓	✓	✓	✓
2. Administrator		✓	✓	✓
3. Operator			✓	✓
4. Guest				✓

5. Enter the user login ID and Password. Click ***Login***. The application will synchronize with the controller and expander modules connected to the controller.

ADDING A SUB-CONTROLLER

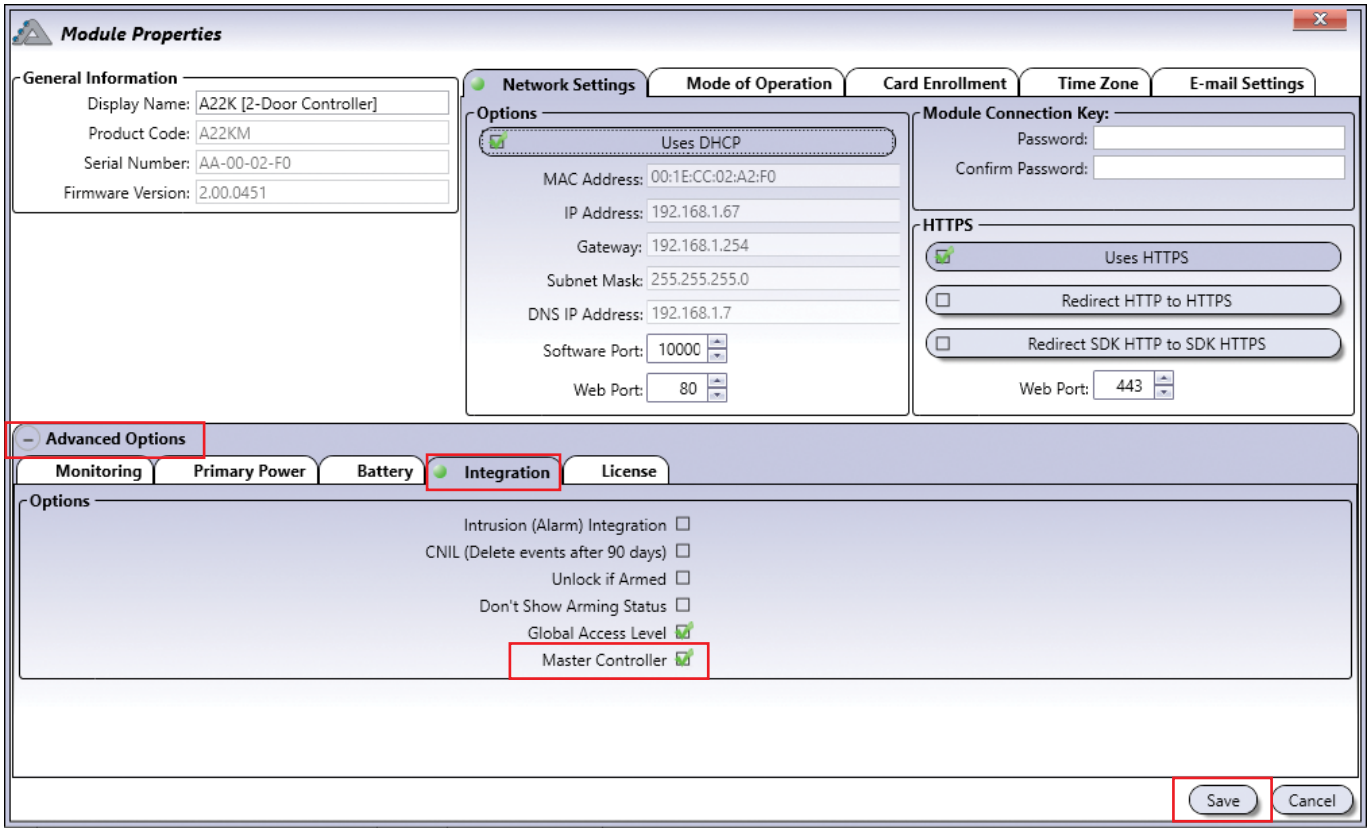
First, set the main controller as a ***"Master"*** controller:

From the ***Hardware*** tab, click on the ***System Overview*** icon.
Select the main controller from the list and click on the ***Properties*** button.

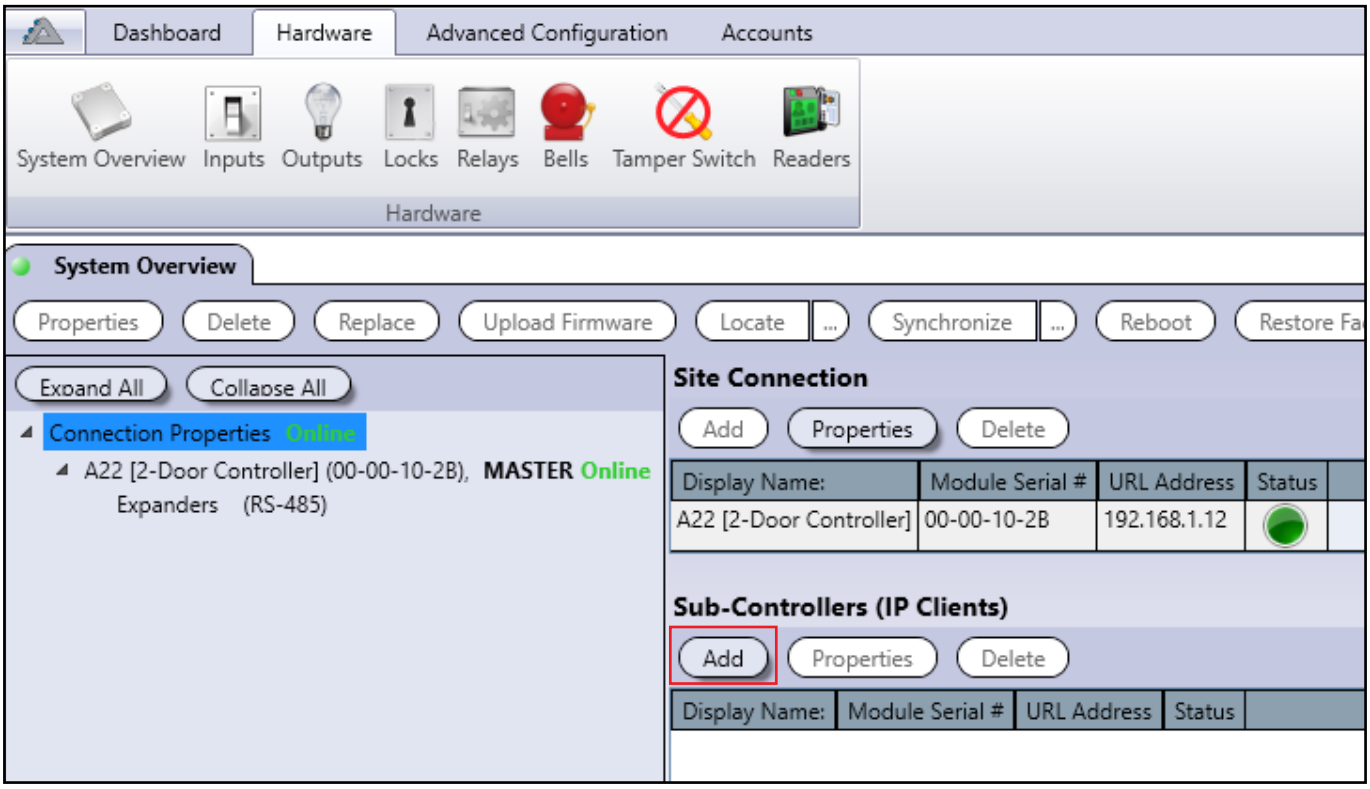
Expand the ***Advanced Options*** menu by clicking on the **+** symbol, then click on the ***Integration*** tab.

Click on the checkbox next to "Master Controller", then click "***Save***" at the bottom right.

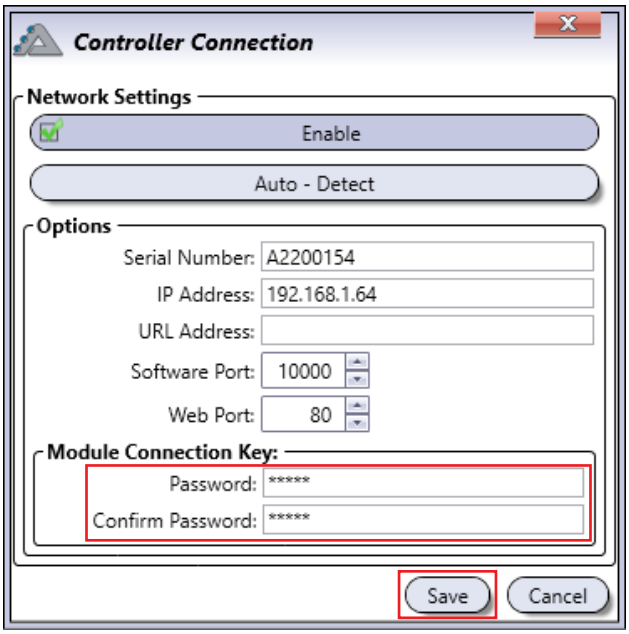
The controller start to reboot and at the end of the process the controller product code will change from A22/ A22K to A22M/A22KM and then you can start adding the other IP controller (49 max. per site) as ***"Sub-Controllers"***.



Click on ***Add*** in the **Sub-Controllers (IP Clients)** menu.



Click on ***Auto-Detect*** in the **Controller Connection** window. Click on the A22/ A22K and click ***Select*** to confirm. You can also manually type in the information if the module is on a different network.



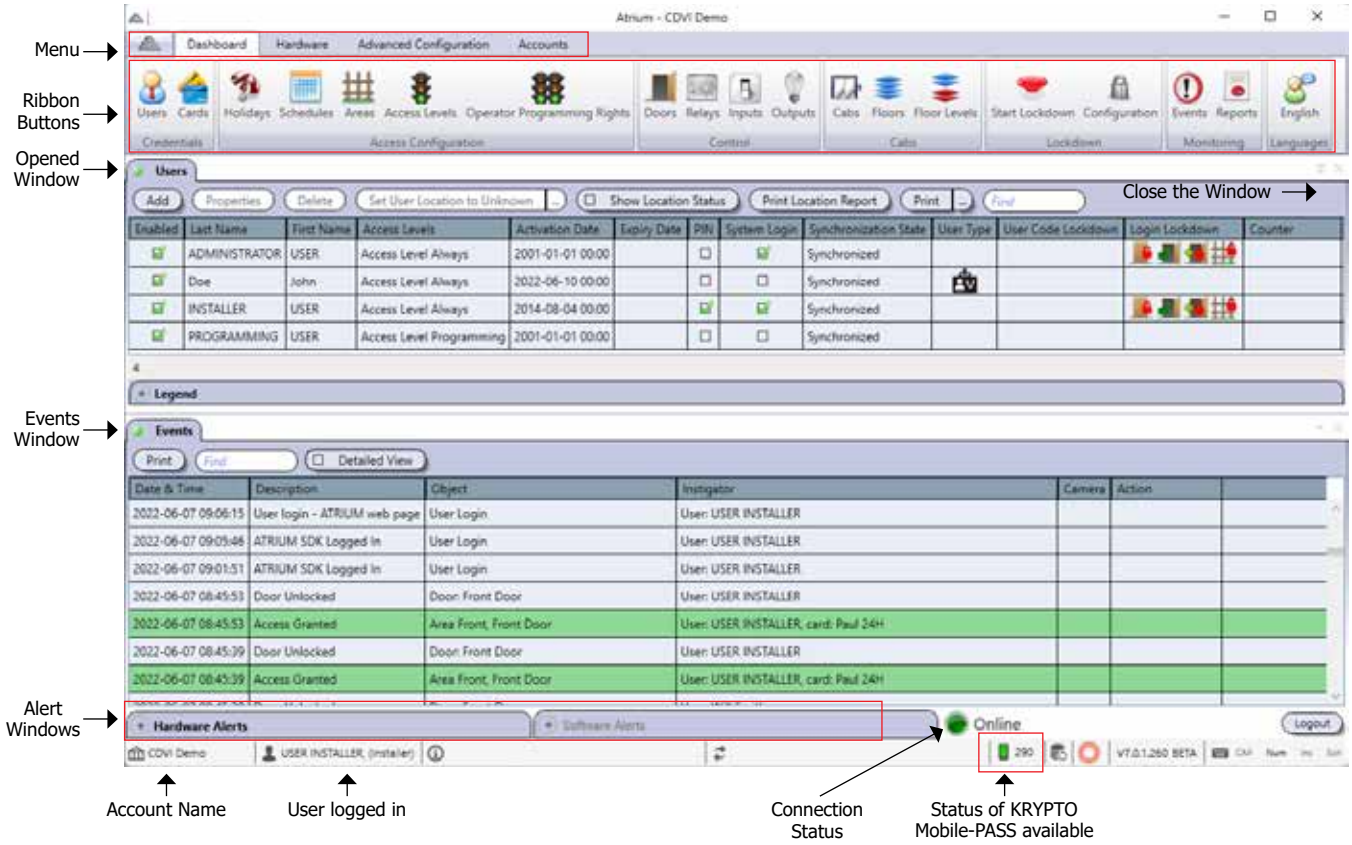
Type "admin" into the ***Password*** and ***Confirm Password*** fields. Click ***Save*** and your Sub-Controller will synchronize.

UNDERSTANDING THE ATRIUM SOFTWARE

The following chapter presents the structure of the main window of the ATRIUM software including the different windows, menus, and buttons.

USER INTERFACE OVERVIEW

The main window of the ATRIUM software is shown below.



MENU AND RIBBON BUTTONS

The menu gives access to the Dashboard, Hardware, Advanced Configuration, and Languages menus/tabs.

ATRIUM Icon

- About, Help and exit

Dashboard

- Credentials
  - Users, refer to page 16.
  - Cards, refer to page 24.

- Access Configuration
  - Holidays, refer to page 31.
  - Schedules, refer to page 34.
  - Areas, refer to page 39.
  - Access Levels, refer to page 42.
  - Operator programming rights, refer to page 44.

- Control
  - Doors, refer to page 46.
  - Relays, refer to page 55 (This icon is also available from the Dashboard tab).
  - Inputs, refer to page 57 (This icon is also available from the Dashboard tab).
  - Outputs, refer to page 62 (This icon is also available from the Dashboard tab).

- Cabs
  - Cabs, refer to page 123
  - Floors, refer to page 123
  - Floor Levels, refer to page 123

- Lockdown
  - Configuration, refer to page 133

- Monitoring
  - Events, refer to page 64
  - Reports, refer to page 66

- Languages:

  The ATRIUM software is a multi-language application. Select the desired language from the list.

Hardware

- Hardware
  - System Overview, refer to page 70.
  - Inputs, refer to page 57 (This icon is also available from the Dashboard tab).
  - Outputs, refer to page 62 (This icon is also available from the Dashboard tab).
  - Locks, refer to page 85
  - Relays, refer to page 55 (This icon is also available from the Dashboard tab).
  - Bells, refer to page 87
  - Tamper Switch, refer to page 90
  - Readers, refer to page 91

Advanced Configuration

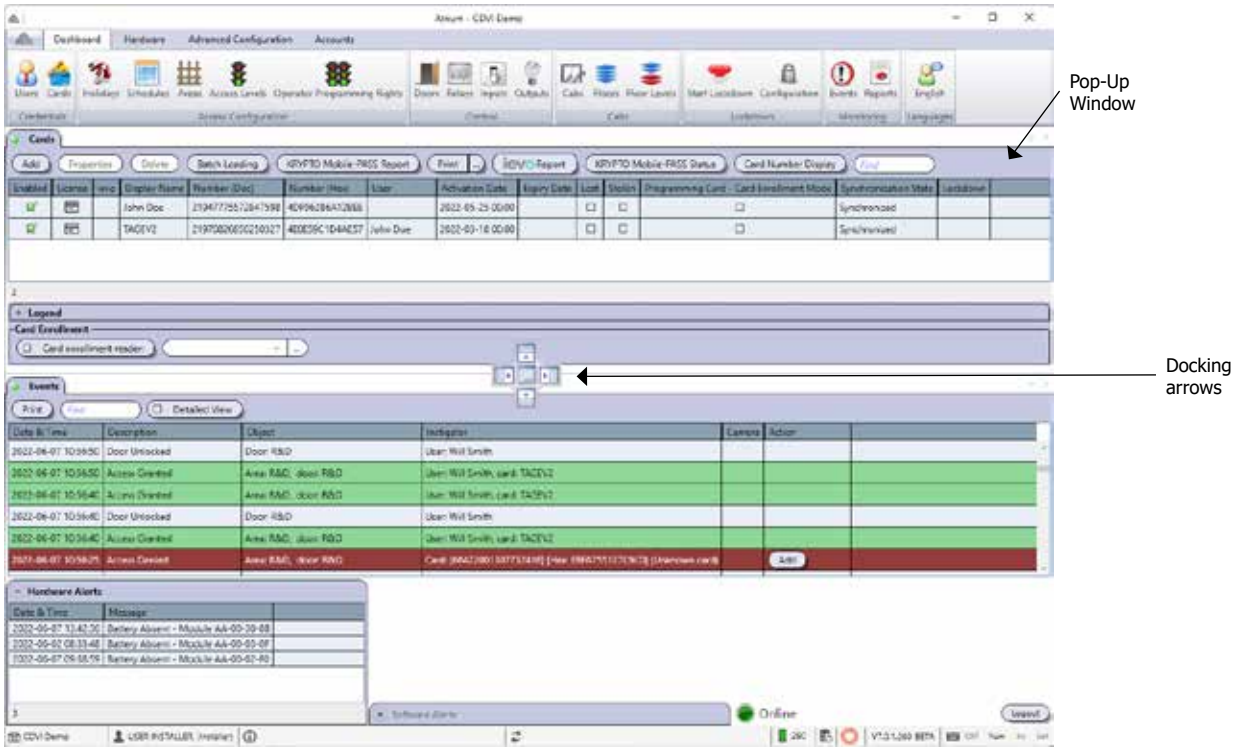
- Programming
  - Macros, refer to page 93
  - Emails, refer to page102
  - Cameras, refer to page 105
  - DESFire Readers, refer to page 108
  - Global Settings, refer to page 114

Accounts

- Management
  - Accounts, refer to page 158.
  - Import/Export (Offline)

OPENED WINDOW AND EVENT WINDOW

To move an opened window, click on the desired window tab and drag it to the desired location on the computer screen or use the docking arrows to dock it either to the left, right, top, or bottom.



Once a window has been moved as a pop-up, the docking mode is enabled meaning that each window that will be opened will be docked as shown in the following picture.

ALERT WINDOWS

The Hardware Alert and Software Alert windows show event status respectively related to hardware and software events. The following table lists examples of hardware and software events.

	Examples of Events
Hardware	Battery Absent - Module 00-00-00-01 Battery Low - Module 00-00-00-01 Bell Shorted - Module 00-00-00-01 Door Lock 0 Bypassed by Emergency Input - Module 00-00-00-02 Input 0 Masked - Module Module 00-00-00-02 Tamper Switch Trouble - Module Module 00-00-00-01 etc.
Software	Attempt to write a duplicate card or keyboard code failed. Module SN: 0, object ID: 1 The module 0 already has an active connection. Module 0 information was successfully changed. Cannot connect to the module 0, User right error. Communication timeout. Module: 0, synchronizer: 1 Login error: the login ID and/or password are wrong. etc.

CONNECTION STATUS

Indicates the communication status with the ATRIUM module(s).

- **Online:** Connection established with the controller.
- **Offline**: Connection not established or lost with the controller.
- **Synchronizing**: Synchronizing the computer and controller data.
- **Limited Connectivity**: Communication is established, however one or more ATRIUM modules is offline.

TYPING NAMES AND NOTES

1. When changing the name of a system component in the ATRIUM software windows (i.e. name of a door, user, relay, etc.), ATRIUM will immediately refresh the screen.

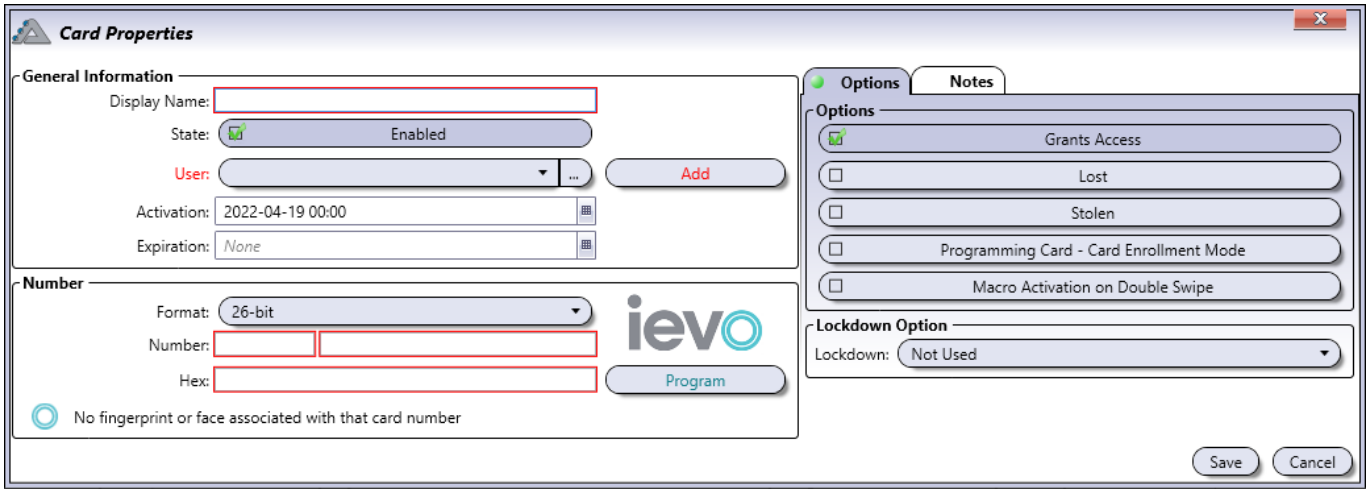
2. Please note that ATRIUM supports up to 15 (first and last names) or 31 (other labels) characters for text fields and up to 1000 characters for Notes fields.

REQUIRED FIELDS

Fields surrounded by a red frame are either required fields or fields in error.

For example, the Display Name, Format, and Hex fields from the Card Properties window are mandatory (required) fields.

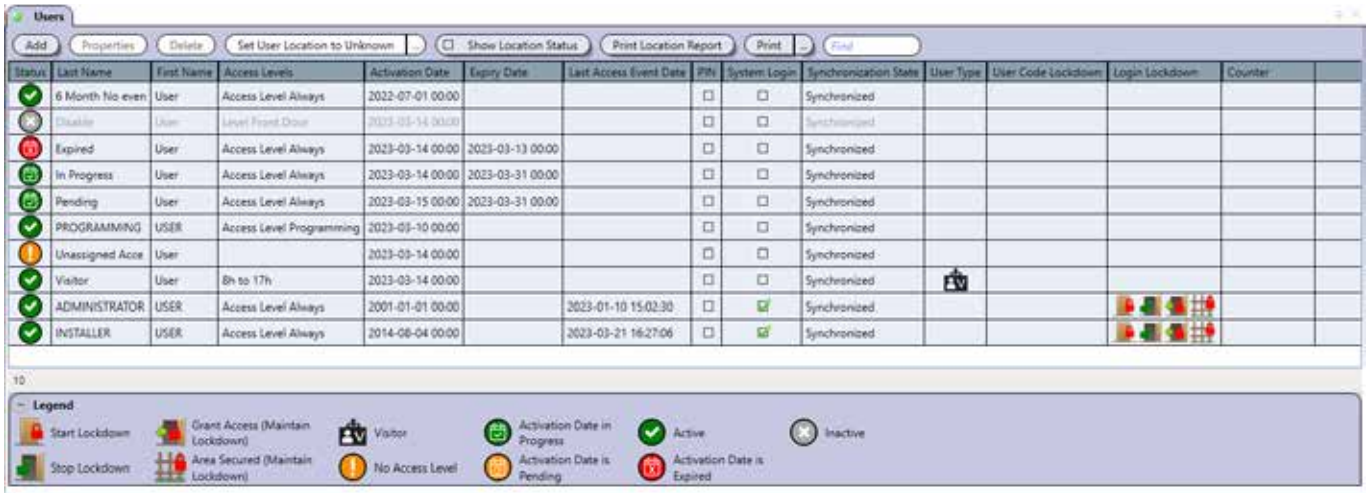
A field in error prevents from saving changes and closing the window.



USERS

Programming a user allows to define the details pertaining to the user. Any individual that needs to access an area (room) must be defined in the system as a user. Once defined, a card can be assigned to a user.

From the ***Dashboard*** tab, click on the ***Users*** icon. From this window, a user may be added, edited, or deleted.



The following users are defined by default:

- **INSTALLER USER:** This user is active by default, can program cards and has a system and web access login. This user is usually the System Installer that configures all hardware related configurations. The installer usually defines along with the owner the perimeters of an area that needs to be protected by an access door and also define with the owner or system manager, the different access levels and access schedules.

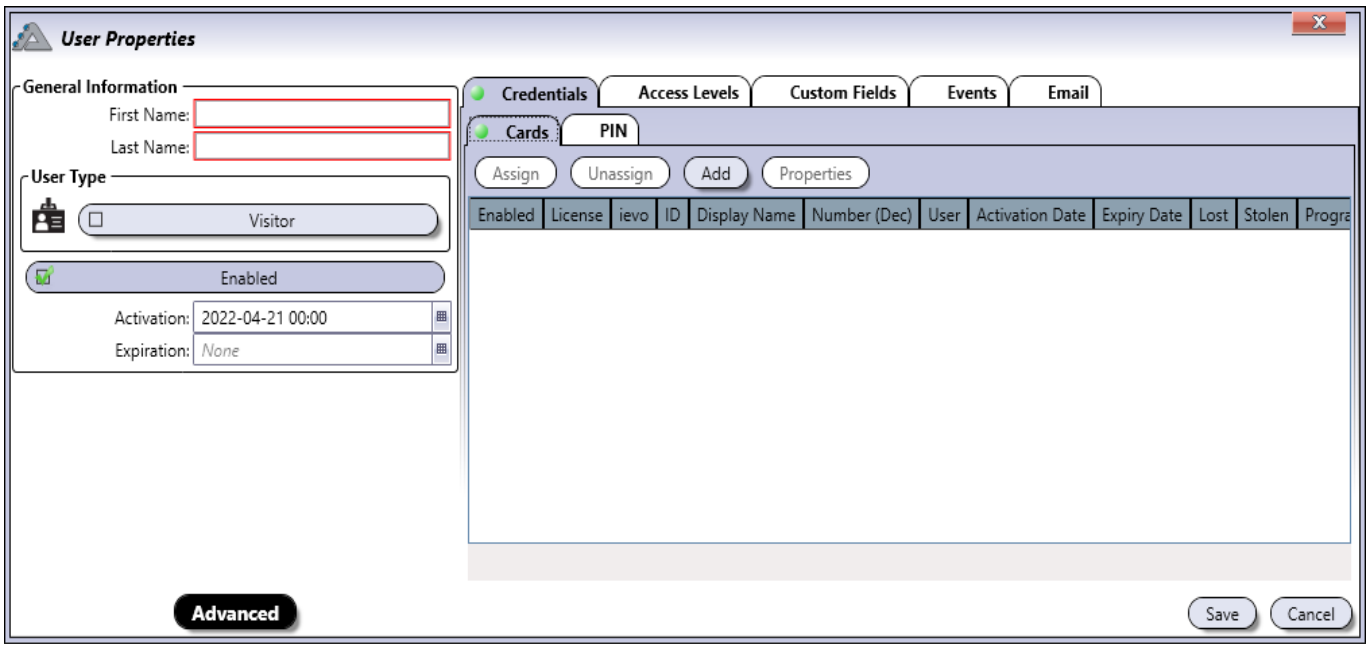
- **ADMINISTRATOR USER:** This user is active by default, can add / delete cards and users, has the ACCESS LEVEL ALWAYS and has a system and web access login. This user is usually the system administrator or manager, the responsible to add and delete user in the system. The ADMINISTRATOR USER also defines the access levels, the operator programming rights, the schedules, the holidays and the different access rights of all the other users.

- **PROGRAMMING USER:** This user is active by default and is used to add new cards to the system. Whenever the CARD ENROLLMENT mode is used, all the new cards programmed will inherit the programming of the user associated to the PROGRAMMING CARD. It is also possible to define multiple PROGRAMMING USER with different configuration and access rights. With this, it is then possible to program different PROGRAMMING USER allowing easy USER programming with a specific template.

ADDING A USER

From the ***Dashboard*** tab, click on the Users icon and click on the ***Add*** button.

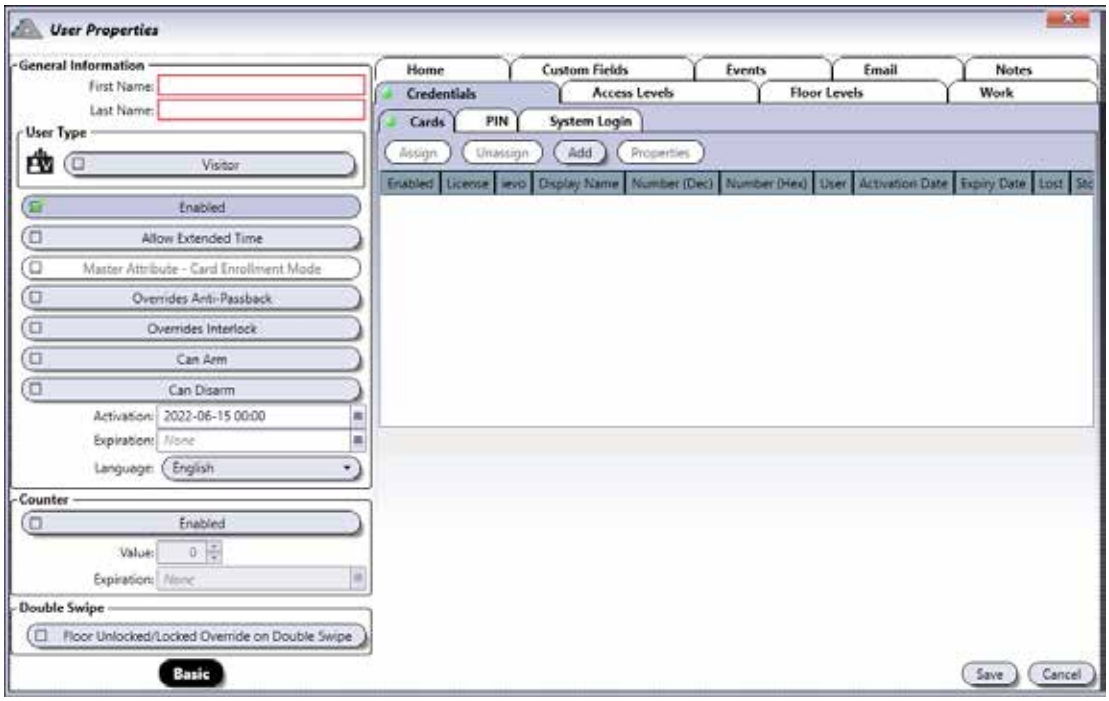
General Information



Basic and Advanced View

- **First Name:** Indicates the first name of the user. A maximum of 15 characters is allowed.
- **Last Name:** Indicates the last name of the user. A maximum of 15 characters is allowed.
- **User Type (Visitor):** Indicates that this user is tagged as a visitor. An icon will be displayed next to this user in the grid.
- **Enabled:** When selected, indicates that the user is active.
- **Activation Date:** Indicates the date the user becomes valid. Enter the year, month, day and time of the day the user becomes valid or click on the ***calendar*** icon and select the date and time. The user will become active at selected activation date and time.
- **Expiration Date:** Indicates the date the user becomes invalid. This is useful for personnel on contract which would require an access for a specific period of time. Enter the year, month, day and time of the day the user expires or click on the ***calendar*** icon and select the date and time. The user will expires at the selected date and time. For permanent users, do not select an expiration date (leave the field empty).

Advanced View Only

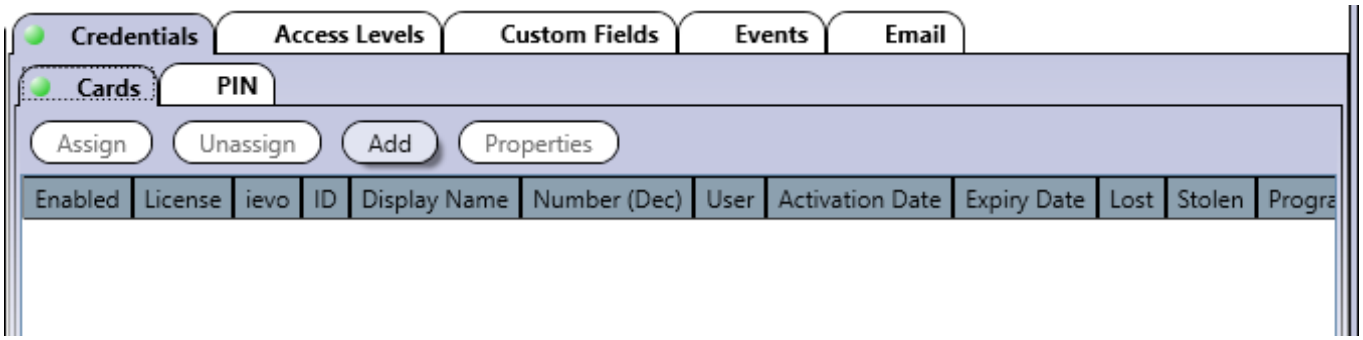


- **Allow Extended Time:** When a user is granted access to a door, the door will remain unlocked for the period defined by the door's Unlock Time. When Allow Extended Access is enabled, the door will remain unlocked for the duration of the door's Extended Time in addition to its Unlock Time. This option is particularly useful for individuals that may require more time to access the door.
- **Master Attribute Card Enrollment Mode:** Enables this user's card to activate "Card Enrollment" mode when a second card, which has the "PROGRAMMING Card" option activated, is presented to the same reader within 5 seconds.
- **Overrides Anti-Passback:** When selected, indicates that the user will override anti-passback.
- **Overrides Interlock:** When selected, indicates that the user will override interlock.
- **Can Arm:** When selected, indicates that the user can arm the integrated alarm system. See "Integration tab" on page 41 for more detail.
- **Can Disarm:** When selected, indicates that the user can disarm the integrated alarm system. See "Integration tab" on page 41 for more detail.
- **Activation:** Indicates the date the user becomes valid. Access rights are permitted.
- **Expiration:** Indicates the date the user becomes invalid. All access rights will be denied.
- **Language:** ATRIUM supports several languages. Select the language this user will use when accessing the ATRIUM software or web server. The user must have a system login ID and password.
- **Counter:** When selected, this enables the counter for any Card or PIN associated with the user, limiting how many times the user can pass through designated doors.
- **Counter Value:** set the number of times the user can pass through selected doors.
  - To activate the decrement counter, select ***Decrement Counter on Card or PIN*** on the side of of the door with the reader (see Doors p. 46).
- **Expiration:** Indicates the date the user counter becomes invalid. The Expiration Date overrides the Counter value. The User is denied access when the counter reaches zero (0) or the when expiration date has passed. Whichever comes first.
- **Double Swipe (Floor Unlocked/Locked Override on Double Swipe):** Indicates that the user can sequentially unlock, lock and return the floor to its normal state by swiping the cab reader twice.

Credentials Tab

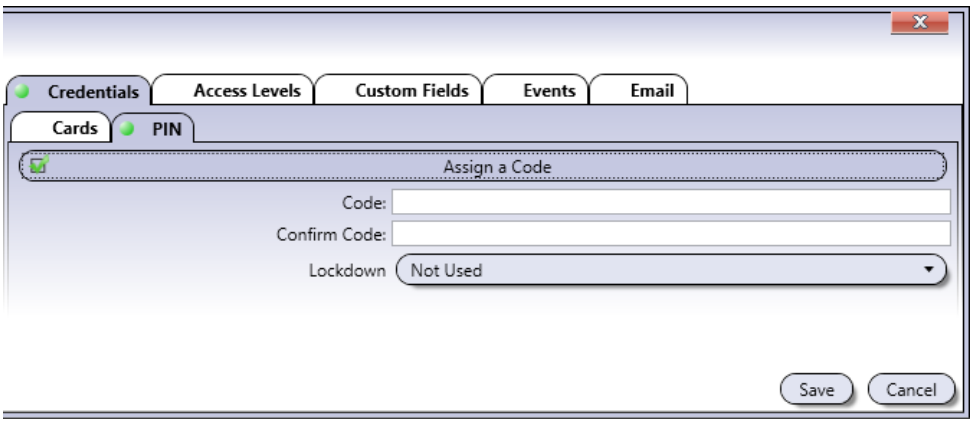
The ***Credentials*** tab allows to assign/unassign card(s), a PIN code (optional) and an ATRIUM system login to a user (optional).

Basic View



Cards

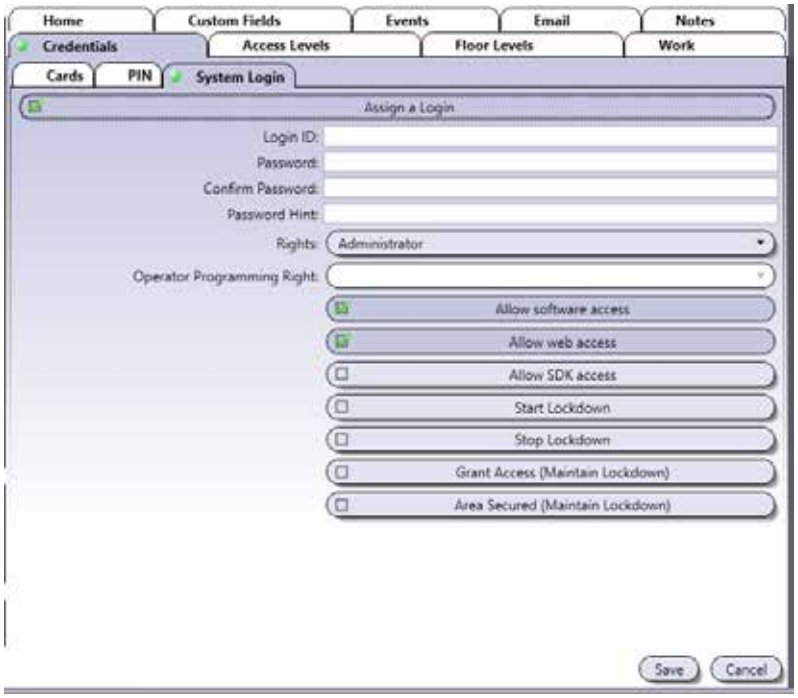
- **Assign:** To assign a card to this user, click on the Assign button and select a card from the list. The cards are listed with the following information: Active, ID, Display Name, Number, User, Activation Date, Expiry Date, Lost, Stolen, and Programming Card. Valid and invalid cards are listed and can be selected but a card will not be operational until its status is changed to Active.
- **Unassign:** To unassign a card, select a card from the list of cards and click on the Unassign button.
- **Add:** To add a new card, click on the Add & Assign button. Refer to "Adding a Card" on page 25 for more information.
- **Properties:** To edit a card, select a card from the list of cards and click on edit. Refer to "Adding a Card" for more information.



PIN

- **Assign a Code:** When selected, allows to assign a code to access a door that is configured to use keypad codes.
- **Code:** The code must contain five digits and must be unique. Each digit can be any numerical value from zero to nine.
- **Confirm Code:** Re-enter the code for confirmation.
- **Lockdown:** Allows to assign the code to start a lockdown, stop a lockdown, grant access or area secured

Advanced View



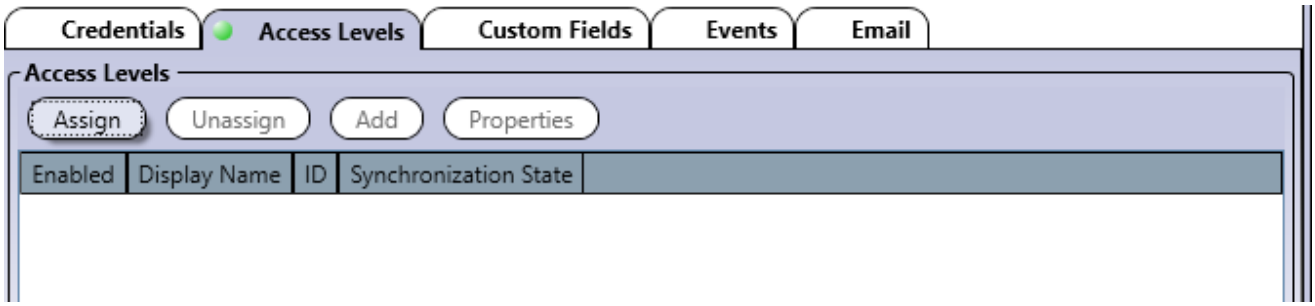
System Login

Allows the user to login to the ATRIUM software and/or web server.

- **Assign a Login:** Select this check box to enable the access to the PC and/or ATRIUM's Web server for this user.
- **Login ID:** Enter a login name that will be used to access the PC and/or ATRIUM's Web server. Up to 31 characters are allowed.
- **Password:** Enter the password that will be used to access the PC and/or WATRIUM's Web server.. Up to 31 characters are allowed.
- **Confirm Password:** Re-enter the password for confirmation.
- **Password Hint:** Enter a password hint that will help you remember your password in case you forget the password.
- **Rights:** Select one of the four software user rights levels. See page 8 for more information on the software user rights.
- **Operator programming rights:** The operator programming rights becomes active once the user right "Operator" is selected. Choose one of the operator programming rights available. See page 44 for details about the operator programming rights.
- **Allow Software Access:** When selected, gives access to the PC version of the ATRIUM software.
- **Allow Web Access:** When selected, gives access to the Web server.
- **Allow SDK Access:** When selected, gives access to the SDK.
- **Start Lockdown:** When selected, gives the user the ability to initiate a lockdown.
- **Stop Lockdown:** When selected, gives the user the ability to stop a lockdown.
- **Grant Access (maintain lockdown):** When selected, grants the user access while maintaining lockdown.
- **Area Secured (maintain lockdown):** When selected, allows the user to secure an area while maintaining lockdown.

Access Levels Tab

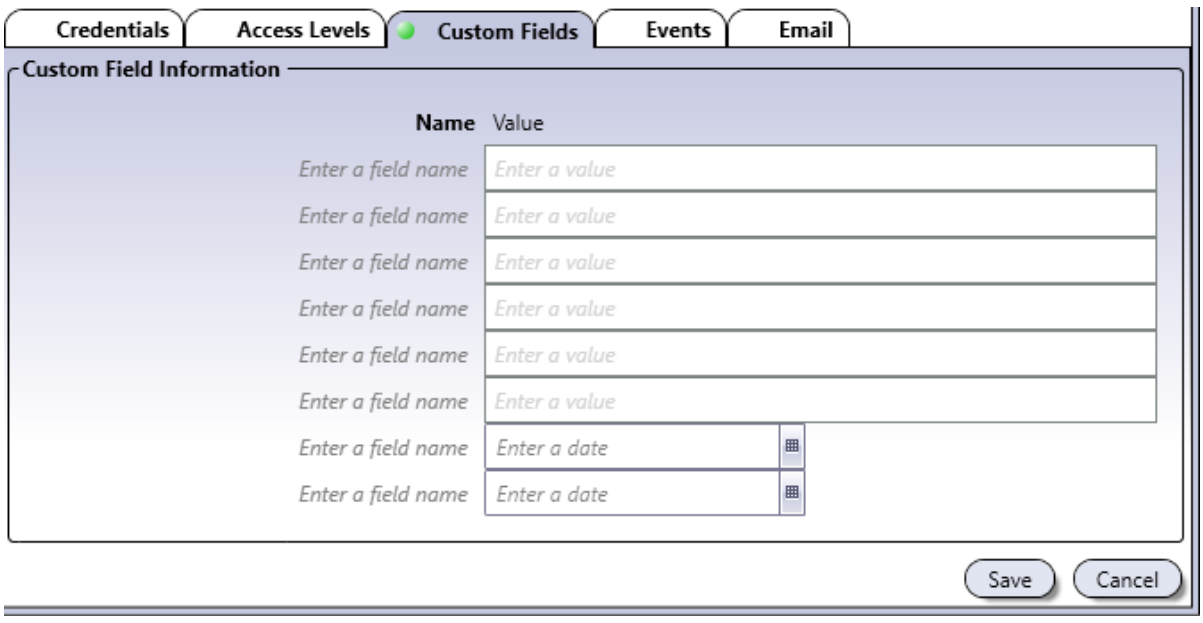
The ***access levels*** tab specifies the area(s) in the building the user will have access to and during which time periods.



- **Assign:** Click on the Assign button and select the access level(s) to be assigned to the user. For information, refer to "Access Levels" on page 42. If two or more access levels are assigned to a user, access is granted as long as one of the defined access levels is valid when the card is presented.
- **Unassign:** Select an access level from the list and click on the Unassign button to revoke this access level for the user.
- **Add:** Allows to define a new access level. Click on the Add & Assign button to add a new access level. Refer to "Adding an Access Level" for more information.
- **Properties:** Allows to edit an access level. Refer to "Adding an Access Level" on page 42 for more information.

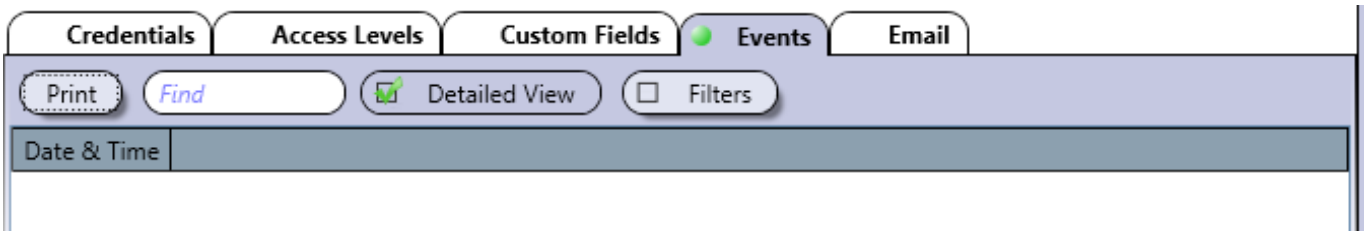
Custom Fields Tab

In the ***Custom Fields*** tab you can customize up to 6 regular fields and 2 fields for dates. As examples, a custom field for employee number, passport number, credit card number, birthday, etc.



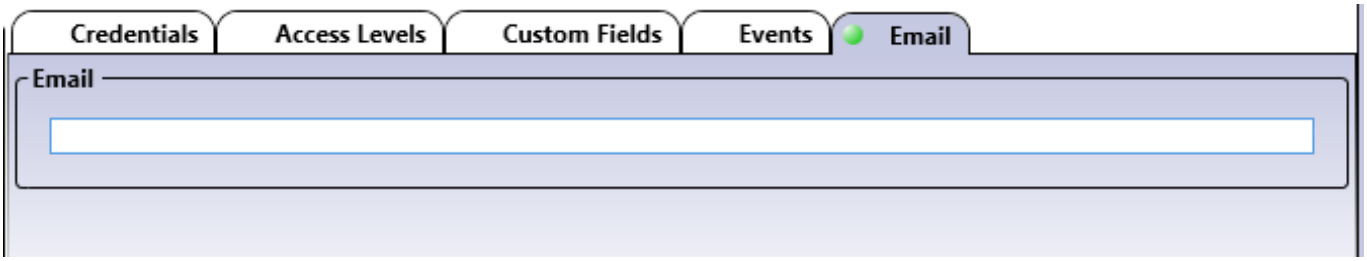
Events Tab

The ***Events*** tab lists, in real-time, the selected user's related events. Refer to "Events" on page 64 for more information.



Email Tab

The e-mail entered in this field will be the one used to send KRYPTO Mobile-PASS. One e-mail per user is allowed.



Advanced View

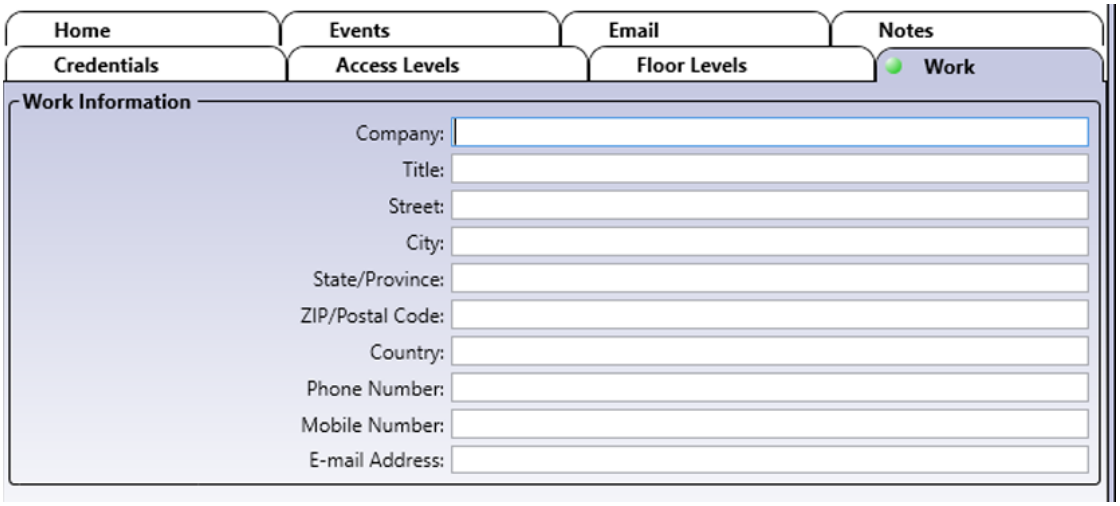
Floor Levels Tab

The ***Floor Levels Tab*** tab specifies the floor(s) in the building the user will have access to and during which time periods.

- **Assign:** Click on the Assign button and select the floor level(s) to be assigned to the user. For more information, refer to "Floor Levels" on page 123. If two or more floor levels are assigned to a user, access is granted as long as one of the defined floor levels is valid when the card is presented.
- **Unassign:** Select a floor level from the list and click on the Unassign button to revoke this floor level for the user.
- **Add:** Allows to define a new floor level. Click on the Add & Assign button to add a new floor level. Refer to "Adding a Floor Level" for more information.
- **Properties:** Allows to edit a floor level. Refer to "Adding a Floor Level" on page 123 for more information.

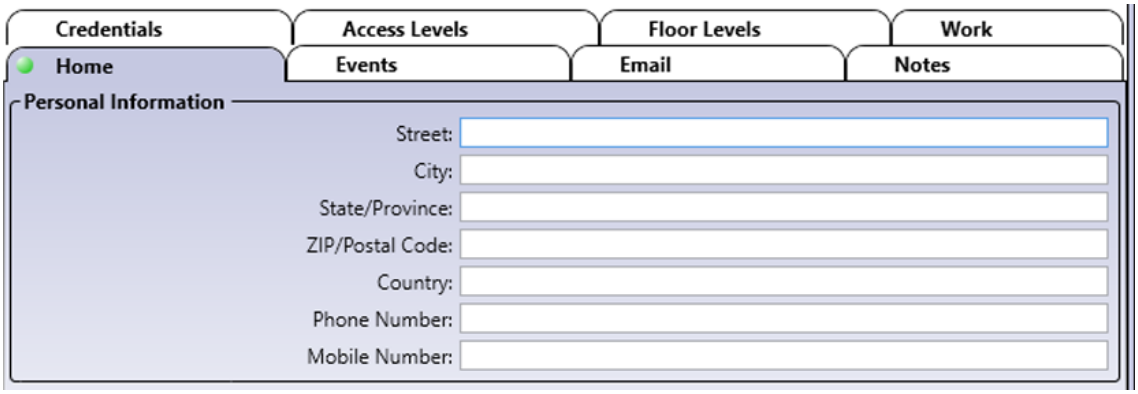
Work Tab

The ***Work*** tab allows to enter the user's professional contact information.



Home Tab

The ***Home*** tab allows to enter the user's personal contact information.



Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save and Cancel Button

Use the ***save*** button to save changes or the ***cancel*** button to ignore changes.

MODIFYING A USER

Select a user from the list and click on the ***Properties*** button. See "Adding a User" for more information.

DELETING A USER

Select the user from the list and click the ***Delete*** button. A dialogue box will appear requesting confirmation.

Administrator and Installer users cannot be deleted.

CARDS

Allows to define the details pertaining to the card. The card may be associated to a user directly from the Card Properties window while defining the card or later from either the Card Properties or User Properties windows.

From the ***Dashboard*** tab, click on the ***Cards*** icon.

General Information

- **Add:** Allows you to add manually a new card in the ATRIUM system.
- **Properties:** It will open the "Card Properties" window of the selected card.
- **Delete:** Allows you to delete selected cards from the ATRIUM system.
- **Batch Loading:** Allows you to quickly add up to 500 sequentially numbered cards to the system. See page 29 for details.
- **KRYPTO Mobile-PASS Report:** Creates a printable report on the Mobile-PASS credentials in the ATRIUM system. Available, Pending and Assigned Mobile-PASS credentials are identified in the report. The report can also be exported in several common file formats.
- **Print:** Allows you to print a simplified or detailed report of the cards of the ATRIUM system.
- **ievo Report:** Creates a printable report on ievo biometrics credentials in the ATRIUM system. The report can be exported in several common file formats.
- **KRYPTO Mobile-PASS Status:** Displays the number of KRYPTO Mobile-PASS available and pending for the ATRIUM system.
- **Card Number Display:** Allows you to display card numbers in decimal, hexadecimal or both.

By default the following cards are defined:

- **MASTER Card:** This card is active, no expiration date, 26-bit format, and is assigned to USER Administrator.
- **PROGRAMMING Card:** This card is active, no expiration date, 26-bit format, has the Programming Card option enabled, and is assigned to USER PROGRAMMING.

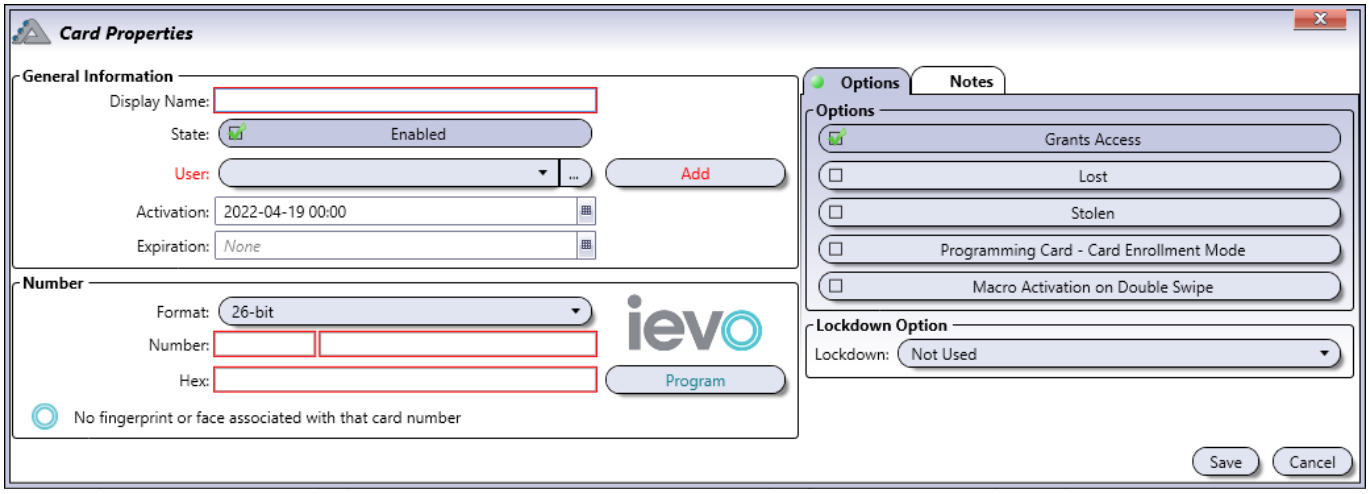
A card set as a ***Programming Card*** cannot be used as an access card.

ADDING A CARD

The card may be added either using the ***Add*** button or the "Card Enrollment mode".

Cards may also be added sequentially using either an access card followed by a programming card or the on-board MODE button; refer to the 2-Door Controller instruction manual for more information. The access card must be assigned to a user having the option "Can Program Cards" selected; refer to "User General Information" on page 17. The programming card must have Programming Card enabled; see "Options Tab" on page 26.

From the ***Dashboard*** tab, click on ***Cards***, and click on the ***Add*** button.



General Information

- **Display Name:** Identifies the card throughout the ATRIUM software. We recommend using a name that is representative of the card.
- **Enabled:** When selected, indicates that the card is active.
- **User:** Allows to assign this card to a user. You can leave this field empty allowing you to assign this card to a user in the "Users" menu.
- **Activation Date:** Allows to enter the date the card becomes valid. Enter the year, month, day and time of the day the card becomes valid or click on the calendar icon and select the date. The card will become active at selected activation date and time.
- **Expiration Date:** Allows to enter the date the card expires. This is useful for personnel on contract which would require an access for a specific period of time. Enter either the year, month, day and time of the day the card expires or click on the calendar icon and select the date and time. The card will expires at selected date and time. For permanent cards, do not select an expiration date.

Number

- **Format:** Choices are 26-bit, Mifare Classic or DESFire EV2, KRYPTO Mobile-PASS and many other format available.
- **Number and Hex:** You will be able to find the card number displayed in the events once read by a card reader. Depending on the format selected, the card number may contain a family code.
- **ievo "Program" button:** Fill in the first name, last name and assign the card to a user before using the biometric integration option. Refer to page 151 for details of ievo biometric integration.

Options Tab

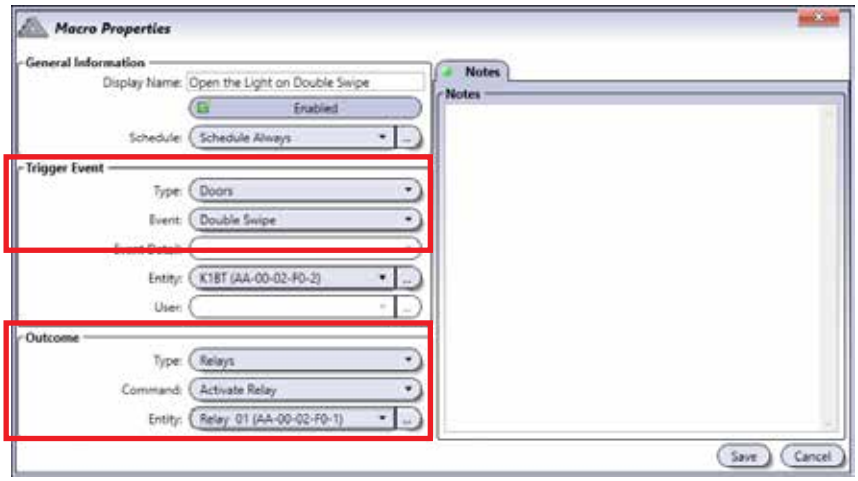
- **Grant Access:** When selected, the card is used for access control.
- **Lost:** When selected, the card status becomes lost.
- **Stolen:** When selected, the card status become stolen.

When the Lost and/or Stolen check box is selected, the card's privileges are indefinitely revoked without having to deactivate or remove the card from the database. As soon as you click ***Save***, the card can no longer be used until its option status is changed.

- **Programming Card (Card Enrollment Mode):** When selected, allows to use this card to add cards sequentially through a door reader; refer to the 2-Door Controller instruction manual for the card enrollment procedure using the MASTER and PROGRAMMING cards. Each card added will be assigned to a new user that will have the same access levels as the user assigned to the Programming Card.

A card set as a Programming Card cannot be used as an access card.

- **Macro Activation on "Double Swipe":** When this option is selected, a double swipe of this card will activate a macro from a door type double swipe event trigger. This macro outcome can activate a command linked either to a door, a relay, an input, an output, a lock, etc. (see p.92 for "Macros").



Lockdown Option

- **Lockdown:** Allows the assigned card the ability to start lockdown, stop lockdown, grant access (maintain lockdown) or keep area secured (maintain lockdown).

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING A CARD

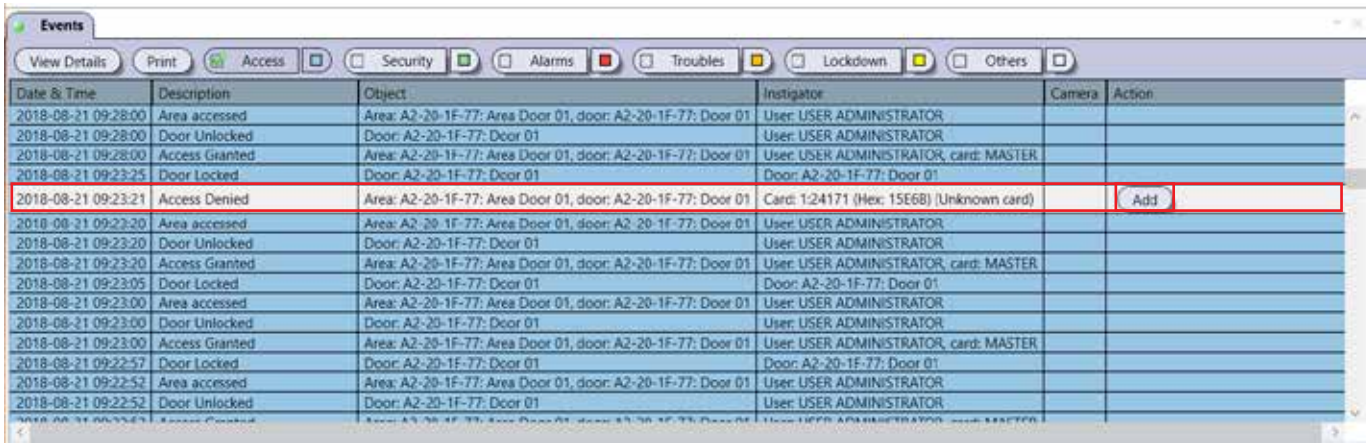
Select a card from the list and click on the ***Properties*** button. See “Adding a Card” on page 25 for more information.

DELETING A CARD

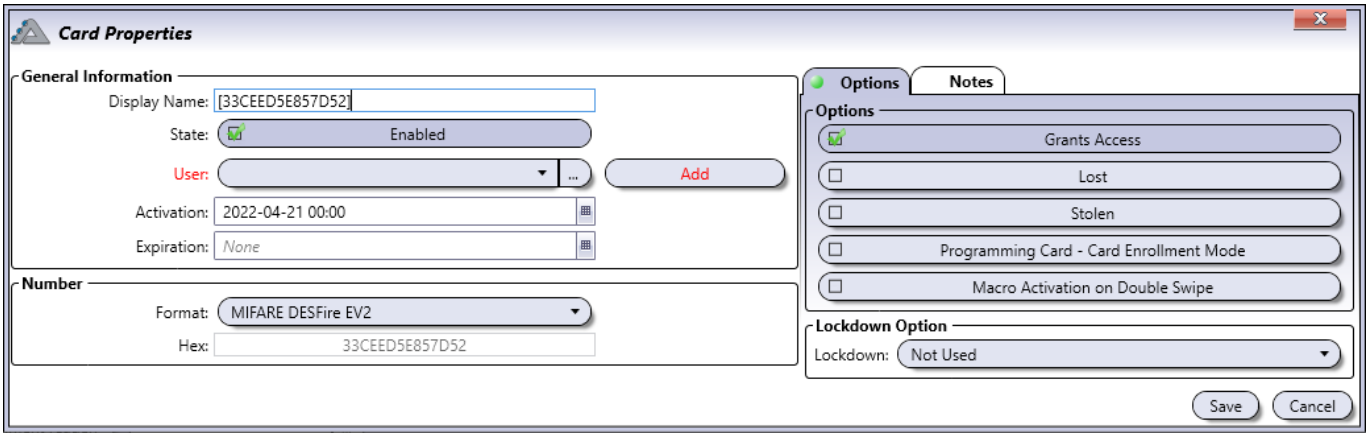
To delete an existing card, select the card from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

ADDING A CARD FROM AN EVENT

A card may also be added from an Access Denied event. When an unregistered card is used the door will not open and the system will record the event.

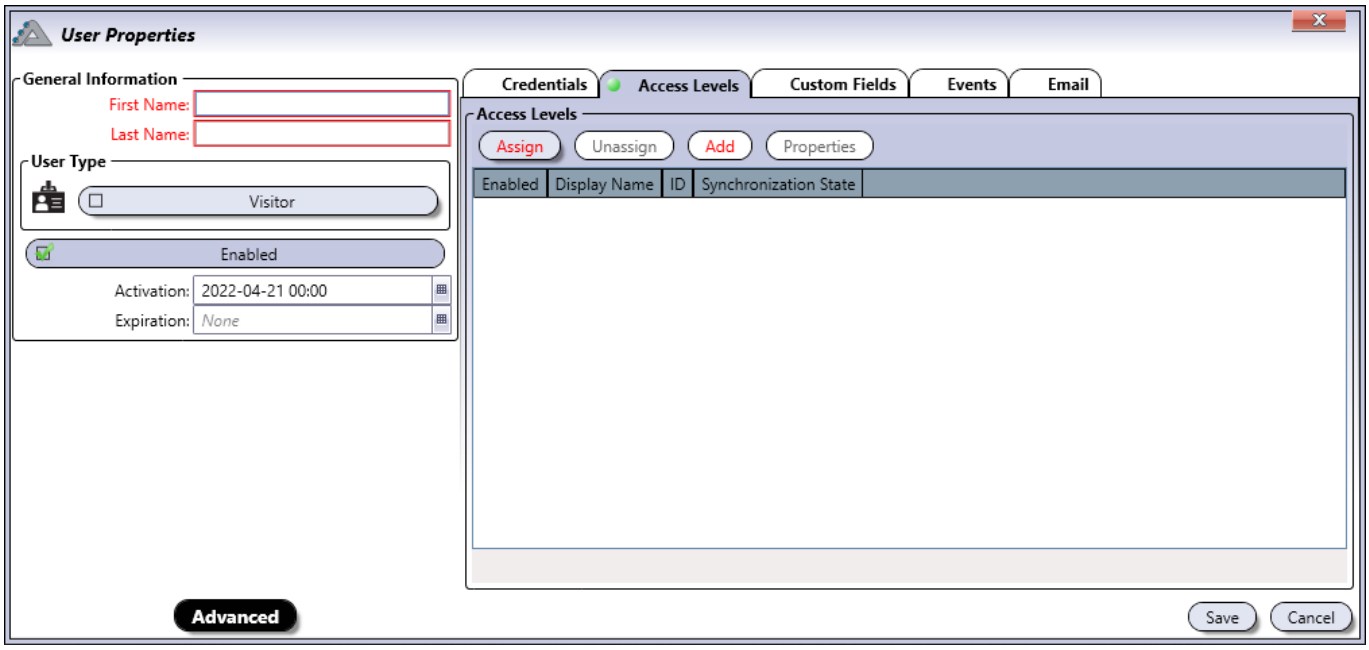


Locate the desired event with the unknown card and click the ***Add*** button.



The card number will fill out automatically. Then assign the card to an existing user with the drop-down menu and click ***“Save”***.

Or click ***"Add"*** to create and assign to a new user. The User Properties window will pop up. Fill out the fields in red (first name and last name) then **"Assign"** its access levels or create a new access level by clicking ***"Add"***. Click **Save** to record changes.



Finally click **Save** in the Card Properties window to finalize the assignment of the new card.

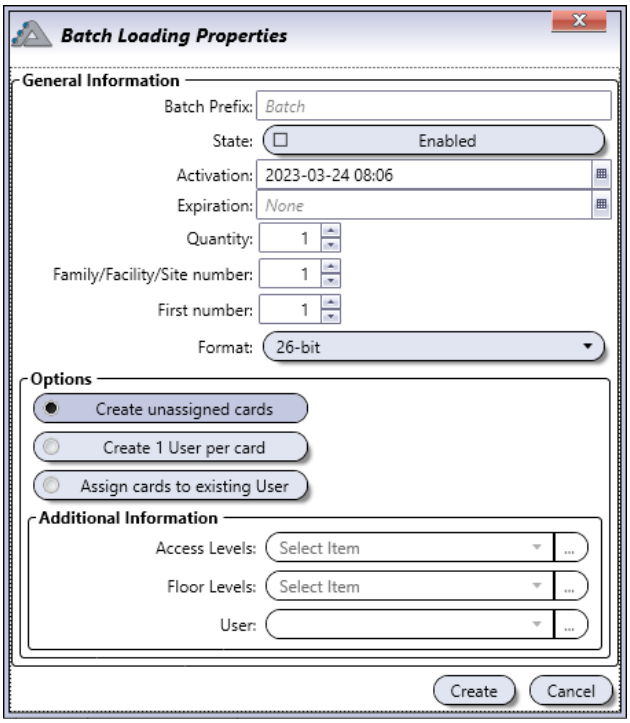
CARD BATCH LOADING

This convenient option is used to quickly add up to 500 sequentially numbered cards to the system. This feature is compatible with most common proximity access card formats.

The cards can be:

- Assigned to Users at a later time (Create Unassigned Cards)
- Assigned to a new User for each card (Create 1 User per Card)
- Assigned to a single existing User (Assign Cards to Existing User)

An "unassigned card" is a card that has NOT been "assigned" to a User (card holder). An unassigned card will not be granted access to any door. Door access rights are given to Users, not cards.



General Information

- **Batch Prefix:** Series of characters (up to 20) placed before the card number to optimize card batch management. For example; put the word "Visitor" for a set of cards dedicated to company visitors.
- **State:** By default, all cards created by batch will be active (Enabled). Uncheck *"Enabled"* to create a batch of cards that will be inactive.
- **Activation:** Enter the activation date for the cards you will create.
- **Expiration:** If needed, enter an expiration date for the cards you will create.
- **Quantity:** Enter the number of cards to create (maximum 500).
- **Family/Facility/Site Number:** Enter the facility number (family code) for the cards to create (ex: Wiegand 26-bit will be number from 001 to 256).
- **First Number:** Enter the starting number of your card sequence.
(ex: Wiegand 26-bit will be any number from 00001 to 65536)
- **Format:** Select the card format (26-bit, 30-bit, 44-bit, KRYPTO Mobile-PASS, etc.).

Options

- **Create Unassigned Cards:** When selected, this option will create unassigned cards only. The cards will appear in the "Cards" menu but are not assigned to a user. When a new user (card holder) is added to the ATRIUM database, simply click the "Assign" button in the "Credentials" tab to select an unassigned card from the list to assign it to the User.
- **Create 1 user per Card:** When selected, this option will create one user per card. You can also assign an access level for all users that will be created. See the "Additional Information" section (shown below) to automatically attribute an access level to the created users. Each new user will be named according to the facility number and card number.
- **Assign Cards to Existing User:** When selected, the created cards will be assigned to the same user. See "Additional Information" to select the user.

A detailed report will be displayed at the end of the batch loading process if one or more cards to be added already exist in the system.

Additional Information

- **Access Levels:** Select the access level to which all created users will be assigned. This option is only available when "Create 1 user per card" option is selected.
- **Floor Levels:** Select the floor level to which all created users will be assigned. This option is only available when "Create 1 user per card" option is selected.
- **User:** Select the user to which all created cards will be assigned. This option is only available when "Assign Cards to Existing User" option is selected.

CARD ENROLLMENT

This option allows to add one or multiples cards sequentially through the selected door reader.

To use the card enrollment feature:

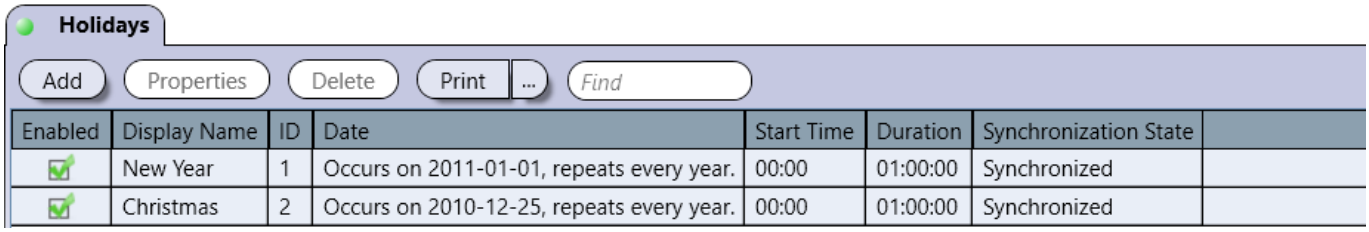
1. Select the "Listen for New Cards on Reader" check box to enable this feature.
2. Select a card reader from the list.
3. Present, one by one, the new cards to be added to the system.
4. For each card presented, a card properties window pops up.
5. For each card, set its name and configure the other parameters as required. See "Adding a Card" on page 25 for more information. Each added card has the following settings by default:
    - Enabled
    - Not assigned
    - No expiry date
    - Card number and format automatically set
6. Click on ***Save*** to complete the addition of the card.

The card enrollment mode ends when no new card is presented for 5 minutes or when the "Listen for New Cards on Reader" check box is cleared.

HOLIDAYS

Holidays define which days in a year are considered as exception. Holidays can be included or excluded from a schedule (refer to "Holidays Tab" on page 37). The holiday is defined by selecting both the start date and time, then the duration. The holiday can be configured to repeat every year. The holiday can be configured to be the same day of the week based on the week the holiday occurs (for example, the first Monday of September).

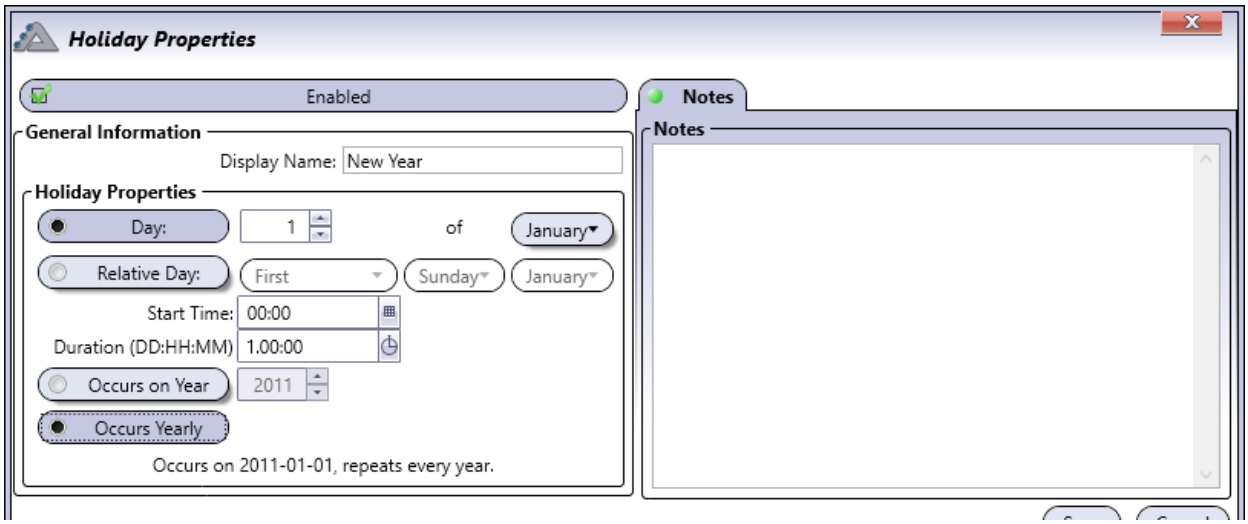
From the ***Dashboard*** tab, click on the ***Holidays*** icon. From this page, holidays may be added, edited and deleted.



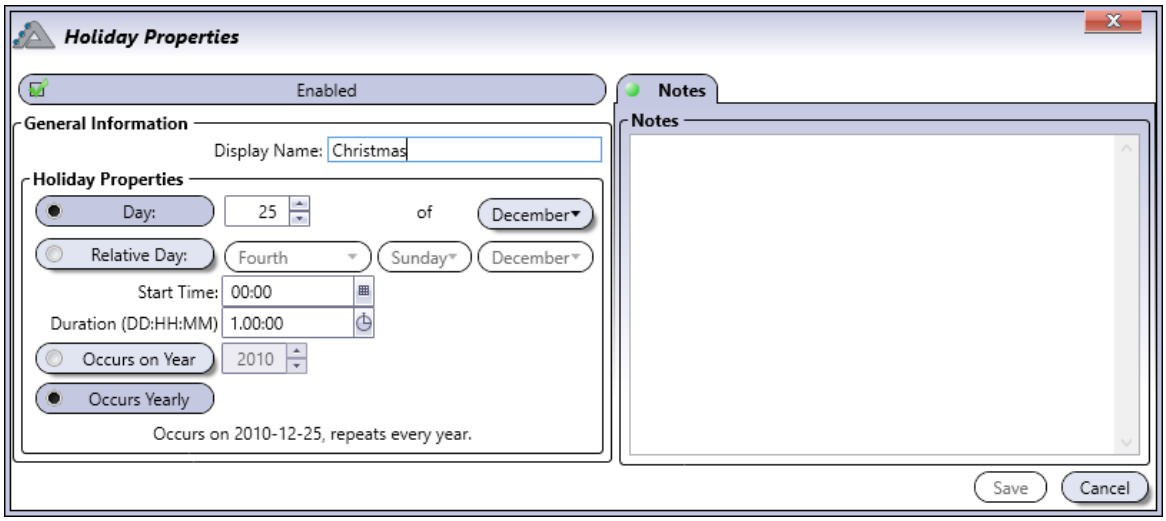
Enabled	Display Name	ID	Date	Start Time	Duration	Synchronization State	
☑	New Year	1	Occurs on 2011-01-01, repeats every year.	00:00	01:00:00	Synchronized	
☑	Christmas	2	Occurs on 2010-12-25, repeats every year.	00:00	01:00:00	Synchronized	

By default the following holidays are defined:

- New Year

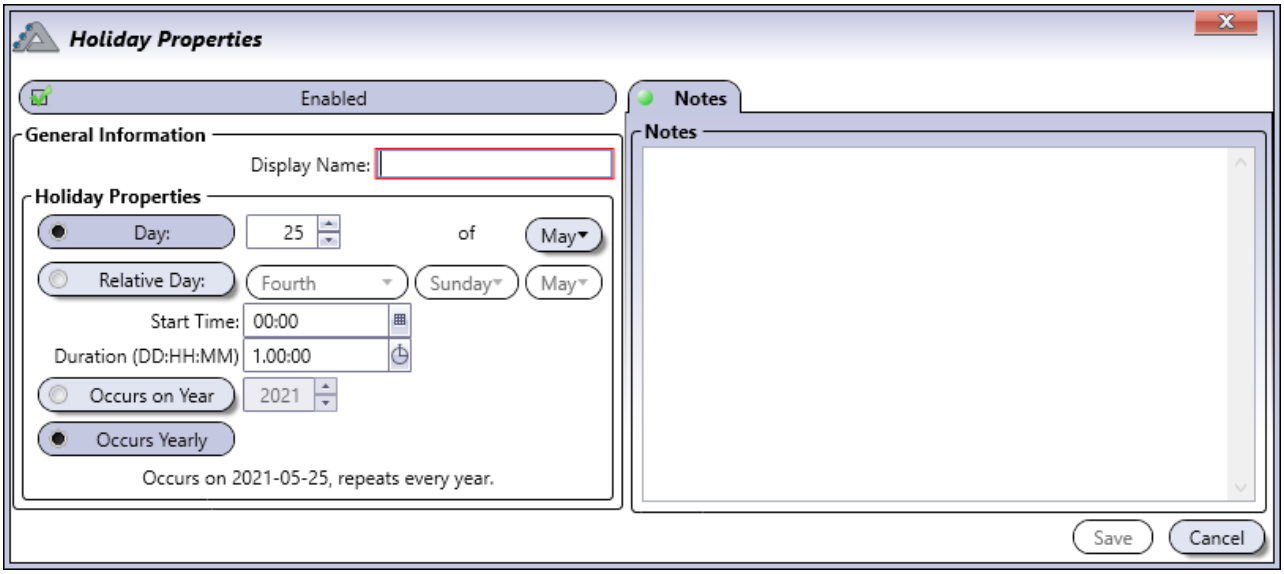


- Christmas



ADDING A HOLIDAY

From the ***Dashboard*** tab, click on the ***Holiday*** icon and click on the Add button.



General Information

- **Enabled:** When selected, activates the usage of the holiday.
- **Display Name:** Identifies the holiday throughout the ATRIUM software. We recommend using a name that is representative of the holiday.
- **Day:** Enter the date of the holiday (day and month)
- **Relative Day:** Enable "Relative Day" if the holiday occurs always the same day of the week. Select the day of the week the holiday occurs. The date entered in the Date field will be used to automatically adjust the holiday date based on which day the holiday occurs. For example if the holiday occurs on the third Monday of May, the date will be adjusted to respect these criteria.
- **Start Time:** Enter the time the holiday starts (hh:mm).
- **Duration (dd:hh:mm):** Enter the duration of the holiday (dd:hh:mm).
- **Occurs on Year:** When selected, the holiday will be effective in the year specifically chosen.
- **Occurs Yearly:** When selected, repeats the holiday every year.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING A HOLIDAY

Select a holiday from the list and click on the ***Properties*** button. See "Adding a Holiday" on page 32 for more information.

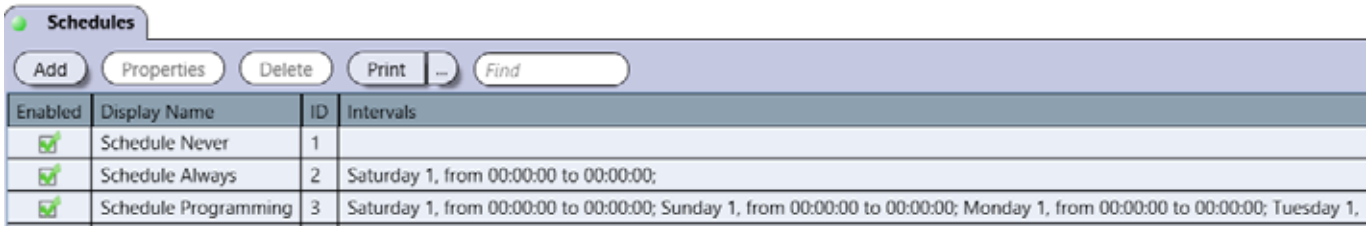
DELETING A HOLIDAY

To delete an existing holiday, select the holiday from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

SCHEDULES

A schedule can be used to unlock doors, control access to areas, and much more. Schedules play an important role in the operation of many ATRIUM functions and are widely used throughout the software (see "Where Schedules Can be Used" below). A schedule is made up of time periods which determine when that schedule will be valid. Each period in a schedule specifies the days and times the schedule will be valid.

From the ***Dashboard*** tab, click on the ***Schedules*** icon. From this page, schedules may be added, edited, and deleted.



By default several schedules are defined. The Never and Always schedules cannot be modified or deleted.

- **Always**: This schedule is valid 24 hours a day, 365 days per year including any programmed holidays.
- **Never**: This schedule is invalid at all times.

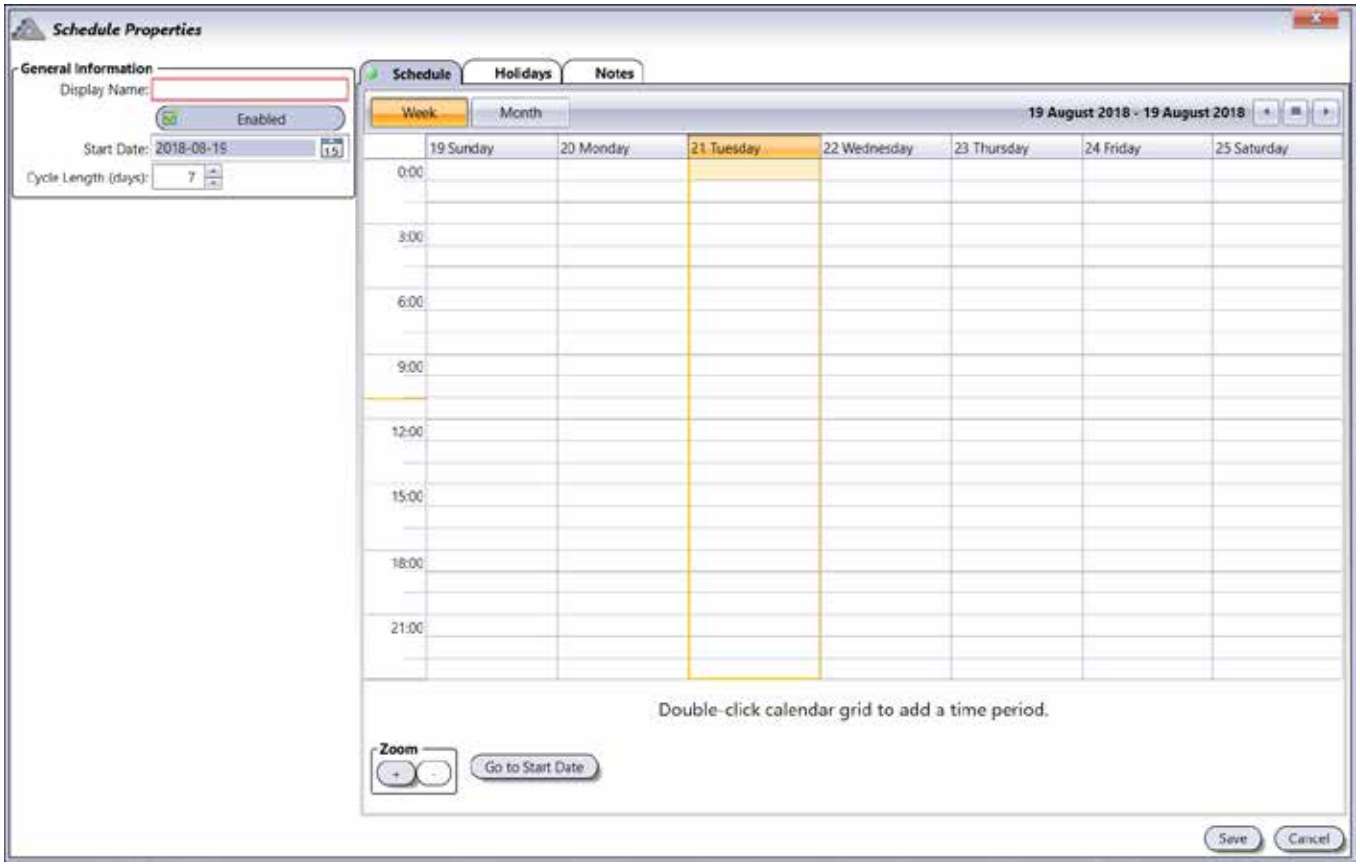
The other pre-defined schedules are not described here. Use the ***Properties*** button to see the parameters of each schedule and to adapt the schedule to your own needs if required.

Where Schedules Can be Used

USED IN	AFFECTS	REFER TO
Access Levels	Areas access	"Access Levels" on page 42
Door	Door Unlock Schedule	"Schedule" on page 49
	REX Unlock Schedule	"Unlock Options" on page 49
Macro	Macro Schedule	"Macros" on page 93
Elevator Integration	Floor Schedule	"Public Access" on page 105
Relays	Relay Schedule	"Relays" on page 55
Emails	Email Notification Schedule	"Emails" on page 102

ADDING A SCHEDULE

From the ***Dashboard*** tab, click on the ***Schedules*** icon and then on the ***Add*** button.

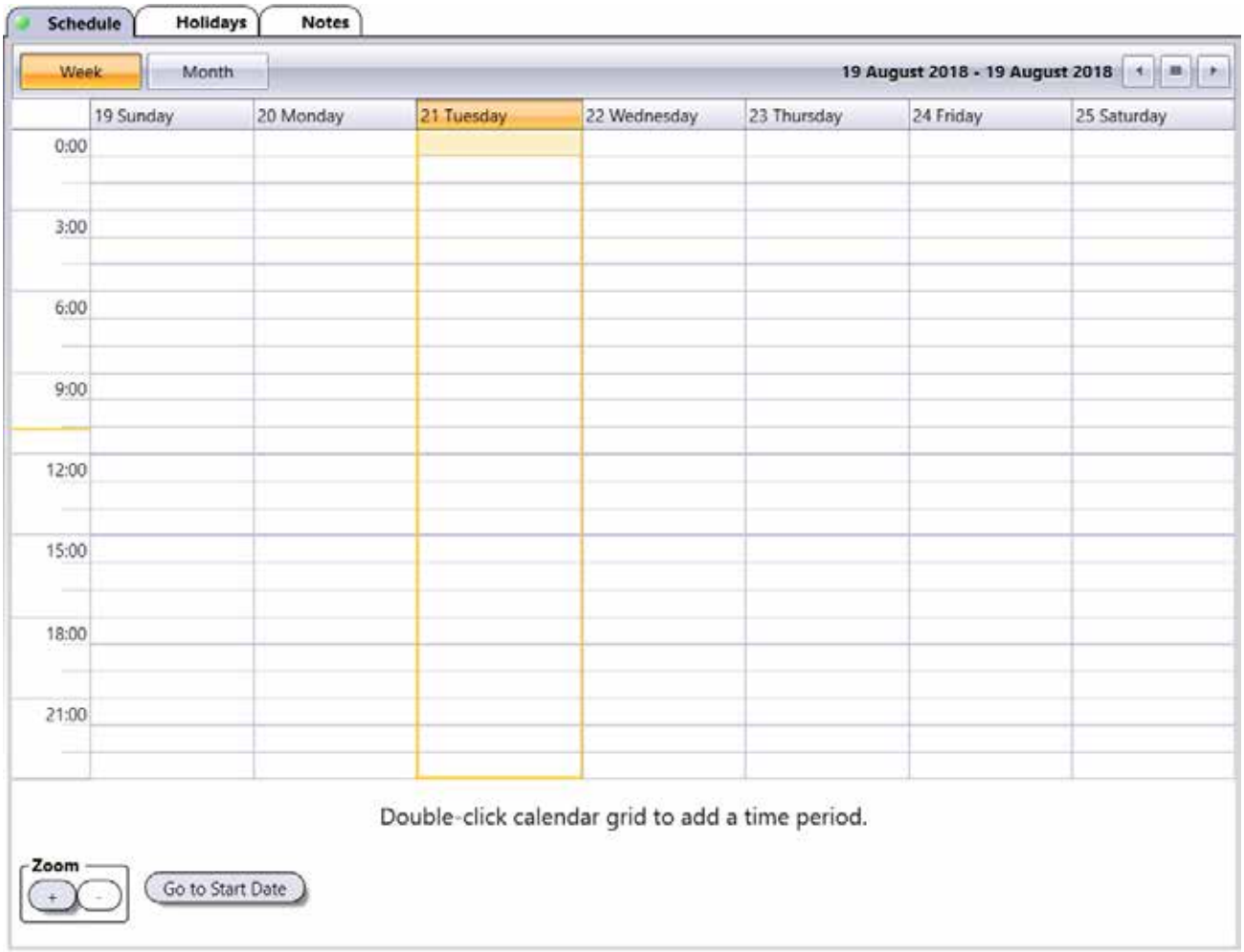


General Information

- **Display Name:** Identifies the schedule throughout the ATRIUM software. We recommend using a name that is representative of the schedule.
- **Enabled:** When selected, activates the schedule.
- **Start Date:** Enter an initiating date for this schedule (yyyy:mm:dd) or select a date using the calendar icon next to the Start Date field. The schedule starts at the date specified.
- **Cycle Length (days):** The schedule is repeated after the number of days specified. The Schedule tab displays up to 7 days at once. If the schedule is based on more than 7 days, use the right/left scrolling arrows located at the top right of the window to access the other days.

Schedule Tab

The ***schedule*** tab allows to set the time period(s) per day.



- **Week button:** Displays a week-based view.
- **Month button:** Displays a month-based view.
- **Zoom "+" and "-" buttons:** Increase and decrease the calendar grid granularity. The granularity goes from 5 minute to 1 hour increments. The Zoom buttons are only available in the Week view.
- **Go to Start Date:** Brings the display to the start of the schedule.

To add a time period:

1. Double-click the corresponding day in the calendar grid to add a new time period.
2. Extend the created period to the desired starting and ending times.
3. Proceed with steps 1 and 2 to add additional time periods the same day or to other days.

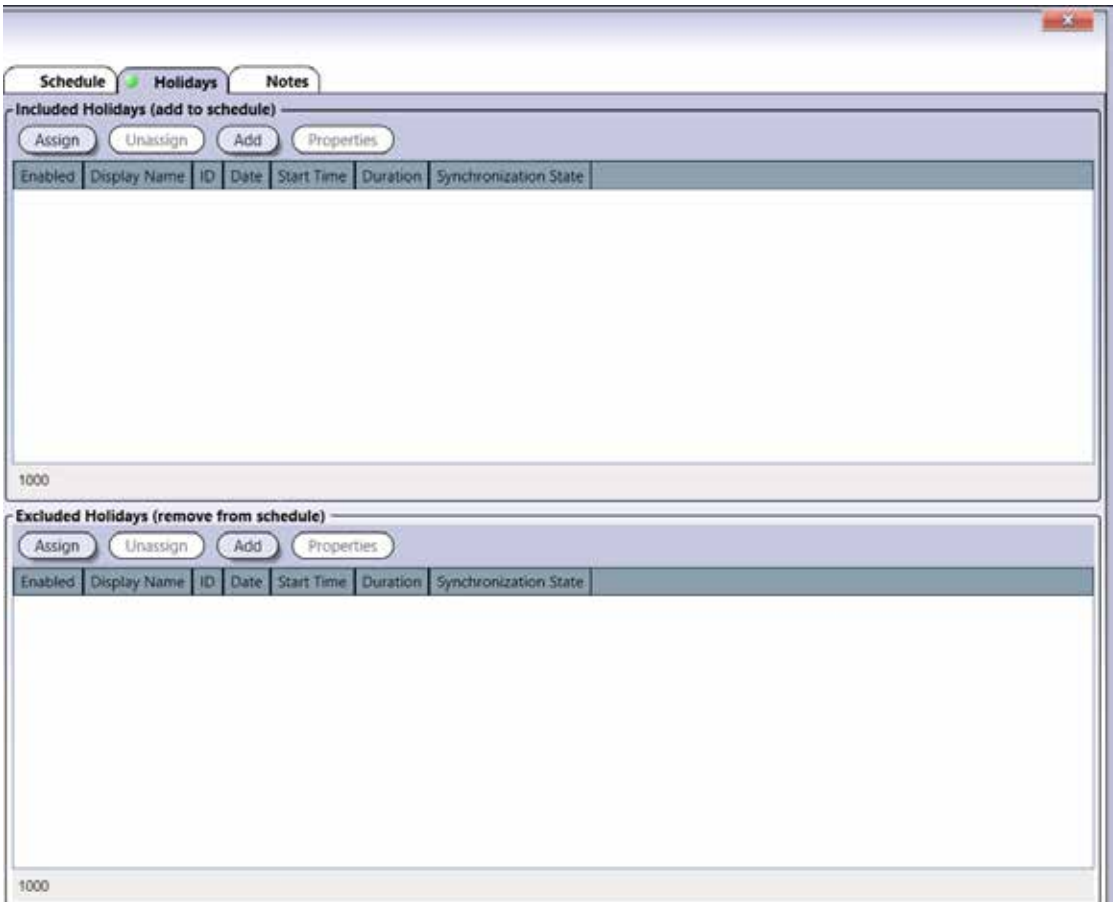
To delete a time period:

- Click on the desired time period and click on X to delete the time period.

Holidays Tab

Allows to include or exclude holidays to/from the schedule. A schedule with an included holiday will remain valid. A schedule with an excluded holiday will become invalid for the duration of the holiday.

Holidays must be defined first, refer to “Holidays” for more information.



Included Holidays and Excluded Holidays

An included holiday adds the holiday period to the regular schedule while an excluded holiday removes the holiday period from the regular schedule.

- **Assign:** Select the holidays that should be included/excluded in/from the current schedule and click on Assign.
- **Unassign:** Select the holiday that should be removed from the list of included/excluded and click on Unassign.

The choice of including and excluding a specific holiday must be exclusive (not both).

- **Add:** Allows to define and add a new holiday. Click on the ***Add*** button to add a new holiday. Refer to “Adding a Holiday” on page 32 for more information.
- **Properties:** Allows to edit a holiday. Select a holiday from the list and click on ***Properties***. Refer to “Adding a Holiday” on page 32 for more information.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

MODIFYING A SCHEDULE

Select a schedule from the list and click on the ***Properties*** button. See "Adding a Schedule" on page 35 for more information.

DELETING A SCHEDULE

To delete an existing schedule, select the schedule from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

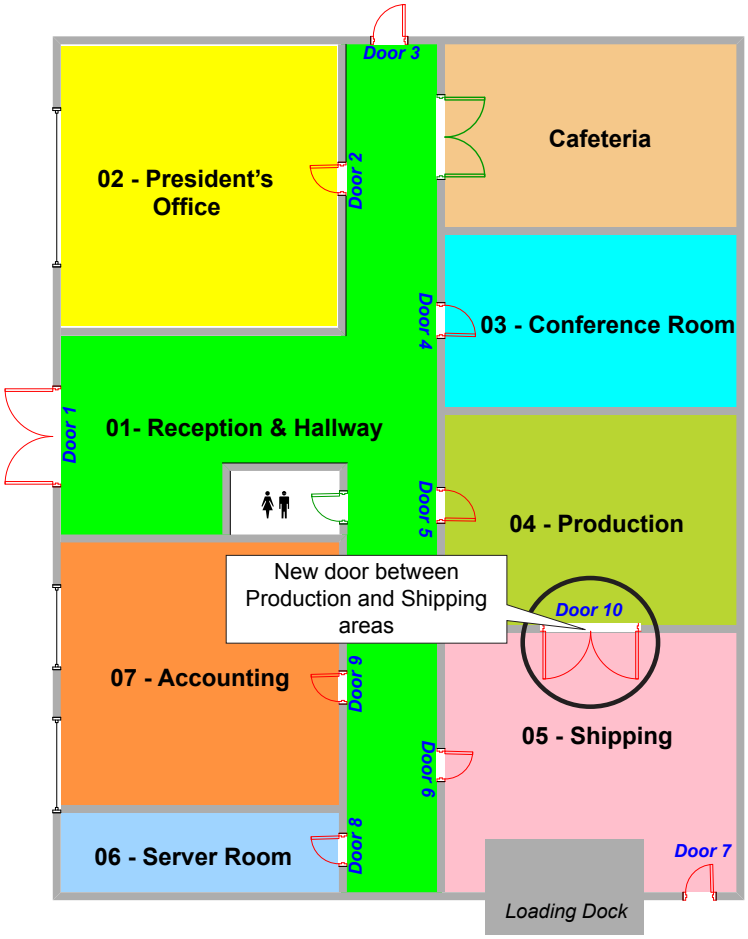
AREAS

Programming areas determines the different access rooms that will be controlled by the ATRIUM system. Once defined, an area can be assigned to an access level which can be assigned to one or more users/card holders.

Area are an important concept in the ATRIUM system. Instead of giving access to doors, ATRIUM gives access to areas. Thus, if a user has access to an area, it will be possible for him to access the area using any door that directly gives access to that area. This avoids having to configure the access for each door individually for this user.

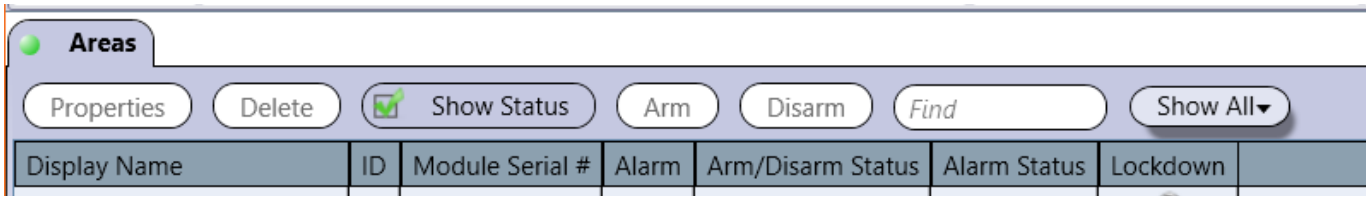
The ATRIUM Access Control System differs from all the other access control system on the market today. The existing access control system determines access levels based on a door to door basis while ATRIUM determines access levels based on areas delimited by doors. This new method greatly simplifies the programming of the system. Since an area (room) can consist of many doors, with ATRIUM, you only need to tell the system that a group of user has access to this room (area) or not and not which door of this room. In some installations, some rooms can have 10 or more access points (doors). With ATRIUM, as soon as you tell the system that a group of user (access levels) have access to this room, all the door leading to this room are added. This is also a great innovation when adding a new door between two rooms (areas). Since you have already defined the access levels based on areas (rooms), when you add a new door between two existing areas, you do not need to modify any of the access levels. The programming is already done, no need to add this door to the access level. Adding a door thus becomes very simple and very efficient.

Example of Areas



The ATRIUM system then decides to grant access, or not, to a door only if the destination room (area) is accessible to this user (defined in his access level) within the defined access schedule (also defined in the access level). This principle is similar to crossing borders between countries. The country decides if you are allowed to enter insides its borders or not; the same applies to the ATRIUM access control system which decides if you are allowed to enter in the room (area) or not based on access levels, access schedules and other conditions.

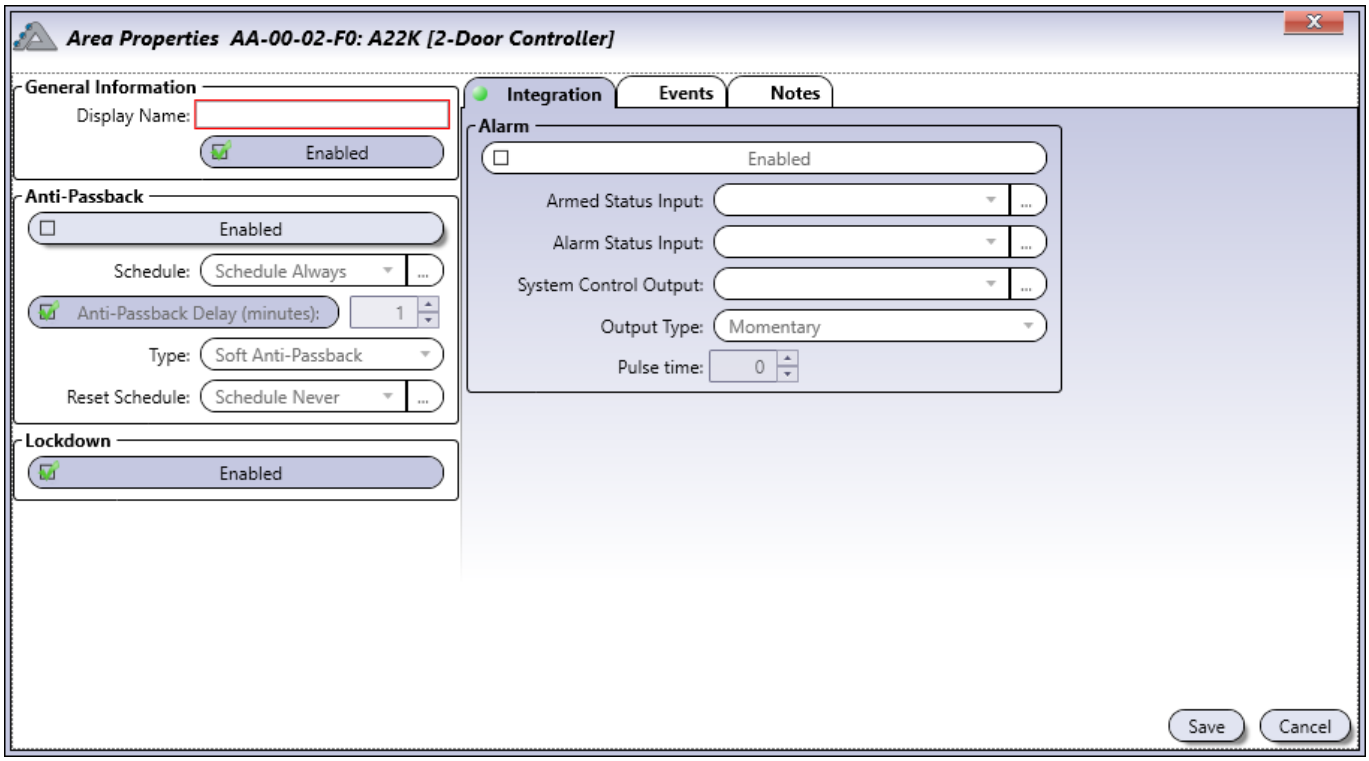
From the ***Dashboard*** tab, click on the ***Areas*** tab. From this page, areas may be added, edited, and deleted.



By default one ***Area*** per door is defined.

CONFIGURING AN AREA

From the ***Hardware*** tab, click on the ***System Overview*** icon. Under the master controller menu list, select ***Areas*** then click on the ***Properties*** button.



General Information

- **Display Name:** Identifies the area throughout the ATRIUM software. We recommend using a name that is representative of the area.

Anti-Passback

You can use anti-passback to closely monitor the movements of users and prevent any tailgating. Tailgating occurs when a user does not use a card at the reader and enters through the door opened by another user who has already used their card. To use this feature, each door of the selected area must have readers on each side. When a user present is card to an "Entry reader", the system labels the user as in. The next time the user present is card, it must be presented to an "Exit reader", in which case user will be labeled as out. Two subsequent Entries or two subsequent Exits will cause the system to generate the appropriate Access Denied - Anti-passback violation event.

- **Enabled:** When selected, indicates that the anti-passback is active.
- **Schedule:** Select on which schedule the anti-passback will be operational.
- **Anti-passback delay (minutes):** Anti-passback delay prevents user from entering the same area twice during a set time duration. This is useful where there is an exit button or turnstile and no "Exit reader". It would prevent a user being able to enter an area and hand their card immediately to a friend or colleague to also gain entry.
- **Type:** There are two anti-passback mode, soft and hard. The soft mode will generate an event and access will be granted, while hard mode will generate an event and the access will be denied.
- **Reset Time:** Select on which schedule the anti-passback will reset. Each user that are within the sector will be given to unknown at the start of each period included in the selected schedule.
- **Lockdown:** When selected, indicates lockdown will be enabled for the area.

Integration Tab

These settings are for the intrusion integration feature and allows each card readers or keypads associated within the area, to arm and/or disarm an intrusion alarm panel.

These setting will apply only if the "Intrusion (Alarm) Integration" feature has been enabled. Refer to page 119 on how to activate this feature.

- **Enabled: C**heck to activate this area to arm and disarm the intrusion alarm panel.
- **Arm Status Input:** Select the input that will be used to monitored the "Arm Status"
- **Alarm Status Input::** Select the input that will be used to monitored the "Alarm Status"
- **System Control Output:** Select the relay output that will be used to arm or disarm the intrusion alarm panel.
- **Output Type:** Select the relay output type. Typically, momentary output is used for key switch arming input (Refer to the intrusion alarm panel manual for output options).
- **Pulse Time:** Enter the relay output pulse delay (in second) that you need for the keyswitch arming input. Typically, 1 second.

Events Tab

The ***Events*** tab lists in real-time the selected area events. Refer to "Events" on page 64 for more information.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING AN AREA

Select an area from the list and click on the ***Properties*** button. See "Adding an Area" on page 40 for more information.

DELETING AN AREA

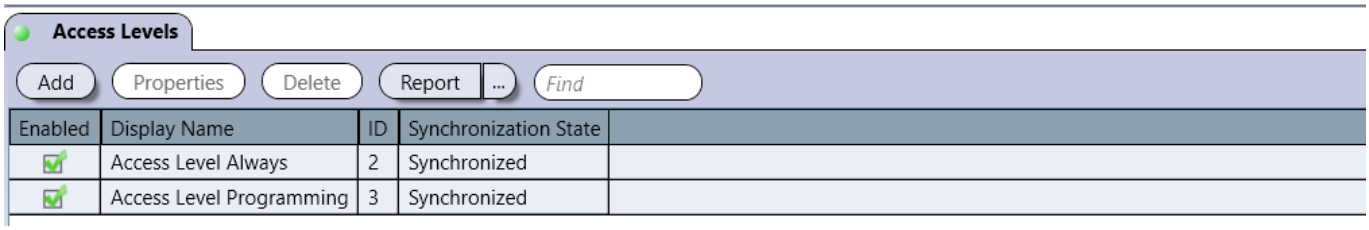
To delete an existing area, select the area from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

ACCESS LEVELS

Access levels determine which areas in the building a user will have access to and during which schedules. This is done by enabling the access level and then assigning a schedule to each area.

In order to define access levels, make sure that the schedules and areas are well defined. By default, there are two schedules defined, always and never, and one area per door is defined.

From the Dashboard tab, click on the ***Access Levels*** icon. From this page, access levels may be added, edited, and deleted.

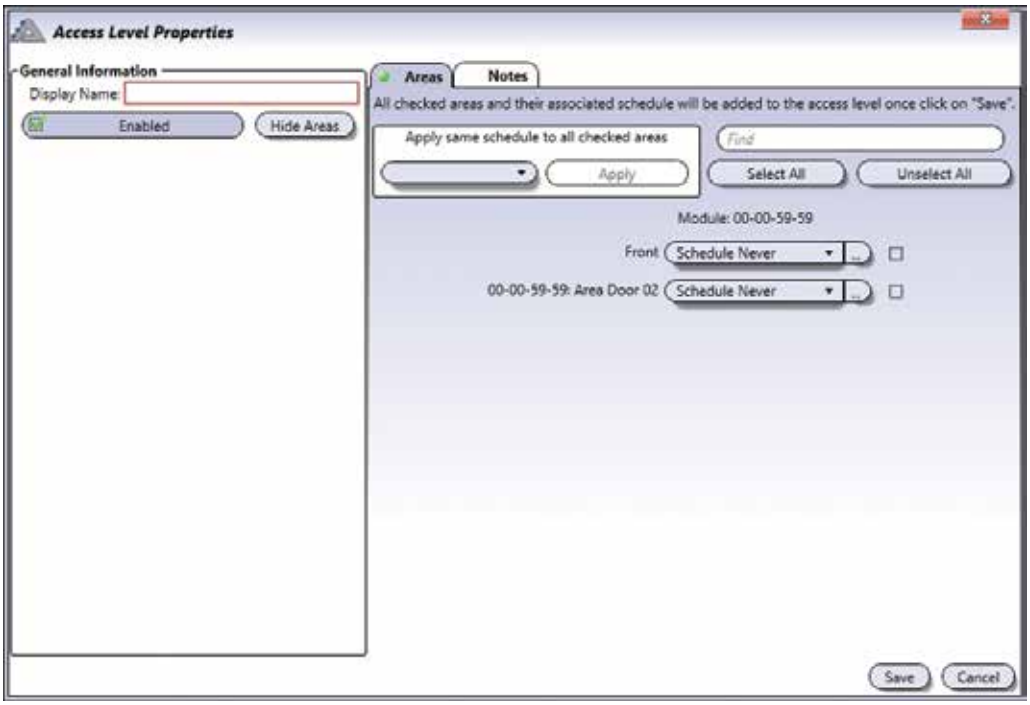


By default the following access levels are defined:

- **Access Level Always:** This access level has the Schedule Always assigned to all areas meaning that the access is valid 24 hours a day, 365 days per year including any programmed Holidays. This access level cannot be modified or deleted.
- **Access Level Programming:** This access level has the Learning Mode schedule assigned to all areas meaning that the access is by default valid 24 hours a day, 365 days per year including any programmed Holidays. This can be modified.

ADDING AN ACCESS LEVEL

From the Dashboard tab, click on the ***Access Levels*** tab and click on the ***Add*** button.



General Information

- **Display Name:** Identifies the access level throughout the ATRIUM software. We recommend using a name that is representative of the access level.
- **Enabled:** When selected, activates the access level.
- **Hide/Show Areas:** Click to show or hide areas.

Areas Tab

Assign a schedule to each area (doors) to determine which areas in the system a user, having this access level, will have access to and during which periods. As for example, production employees will have access to their department between 9 a.m. and 5 p.m. from Monday to Friday. But will not have access to research and development, marketing or all other departments. An access level can be used for a group of users.

Areas (page 39) and Schedules (page 34) must be defined before creating access levels.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING AN ACCESS LEVEL

Select an access level from the list and click on the ***Properties*** button. See "Adding an Access Level" on page 42 for more information.

DELETING AN ACCESS LEVEL

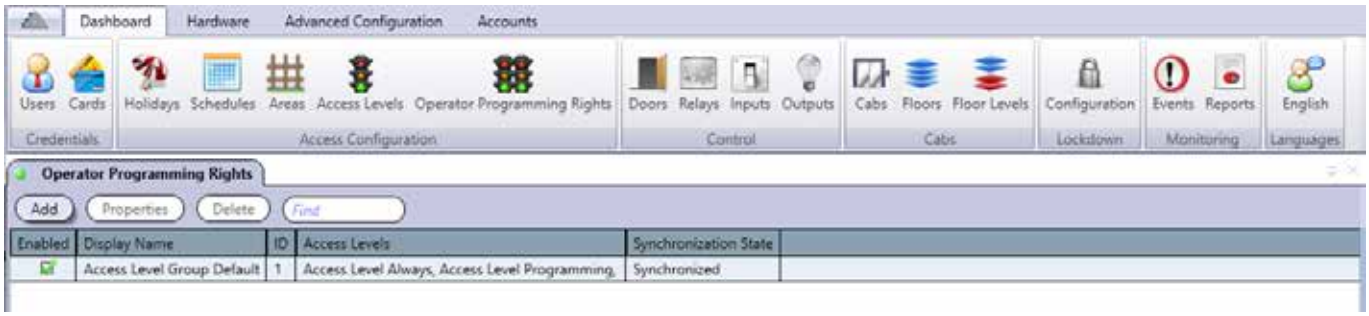
To delete an existing access level, select the access level from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation. The Access Level Always cannot be deleted.

OPERATOR PROGRAMMING RIGHTS

Operator programming rights determine which access levels a user with "Operator" rights will have access to create users and cards. This is done by creating a group of access levels.

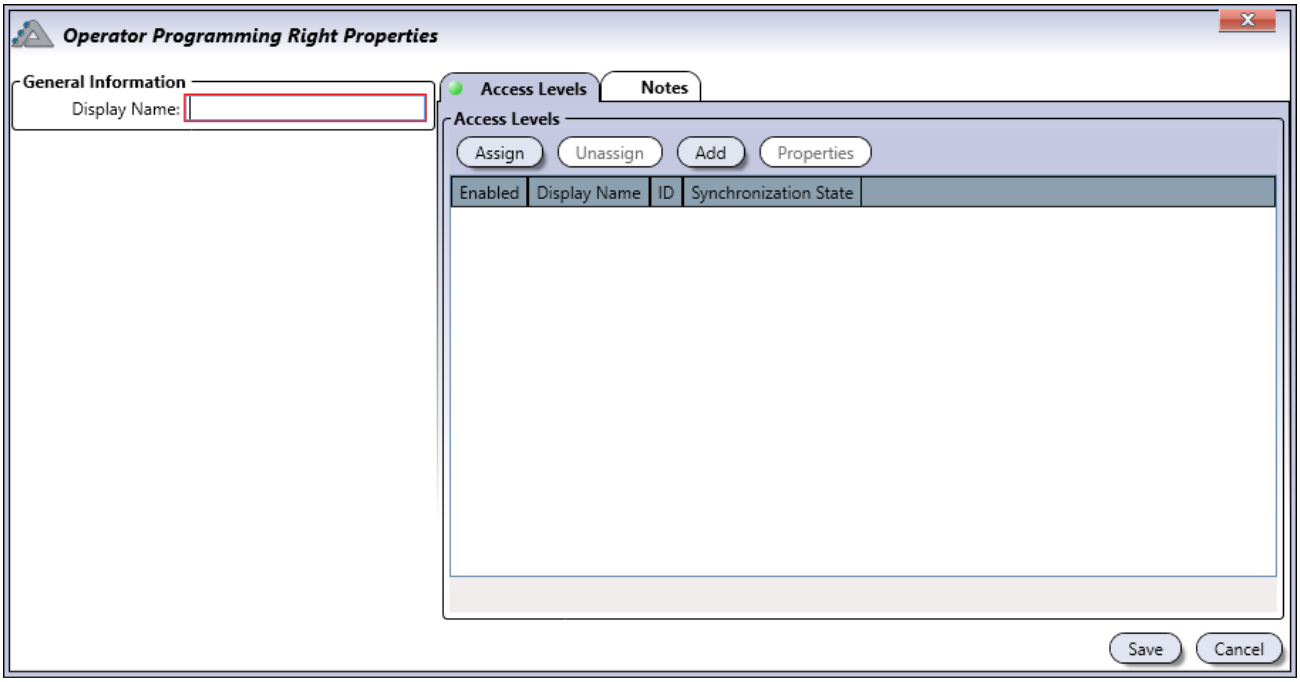
In order to define operator programming rights, you must first create access Levels.

From the Dashboard tab, click on the ***Operator Programming Rights*** icon. From this page, operator programming rights may be added, edited, and deleted.



ADDING AN OPERATOR PROGRAMMING RIGHTS

From the Dashboard tab, click on the ***Operator Programming Rights*** tab and click on the ***Add*** button.



General Information

- **Display Name:** Identifies the access level throughout the ATRIUM software. We recommend using a name that is representative of the access level.

Access Levels Tab

Assign access levels to which the operator will have access to create users and cards.

Access levels (page 42) must be defined first.

- **Assign:** Click on the Assign button and select the access level(s) to be assigned to the user. For information, refer to "Access Levels" on page 42. If two or more access levels are assigned to a user, access is granted as long as one of the defined access levels is valid when the card is presented.
- **Unassign:** Select an access level from the list and click on the Unassign button to revoke this access level for the user.
- **Add:** Allows to define a new access level. Click on the Add & Assign button to add a new access level. Refer to "Adding an Access Level" for more information.
- **Properties:** Allows to edit an access level. Refer to "Adding an Access Level" on page 42 for more information.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING AN OPERATOR PROGRAMMING RIGHTS

Select an operator programming rights from the list and click on the ***Properties*** button. See "Adding an Operator programming rights" on page 44 for more information.

DELETING AN OPERATOR PROGRAMMING RIGHTS

To delete an existing operator programming rights, select the operator programming rights from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

DOORS

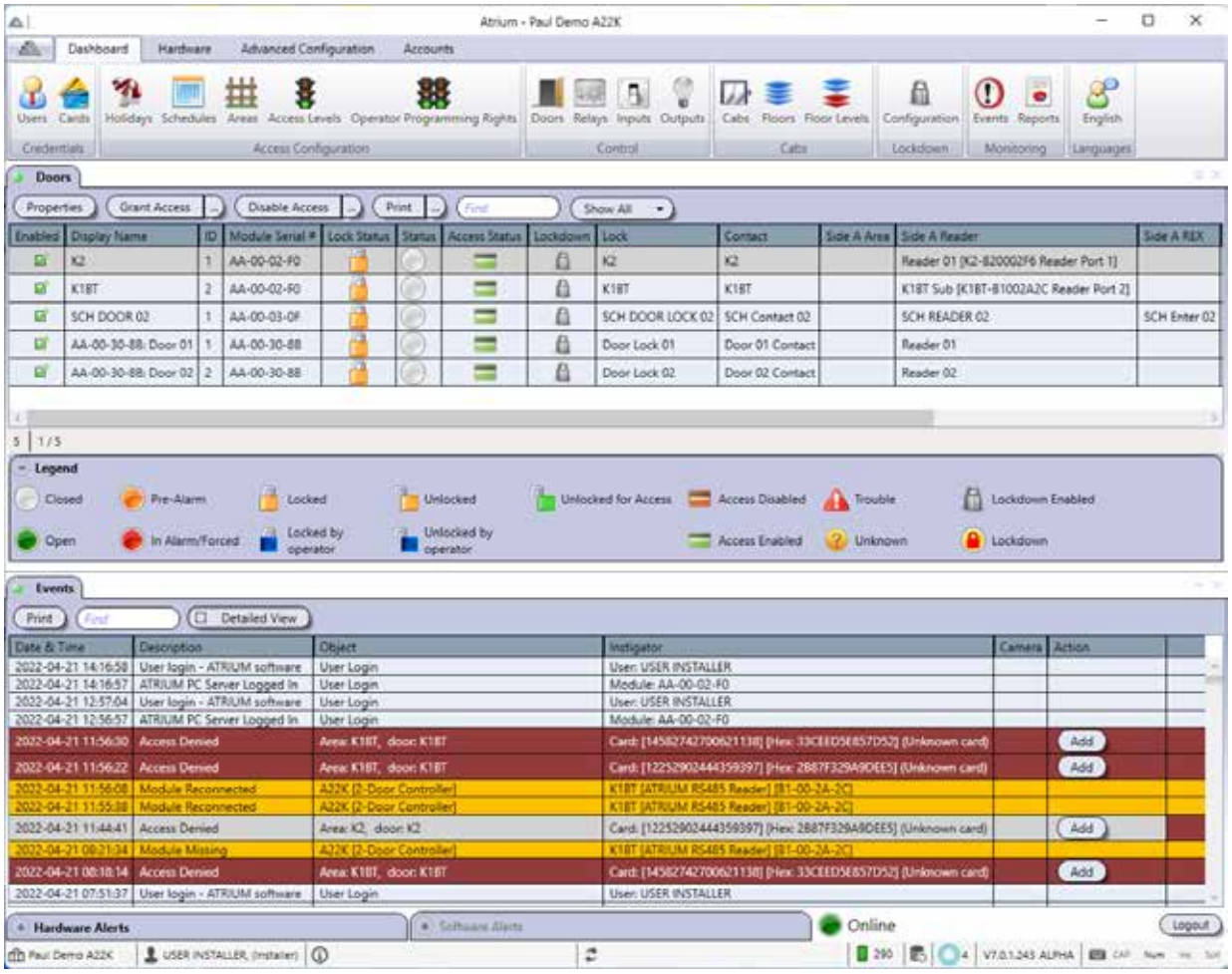
The term door refers to any access point controlled by a reader and/or keypad such as a door, turnstile, gate, and wireless or wired door handles. To control entry and exit through an access point (door), a reader and/or keypad can be used on both sides of the door.

The use of door contacts on all controlled doors is recommended, as they greatly improve the level of security provided by an access control system. Many of the door's programmable options can only be used if a door contact is installed.

Each 2-Door controller supports two readers and up to four 2-Door Expansion Modules, which provide an additional 2 doors each. Therefore, each controller can monitor the state of up to 10 doors.

From the ***Dashboard*** tab, click on the ***Doors*** icon. All Atrium controller, subcontroller and expander doors are listed here. Use the **Legend** to quickly identify the door status.

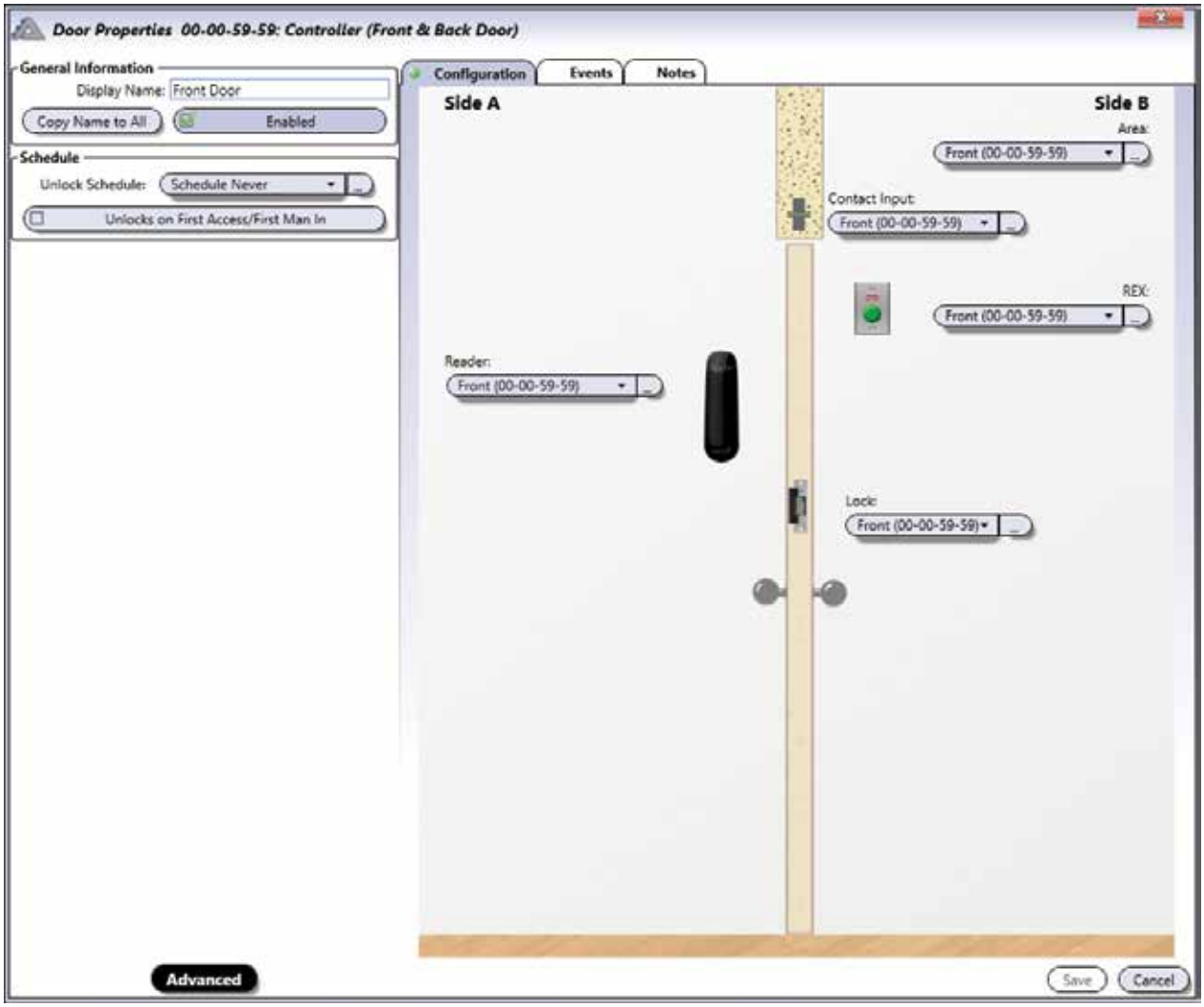
To access doors per controller, subcontroller or expander, refer to "System Overview" on page 70.



LEGEND for	ICON	NAME	DESCRIPTION
Door Status		Closed	Indicates that the door is closed.
		Open	Indicates that the door is opened.
		Pre-Alarm	Indicates that the door has been opened for too long. This state lasts until either the door is closed, returning its status to Closed, or the Open Too Long alarm expires, changing the door's status to In Alarm/Forced.
		In Alarm/Forced	Indicates that the door is forced open or was left opened too long.
Lock Status		Locked	Indicates that the door is locked following its programmed parameters.
		Locked by Operator	Indicates that the door has been manually locked by the operator.
		Unlocked	Indicates the door is unlocked following its programmed parameters.
		Unlocked by Operator	Indicates that the door is manually unlocked by the operator.
		Unlocked for Access	Indicates that the door is unlocked following a valid access event.
Access Status		Access Disabled	Access to the door has been manually de-activated by the operator.
		Access Enabled	Access to the door is allowed following its programmed parameters.
		Trouble	Indicates that the ATRIUM software is not able to retrieve the status of an expander's door contact because the module is probably turned off.
		Unknown	Indicates that either the module is not synchronized or the module has an older firmware version that is not compatible with the ATRIUM software.
Lockdown Status		Lockdown Enabled	Indicates that the door will remain locked following the activation of a "Lockdown".
		Door is in Lockdown	Indicates that the door is in "Lockdown".

MODIFYING A DOOR

From the Dashboard tab, click on the ***Doors*** icon, then select a door in the list and click on the ***Properties*** button. Configureable options in the **Door Properties** are listed below.



Basic and Advanced View

General Information

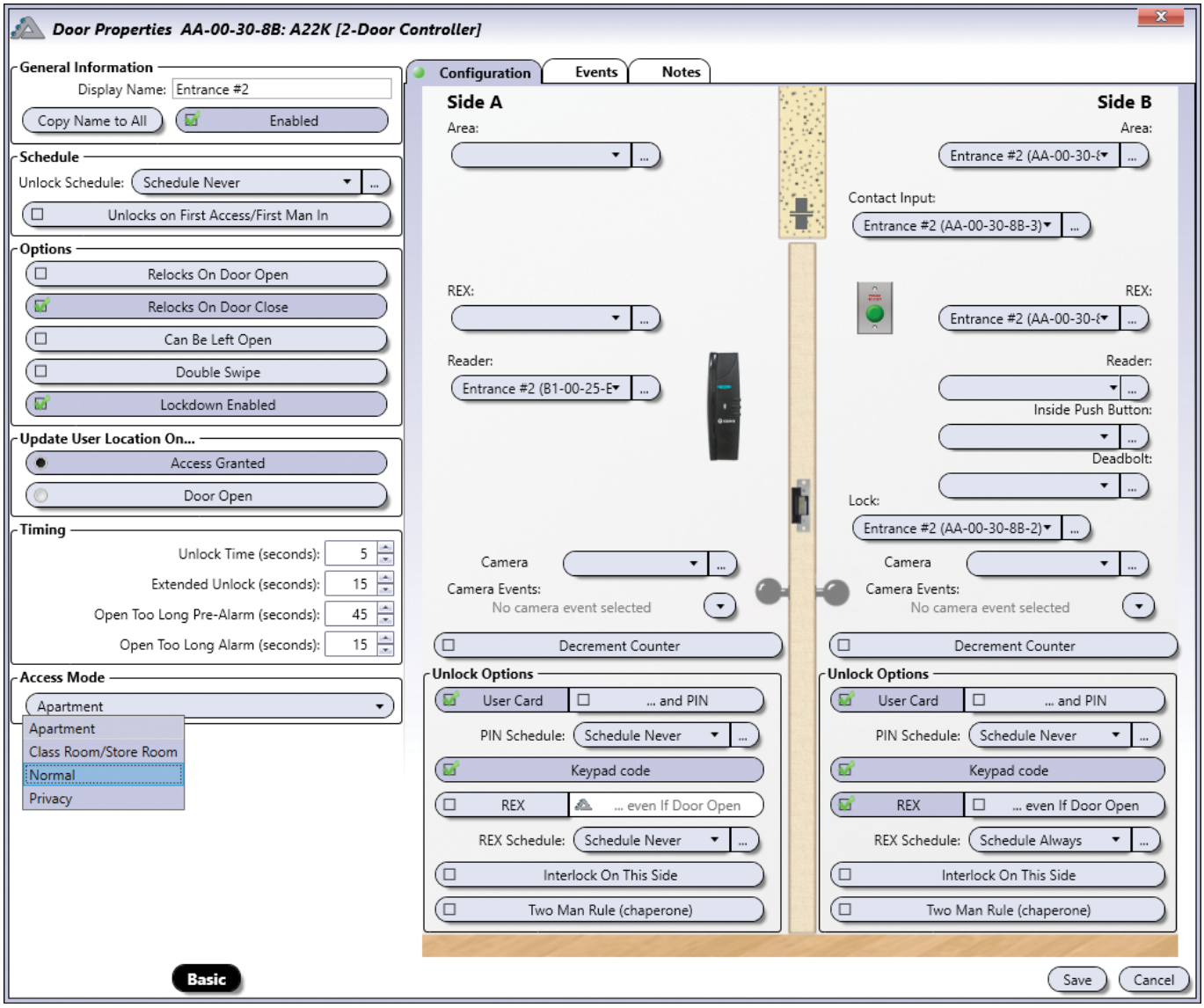
- **Display Name:** Identifies the door throughout the ATRIUM software. We recommend using a name that is representative of the door.
- **Copy Name to All**: Automatically copies the ***"Door Display"*** name to the door components (Contact, Rex, Reader & Lock)
- **Enabled:** When selected, activates the usage of this door.

Schedule

- **Unlock Schedule:** Select the schedule during which the door will automatically unlock. For example, you may want a door to remain unlocked from 9 a.m. to 5 p.m. Monday to Friday. To do so, create the appropriate schedule and select it from the Unlock Schedule drop-down list. Refer to "Schedules" on page 34 for more information.

- **Unlocks on First Access/First Man In:** Select the Unlocks on First Access/First Man In check box to prevent the door from unlocking automatically until the first user with valid access presents his card at the door.

Advanced View Only



Options

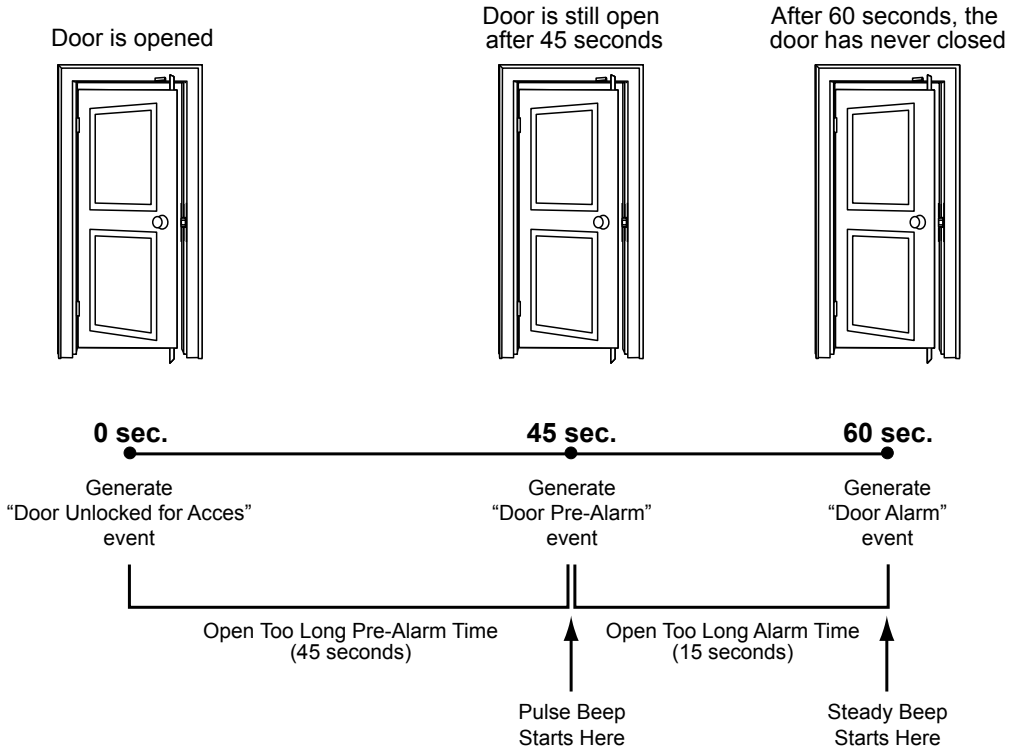
- **Relocks on Door Open:** Select the Relocks On Door Open check box to relock the door as soon as it opens. When the check box is cleared, the system relocks the door when the unlock time has elapsed (see Unlock Time).
- **Relocks on Door Close:** Select the Relocks On Door Close check box to relock the door as soon as the door closes.
- **Can be Left Open:** Select the Can be Left Open check box to allow a door to stay open without generating a door open too long alarm.
- **Double Swipe:** Select the Dual Badge check box to relock the door during its unlock time (including on an unlock schedule) or to arm a burglar alarm system (see page 119 for alarm integration). The ”Unlock on First Access/First Man In” option must be activated for “Dual Badge” to function.
- **Lockdown Enabled:** When selected, the lockdown feature will be enabled for the door.

Update User Location On...

- **Access Granted:** Select the Access Granted check box to update the user’s location upon an access granted.
- **Door Open:** Select the Door Open (Contact) check box to update the user’s location upon a door opening. To use this option, a door contact must be installed on the selected door.

Timing

- **Unlock Time (seconds):** Enter a value between 1 and 254 seconds (Default: 5 seconds). Represents the amount of time the door will remain unlocked when an access granted or unlock event is generated at the door.
- **Extended Unlock (seconds):** When a user is granted access, the controller will unlock the door for the period defined by the Unlock Time. However, if the user has been programmed with the extended time allowed (see Allow Extended Time on page 18), the controller will unlock the door for the duration of the Unlock Time in addition to the value programmed in the Extended Time. In the Extended access text field, type a value between 1 and 254 seconds (Default: 15 seconds). This option is particularly useful for individuals that may require more time to access the door.
- **Open Too Long Pre-Alarm (seconds):** Before generating an Open too long event, the controller can be programmed to generate a pre-alarm as a warning of the upcoming alarm. Enter a value between 1 and 254 seconds (Default: 45 seconds) that represents the amount of time a door can remain open after an access granted or door unlock event before generating a door left open event.
- **Open Too Long Alarm (seconds):** Enter a value between 1 and 254 seconds (Default: 15 seconds) that added with the Open Too Long Pre-Alarm value represents the amount of time a door can remain open after an Access Granted or Door Unlock event before generating a Door Open Too Long event (see example on page 49).



Access Mode

Access Modes provide additional ways to secure access when using wireless and wired electronic door handles. Classroom mode does not require an electronic door handle.

The Interior Push Button (IPB) and door handle allow egress in any of these door modes.

- **Normal:** This is the default access mode. The door is always locked and can be unlocked by a valid credential for the duration of its unlock time (five seconds by default).
- **Classroom/Store Room:** A valid credential presented to the outside reader toggles the lock status to locked or unlocked.
- **Privacy:** Pressing the Inside Push Button (IPB) disables credential access. Opening the door or pressing the IPB a second time enables credential access.
- **Apartment:** The Interior Push Button (IPB) toggles the lock status to locked or unlocked. Opening the door toggles the door status to unlocked. While unlocked, the door can be locked again by closing the door first, then pressing the IPB or by presenting a valid credential to the outside reader. Access with a valid credential is always allowed.

Configuration Tab - Side A and Side B

Allows to define the options for devices on both sides of the door: Side A and Side B.

Area: Select the area from the list for each side of the door. Leave the field empty if the side of the door is outside the building.

Contact Input: Select the door's contact from the list.

REX: If there is a REX associated with this side of the door, select the REX from the list, otherwise leave the field empty.

Reader: If there is a reader associated with this side of the door, select the door from the list, otherwise leave the field empty.

Inside Push Button (IPB): Select the input being used for your IPB here.

Deadbolt: Select the input being used to monitor the deadbolt here. If the input is selected, the outside reader will be disabled when the deadbolt is locked. When the deadbolt is unlocked, the outside reader is enabled.

The **«Inside Push Button (IPB)»** and **«Deabolt»** features only appear when the Access Mode is either in Classroom / Store Room, Privacy or in Apartment mode. See page 51 for the different descriptions of Access Mode.

Lock: Select the door's lock from the list.

Camera: Select the door's camera from the list.

Camera Events: Select the camera event(s) from the list to be recorded.

Decrement Counter: When selected, the door will count down the uses of a card or PIN.

Unlock Options

- **Card:** When selected, allows to use a card to access this door. Used when a reader is installed at the door
- **... and PIN:** When selected, specifies that the user, after presenting his card, has to enter a PIN (Personal Identification Number) on the door keypad to access this door. Refer to "Keypad Code" on page 19 for more information. Used when both a reader and a keypad are installed for this door.
- **PIN Schedule:** Allows to select the schedule that will specify when the PIN can be used.
- **Keypad Code:** When selected, allows to use a PIN (Personal Identification Number) to access this door. Refer to "Keypad Code" on page 19 for more information. Used when a keypad is installed.
- **REX:** When selected, unlocks the door when the controller receives a valid Request for Exit (the door must be closed and locked when the option "... even if Door Open" is not selected).
- **... even if Door Open:** When selected, unlocks the door regardless of its current status (i.e. Door forced, Door open too long, etc.) when receiving a valid request for exit (REX).
- **REX Schedule:** Allows to select the schedule that will specify when the REX can be used.
- **Interlock On This Side:** When selected, it activate interlock mode. This feature allows you to set up the doors, within the same area, for use with Interlock (Mantrap) applications. A "mantrap" consists of two or many doors, each controlled by a card reader and/or keypad. When one of the doors is open or unlock, it is impossible to open the other door until all interlock doors are closed. An input is required if the door will be used in a "mantrap" configuration.
- **Two Man Rule (chaperone):** When selected, two different users will have to present their cards one after the other, within 10 secondes, to unlock the door.

Events Tab

The ***Events*** tab lists in real-time the events associated to this door. Refer to ***Events*** on page 64 for more information.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

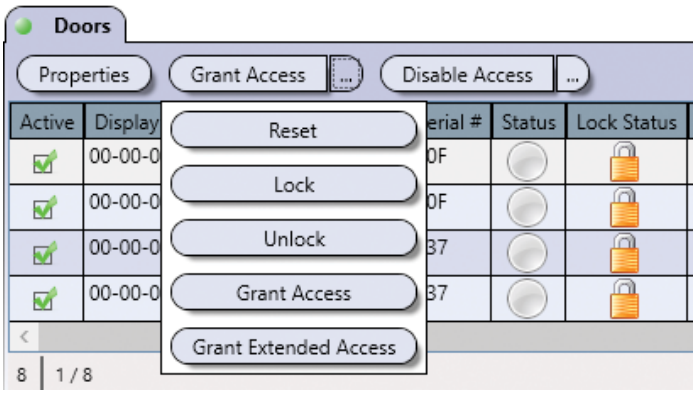
The following buttons change the state of a door. These changes override the normal scheduled state. To cancel the override command, click on the ***Reset*** button.

DOOR CONTROL BUTTON

The following button allows to manually control the access to this door.

Reset

Cancels the operator's override door control, returning the door to its current scheduled state.



Lock

Manually locks the selected door if it was unlocked either on schedule, manually or by an operator.

Unlock

Manually unlocks the selected door, overriding its scheduled state. The door will remain unlocked permanently. Use the ***reset*** button to enable schedule settings.

Grant Access

Manually unlocks the selected door temporarily for the period specified by the door's ***Unlock Time.***

Grant Extended Access

Manually unlocks the selected door for the period corresponding to the addition of the door's ***Unlock Time*** and ***Extended*** Timeperiods.

DOOR ACCESS BUTTON

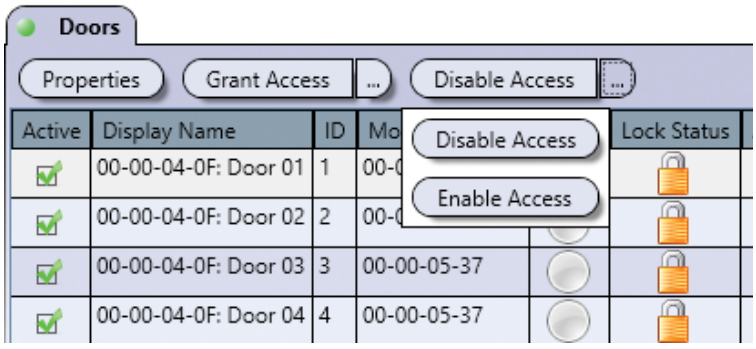
Allows to manually activate or deactivate the access to this door.

Disable Access

Manually revokes the access to this door by disabling its readers and REX devices.

Enable Access

Manually returns the door to its programmed parameters.

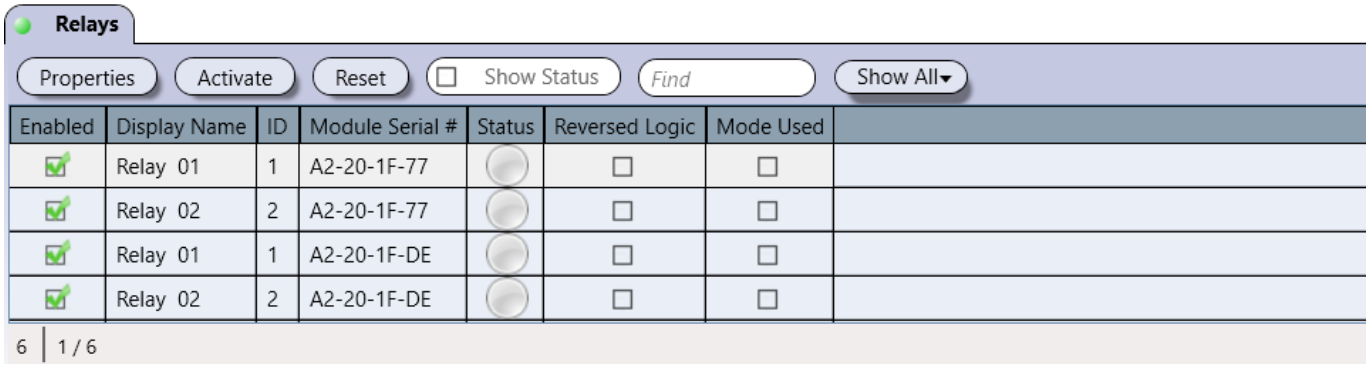


RELAYS

Typically, relays are used to activate alarm sounders or other devices such as lighting control units and air conditioners. Relays are controlled using macros. For example, a relay can be activated by a macro when the trigger event occurs whithin the schedule (refer to “Macros” on page 93).

The controller includes two relay outputs.

From the ***Dashboard*** tab, click on the ***Relays*** icon. From this page, relays may be edited, manual control may be applied and live status may be displayed.



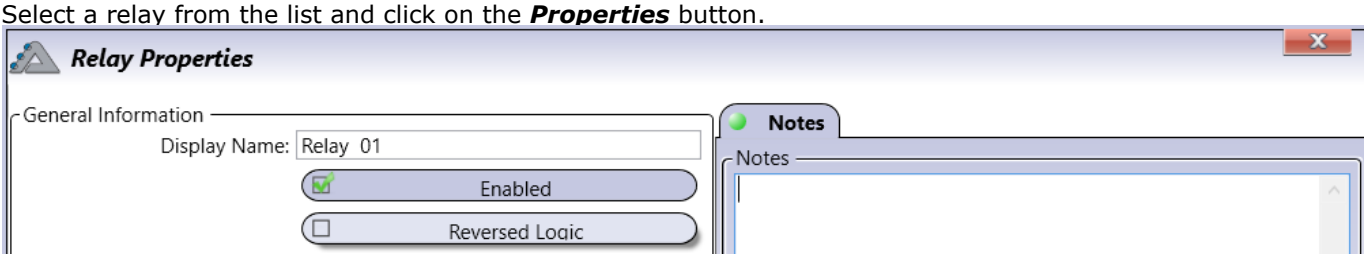
Relays are only used with macros, refer to “Macros” on page 93 for more information.

Legend

ICON	NAME	DESCRIPTION
	Inactive	Indicates that the relay is not activated.
	Enable	Indicates that the relay is activated.
	Timed Activation	The relay has been activated for a set time period and will deactivate when the period expires.
	Unknown	Indicates that either the module is not synchronized or the module has an older firmware version that is not compatible with the ATRIUM software.

MODIFYING A RELAY

Select a relay from the list and click on the ***Properties*** button.



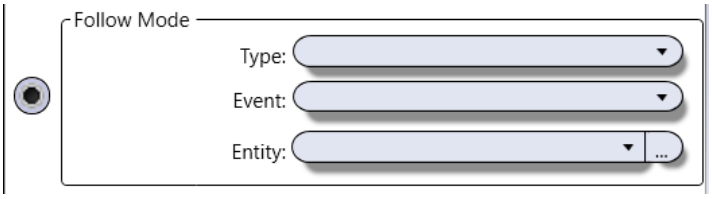
General Information

- **Display Name:** Identifies the relay throughout the ATRIUM software. We recommend using a name that is representative of the usage of this relay.
- **Enabled:** When selected, enables the usage of this relay.
- **Reversed Logic:** When selected, reverses the logic from either normally closed (N.C.) to normally open (N.O.) or vice-versa. Refer to Jumper Settings from the module instruction manual for more information on N.C. and N.O.

A relay can be set through one of two available modes:

Follow Mode

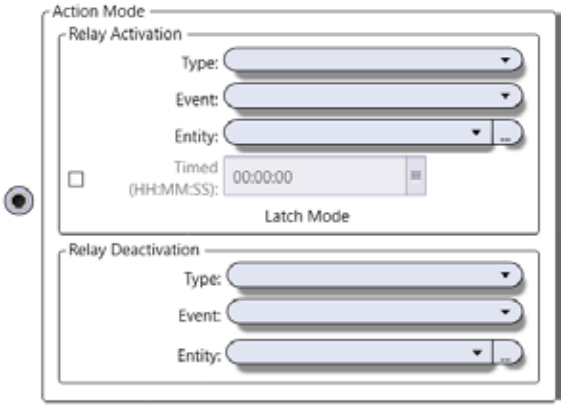
The relay will activate and remain activated when the status of the selected type is in alarm (input in alarm) or active (output or schedule).When the input alarm, output status changes or the schedule expires, the relay deactivates automatically.



- Select one type, one event, and one entity from the list

Action Mode

In Action Mode, a seperate action can be programmed to activate and/or deactivate the relay.



- **Relay Activation:** Select the type, event and entity from the list that will activate the relay.
- **Timed:** When selected, a timer can be set for the relay by entering the desired time (hh:mm:ss)
- **Relay Deactivation:** Select the type, event and entity from the list that will deactivate the relay.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

RESET

Cancels the operator's override relay control, returning the relay to its current scheduled or event state.

ACTIVATE

Manually activates the relay, overriding its current scheduled or event state.

INPUTS

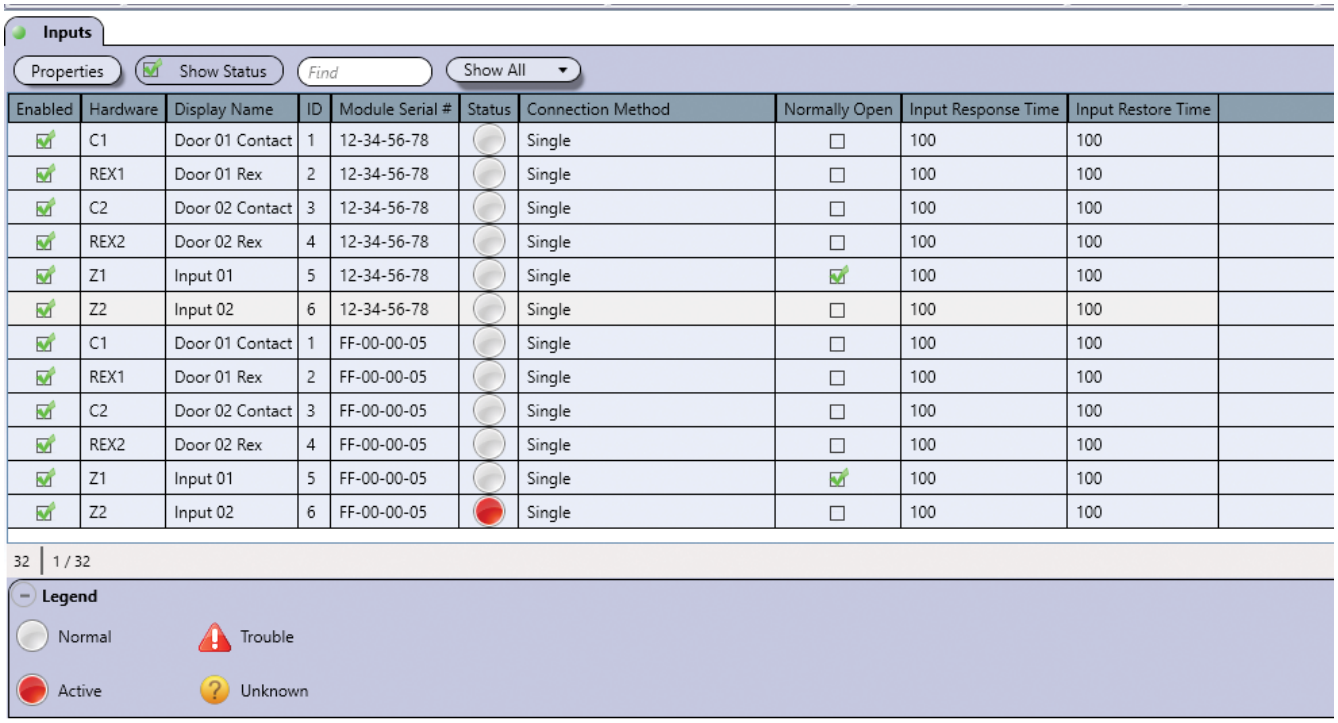
Typically, the inputs are used to monitor the status of door contacts and request for exit devices installed on the controlled door. Inputs can activate relays reader outputs or the bell outputs through the use of macros.

Each ATRIUM controller has 6 inputs. 4 are dedicated, 2 per door, one input for the door contact and one for the request to exit. In addition, 2 general purpose inputs are included with the ATRIUM controller.

Additional general-purpose inputs cans be added with the AIOM Input/Output modules. Each AIOM module provides 10 additional inputs and outputs. Up to 100 inputs and outputs can be monitored by one ATRIUM controller

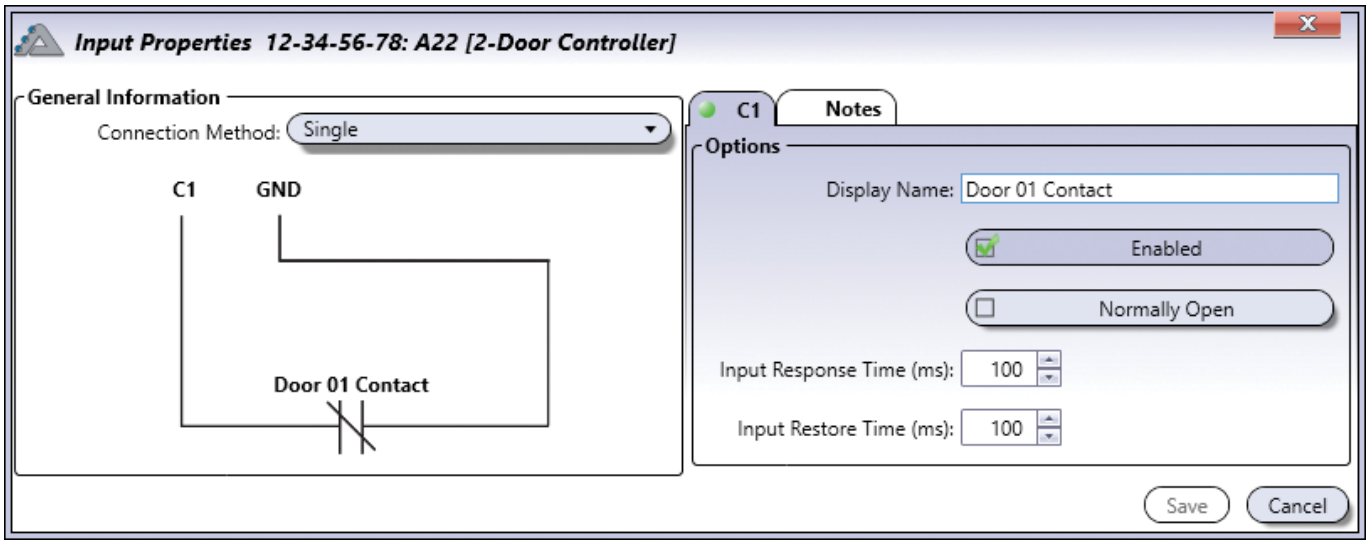
All inputs of the ATRIUM access control system including the ATRIUM controller and all door expanders are listed. To access Inputs per ATRIUM controller or door expander, refer to “System Overview” on page 70.

From the Dashboard tab, click on the ***Inputs*** tab. From this page, inputs may be edited and live status may be displayed.



MODIFYING AN INPUT

From the ***Dashboard*** tab, click on the ***Inputs*** icon, select an input from the list and click on the ***Properties*** button.



Input Tab
(A second input tab will appear when using any of the zone doubling connection methods)

Options

- **Display Name:** Identifies the input throughout the ATRIUM software. We recommend using a name that is representative of the input.
- **Enabled:** When selected, activates the input.
- **Normally Open:** Select this function if you are using a "Normally Open" devices on the input. By default, the inputs are ready for "Normally Closed" devices.
- **Input Response Time (ms):** This delay defines how quickly the controller will respond to the trigger of an opening input. This prevents any momentary glitch from causing unnecessary alarms. If the input remains triggered for the defined time delay, the controller will react according to its programming. The default value is 100ms. Type a value from 0 to 3 600 000 ms (1 hour).
- **Input Restore Time (ms):** This delay defines how quickly the controller will respond to the trigger of a closing input. This prevents any momentary glitch from causing unnecessary zone closure. If the input remains closed for the defined time delay, the controller will consider the inputs as being closed. The default value is 100ms. Type a value from 0 to 3 600 000 ms (1 hour).

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

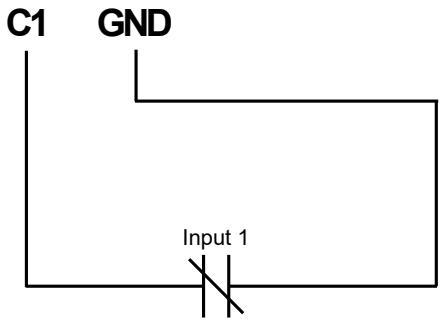
EXAMPLES OF INPUT CONNECTION METHODS

Single (1 Detection Device per Input)

When using this method, only one device is detected by the input. Normally open or normally closed devices can be used. Normally closed circuit shown below.

Here are the different options for a single input configuration:

Single

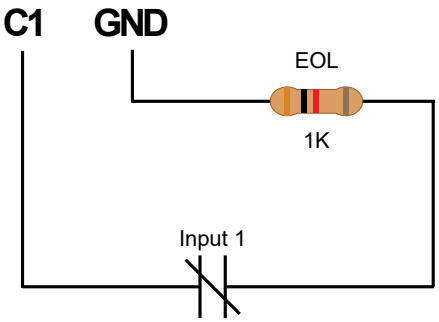


SHORT CIRCUIT supervision: No

WIRE CUT supervision: No

(Factory Default)

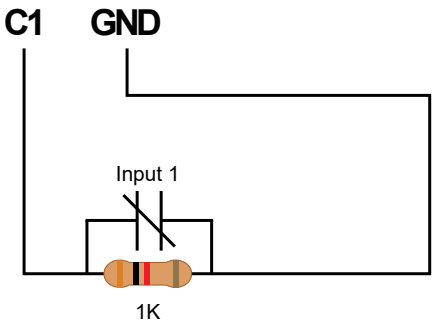
Single with short circuit (EOL) supervision



SHORT CIRCUIT supervision: Yes

WIRE CUT supervision: No

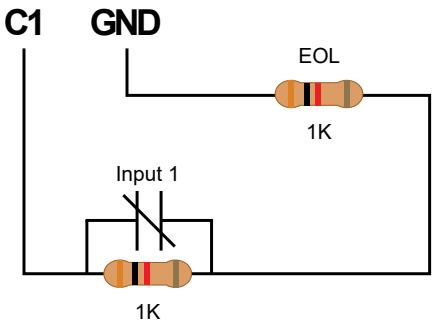
Single with wire cut supervision



SHORT CIRCUIT supervision: No

WIRE CUT supervision: Yes

Single with wire cut and short circuit (EOL) supervision



SHORT CIRCUIT supervision: Yes

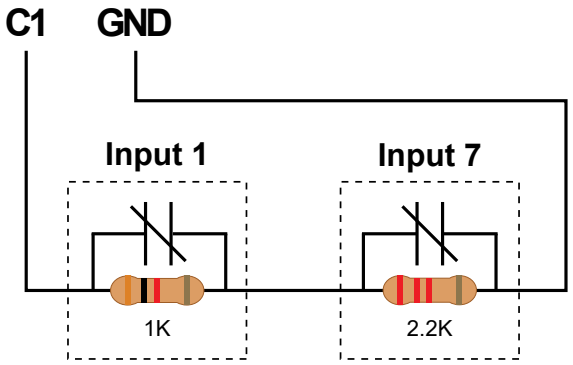
WIRE CUT supervision: Yes

Doubled (2 Detection Devices per Input)

When using this method, two devices are detected by the input. Normally open or normally closed devices can be used. Normally closed circuit shown below.

Here are the different options for a double input configuration:

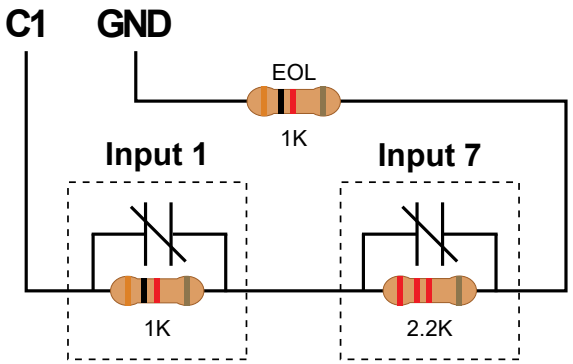
Doubled with wire cut supervision



SHORT CIRCUIT supervision: No

WIRE CUT supervision: Yes

Doubled with wire cut and short circuit (EOL) supervision

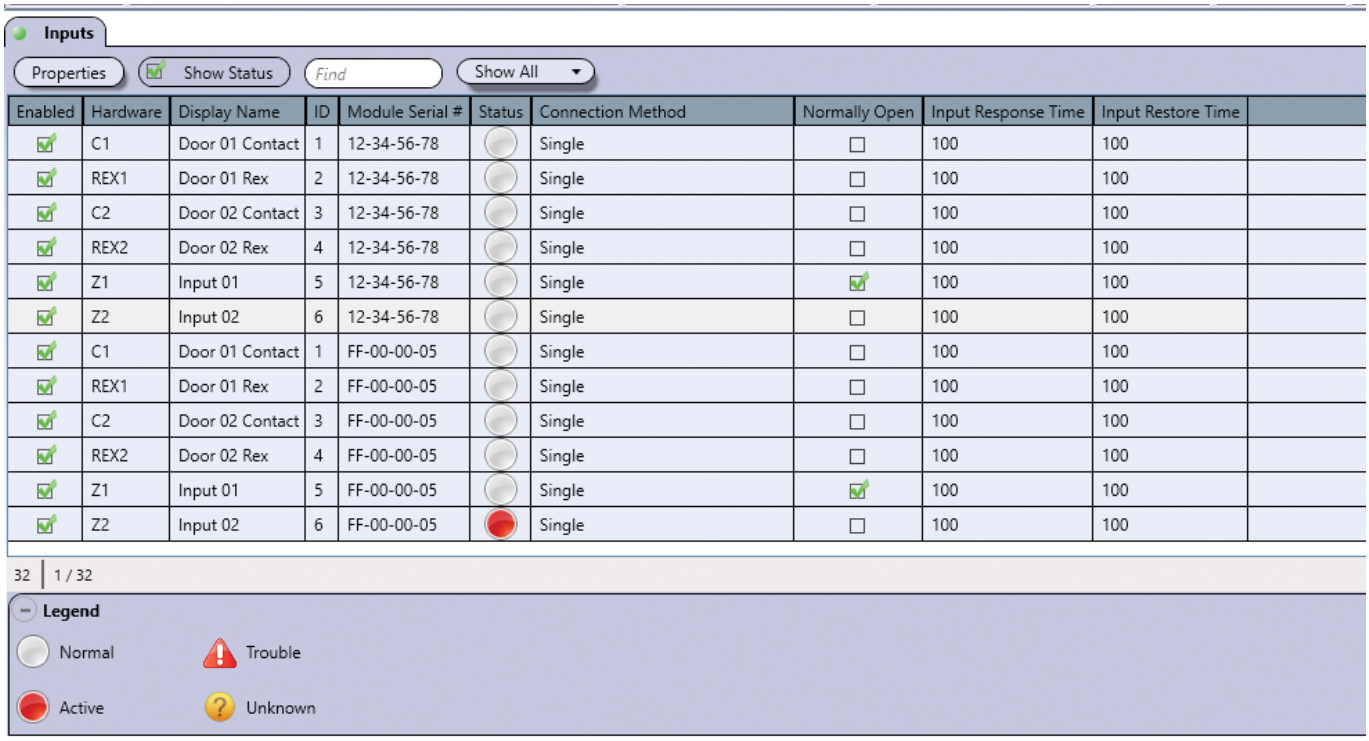


SHORT CIRCUIT supervision: Yes

WIRE CUT supervision: Yes

SHOW STATUS CHECK BOX

When enabled, displays the live status for a period of 5 minutes.



Legend

ICON	NAME	DESCRIPTION
	Normal	Indicates that the input is normal state, not activated.
	Active	Indicates that the input is activated.
	Trouble	Indicates that the state of the input is WIRE CUT or SHORT CIRCUIT.
	Unknown	Indicates that either the module is not synchronized or the module has an older firmware version that is not compatible with the ATRIUM application.

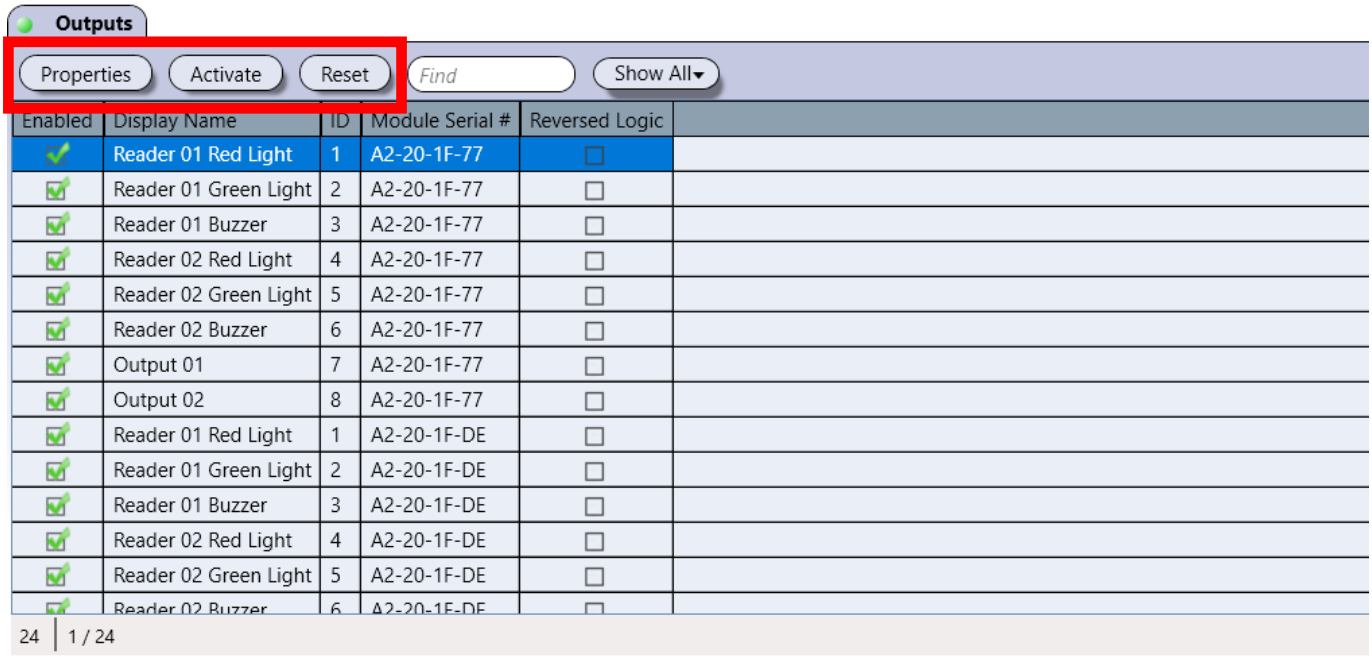
OUTPUTS

By default, the outputs (six per Controller and Expander) are used to control the built-in LEDs and buzzers of card readers and keypads. For example, a red/green indicator on the reader will inform the user that access has been granted (changes from red to green), or the reader buzzer will inform the card user that the door has been left open or the door has been forced open.

Each controller includes six multi-function outputs. Each controller also supports up to four 2-Door Expansion Modules, which provide an additional 6 outputs each.

All outputs of the ATRIUM access control system, including the ATRIUM controller and all door expanders, are listed. To access outputs per ATRIUM controller or door expander, refer to "System Overview".

From the ***Dashboard*** tab, click on ***Outputs***. From this page, outputs may be edited, and manual control may be applied.



PROPERTIES

Opens the "Properties" window of the selected output.

ACTIVATE

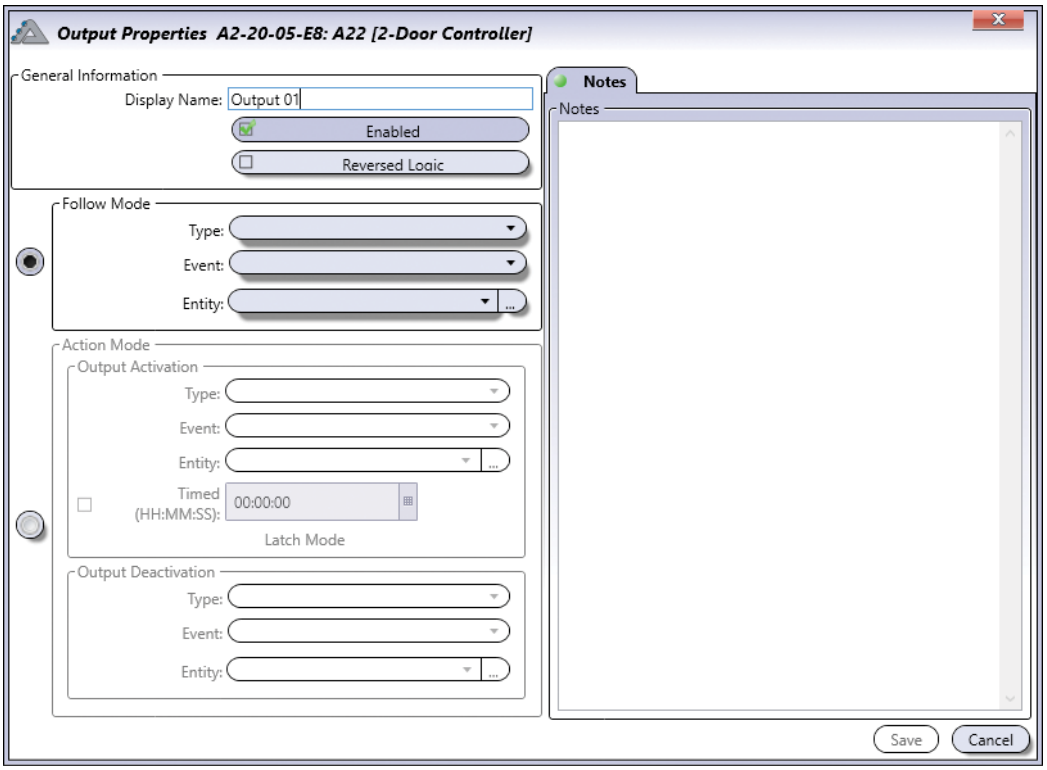
Manually activates the output overriding the activation delay.

RESET

Cancel the override output control, returning the output to its current scheduled or event state.

MODIFYING AN OUTPUT

From the Dashboard tab, click on the ***Outputs*** icon, select an output from the list and click on the ***Properties*** button.



General Information

- **Display Name:** Identifies the input throughout the ATRIUM software. We recommend using a name that is representative of the output.
- **Enabled:** When selected, activates the usage of the output.
- **Reversed Logic:** When selected, reverses the logic from either normally closed (N.C.) to normally open (N.O.) or N.O. to N.C.

Follow Mode: In Follow Mode, the output will be activated/deactivated by following a preset.

- Select one type (inputs, relays or schedules), one event, and one entity from the list

Action Mode: A seperate action can be programmed to activate and/or deactivate the output.

- **Output Activation:** Select the type, event and entity from the list that will activate the output (Timed: when selected, the output will stay activated for the desired time. Output deactivation is not necessary in that case.)
- **Output Deactivation:** Select the type, event and entity from the list that will deactivate the output.

Notes Tab

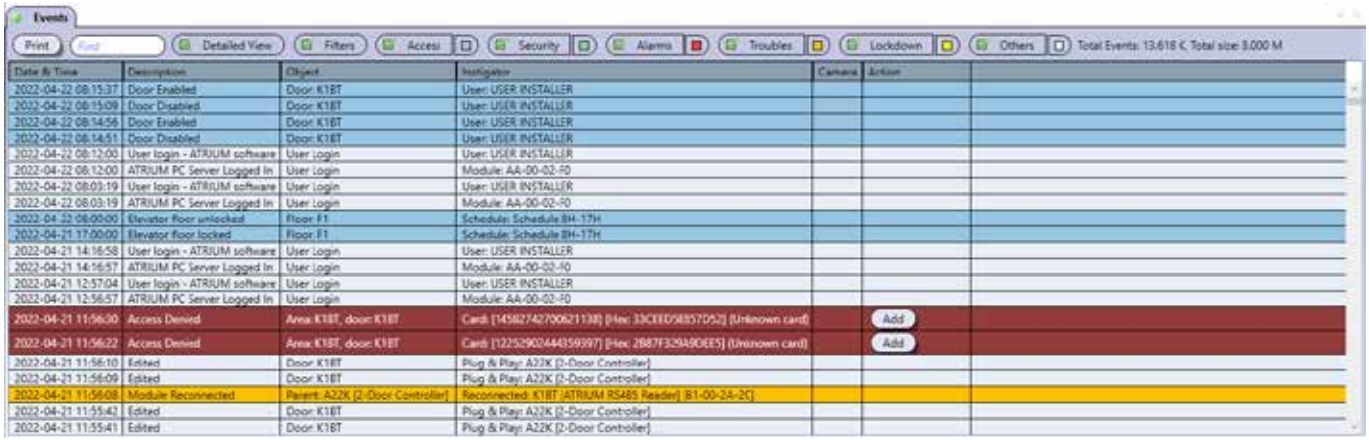
Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

EVENTS

Reports each event that occurs in the system in real-time. A specific event can be programmed to perform an action using the macros (refer to “Macros” on page 93) .

The Events window lists in real-time the events or device status of the ATRIUM system.

From the Dashboard tab, click on the ***Events*** tab or drag up the ***Events*** tab from the bottom of the page. From this page, it is possible to view the event’s details.

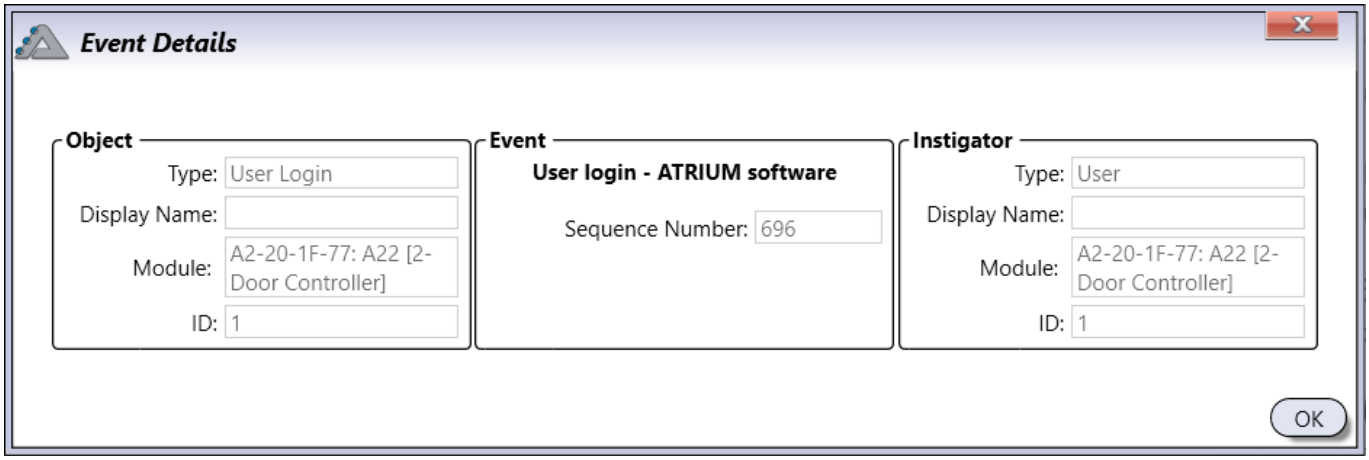


All events are displayed in real time. Use the “Detailed View” button to filter events by category:

- ***Access:*** Displays access-related events when this check box is selected.
- ***Security:*** Displays security-related events when this check box is selected.
- ***Alarms:*** Displays alarm-related events when this check box is selected.
- ***Troubles:*** Displays trouble-related events when this check box is selected.
- ***Lockdown:*** Displays lockdown-related events when this check box is selected.
- ***Others:*** Displays all other events when this check box is selected.

VIEW DETAILED EVENT INFORMATION

Double-click on an event from the list to view its details.



Object

Indicates the provenance of the event.

- Type: Indicates the type of device or component.
- Display Name: Indicates the name of the device or component.
- Module: Indicates which module contains the device or object.
- ID: Indicates which object the event applies to.

Event

Indicates the description of the event.

Sequence Number indicates a sequential number given to each event.

Instigator

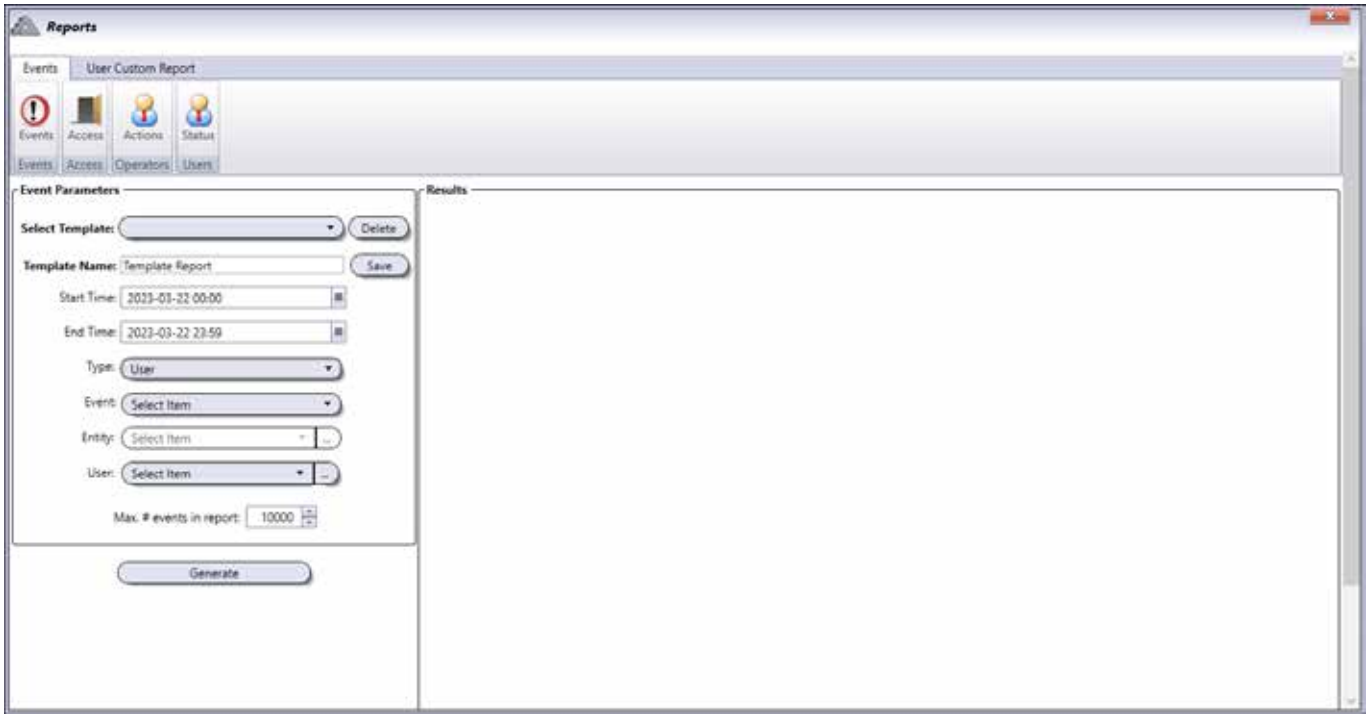
Indicates the instigator of the event

- Type: Indicates the type of instigator.
- Display Name: Indicates the name of the instigator.
- Module: Indicates which module contains the device or object.
- ID: Indicates which object the event applies to.

REPORTS

Generate reports for a specific period of time, user, door and/or area. Reports can also be printed and saved.

From the Dashboard tab, click on the ***Reports*** tab. From this page reports may be generated, viewed, printed and saved.



GENERATING A REPORT

Event Parameters

Select the criteria that will be used to generate the report.

- **Select Template:** Select a previously saved report template
- **Template Name:** Configure your report template according to your needs with the choices below. Type a name then click save to keep the settings for future printing report.
- **Start Time and End Time:** Select the period for the report by entering the start and end date and time using the "yyyy:mm:dd hh:mm" format or select the date and time.
- **Type:** Select one, multiple or all types(s) from the list.
- **Event:** Select one, multiple or all event(s) from the list.
- **Entity:** Select one, multiple or all entity(ies) from the list.
- **User:** Select one, multiple or all user(s) from the list.
- **Maximum # events in report:** Enter the maximum events allowed in the report. The default setting is 1000 events.

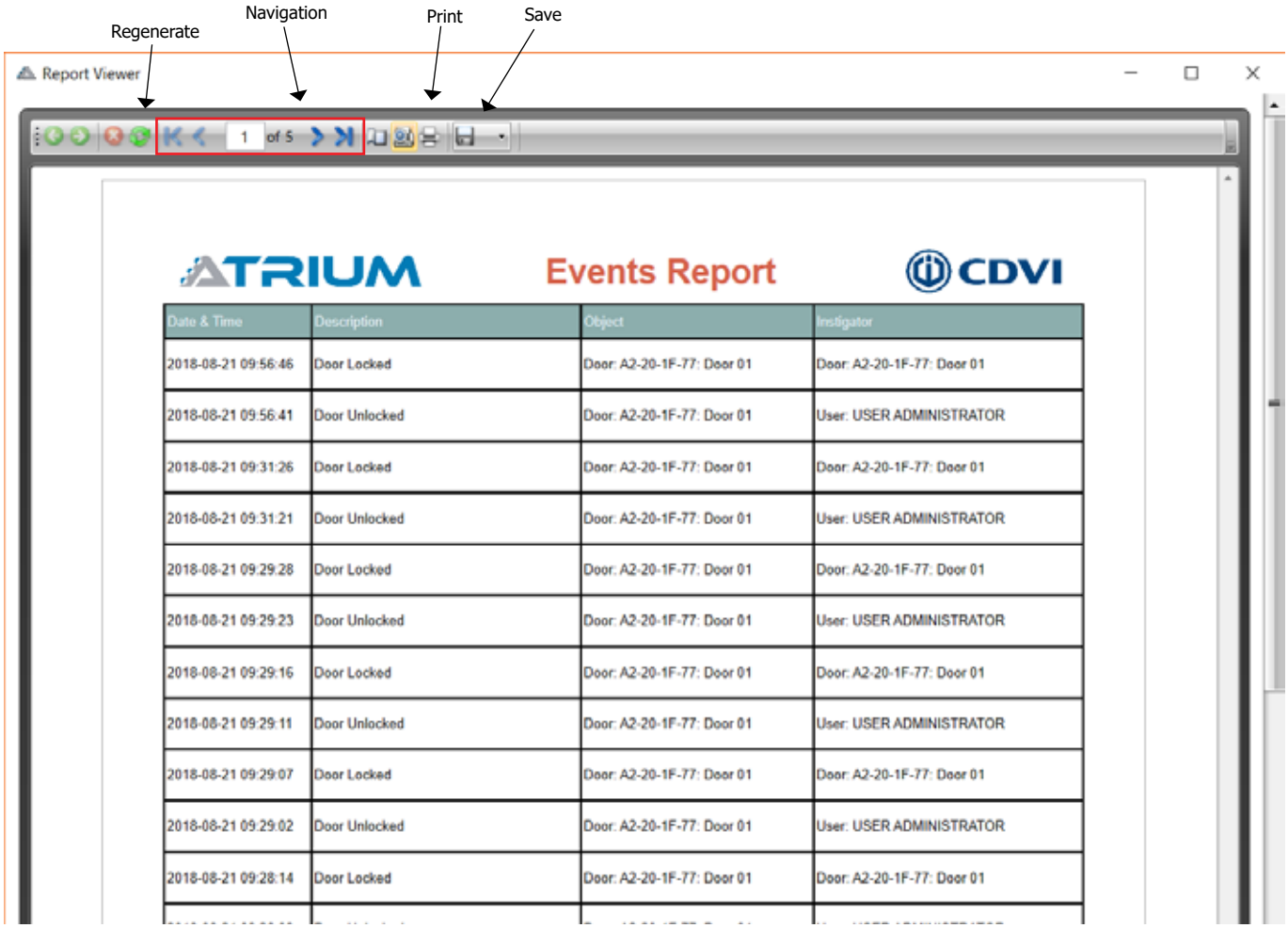
Generate

Generates the report based on the selected parameters and displays its content in the Results section.

VIEWING, PRINTING, AND SAVING A REPORT

Results

Displays the generated report and allows navigating through the report, printing and saving the report results.



Date & Time	Description	Object	Instigator
2018-08-21 09:56:46	Door Locked	Door: A2-20-1F-77: Door 01	Door: A2-20-1F-77: Door 01
2018-08-21 09:56:41	Door Unlocked	Door: A2-20-1F-77: Door 01	User: USER ADMINISTRATOR
2018-08-21 09:31:26	Door Locked	Door: A2-20-1F-77: Door 01	Door: A2-20-1F-77: Door 01
2018-08-21 09:31:21	Door Unlocked	Door: A2-20-1F-77: Door 01	User: USER ADMINISTRATOR
2018-08-21 09:29:28	Door Locked	Door: A2-20-1F-77: Door 01	Door: A2-20-1F-77: Door 01
2018-08-21 09:29:23	Door Unlocked	Door: A2-20-1F-77: Door 01	User: USER ADMINISTRATOR
2018-08-21 09:29:16	Door Locked	Door: A2-20-1F-77: Door 01	Door: A2-20-1F-77: Door 01
2018-08-21 09:29:11	Door Unlocked	Door: A2-20-1F-77: Door 01	User: USER ADMINISTRATOR
2018-08-21 09:29:07	Door Locked	Door: A2-20-1F-77: Door 01	Door: A2-20-1F-77: Door 01
2018-08-21 09:29:02	Door Unlocked	Door: A2-20-1F-77: Door 01	User: USER ADMINISTRATOR
2018-08-21 09:28:14	Door Locked	Door: A2-20-1F-77: Door 01	Door: A2-20-1F-77: Door 01

Top Control Bar

The ***regenerate*** button refreshes the report with new data if available.

The ***navigation*** buttons allow respectively to go to the first page, previous page, type a page number, next page, and last page.

The ***print*** button allows to print the report.

The ***save*** button allows to save the report on disk.
Acrobat (PDF), CSV, Excel 97-2003, Rich text (RTF), Tiff, Web archive (mhtml), XPS document formats are supported.

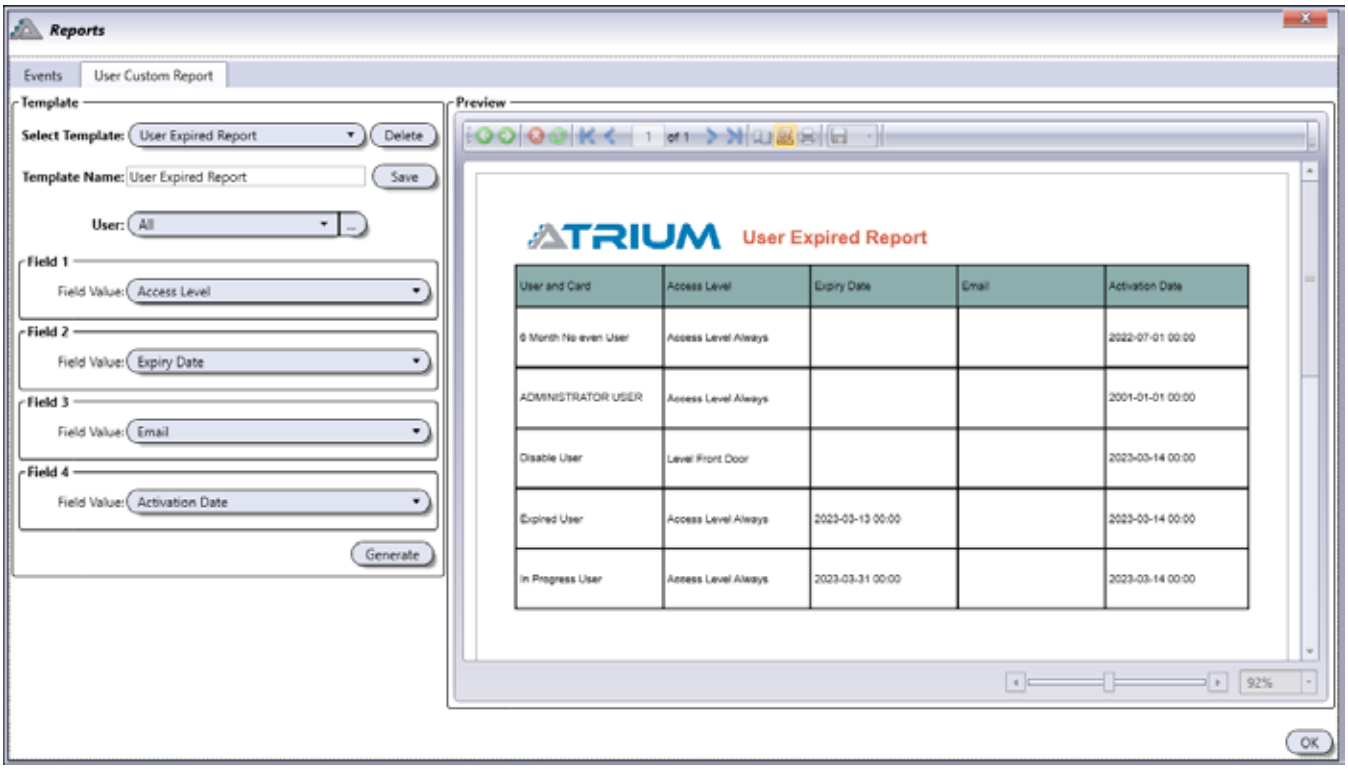
Bottom Control Bar

The bottom control bar allows to zoom in/out the report. Use the arrows, the scroll bar, type a percentage value, or select a predefined zoom from the list.

USER CUSTOM REPORT

Generate user custom reports that will automatically include user name and it's assign cards plus four extra field of your choice. These choices are the most common fields for user as well as all custom fields.

From the Dashboard tab, click on the ***Reports*** icon then click on ***User Custom Report*** tab. From this page reports may be generated, viewed, printed and saved.



GENERATING A REPORT

Parameters

Select the parameter criteria that will be used to generate the report.

- **Select Template:** Select the desired saved custom report template to generate its report.
- **Template Name:** Configure your custom report template according to the choices below. Type a name and save your choices in order to keep them for the futur printing.
- **User:** Select one or more users from the list for whom you want to produce a report.
- **Field 1, 2, 3 or 4:** Select which User database fields to include in the report.

Generate

Generates the report based on the selected parameters and displays its content in the Results section.

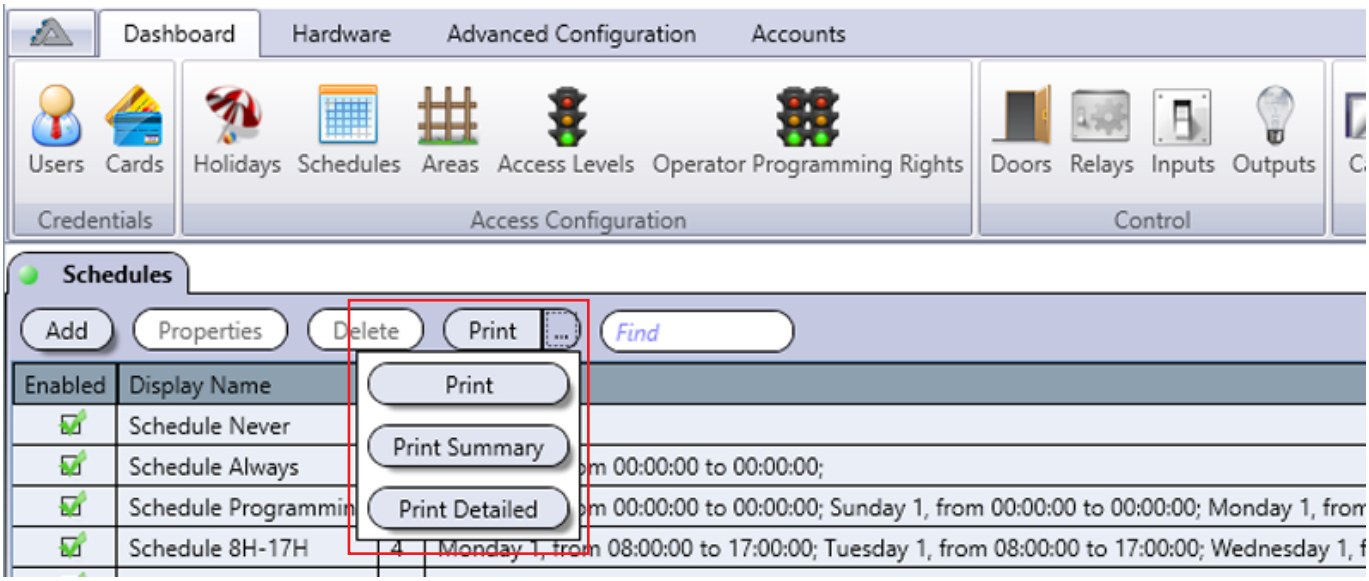
QUICK "PRINT" REPORT

Quick reports can also be generated from various menus (ex: Users, Cards, Schedules) by clicking the ***Print*** button dropdown menu.

There are three modes available:

- ***Print:*** The report will be ready to print or save according to the chosen menu grid (report display by column and one row per entity).
- ***Print Summary:*** The report will be ready to print or save with a little more detail than in "Print" mode (report display by block).
- ***Print Detailed:*** The report will be ready to print or save with full detail per entity. (report display full details per entity).

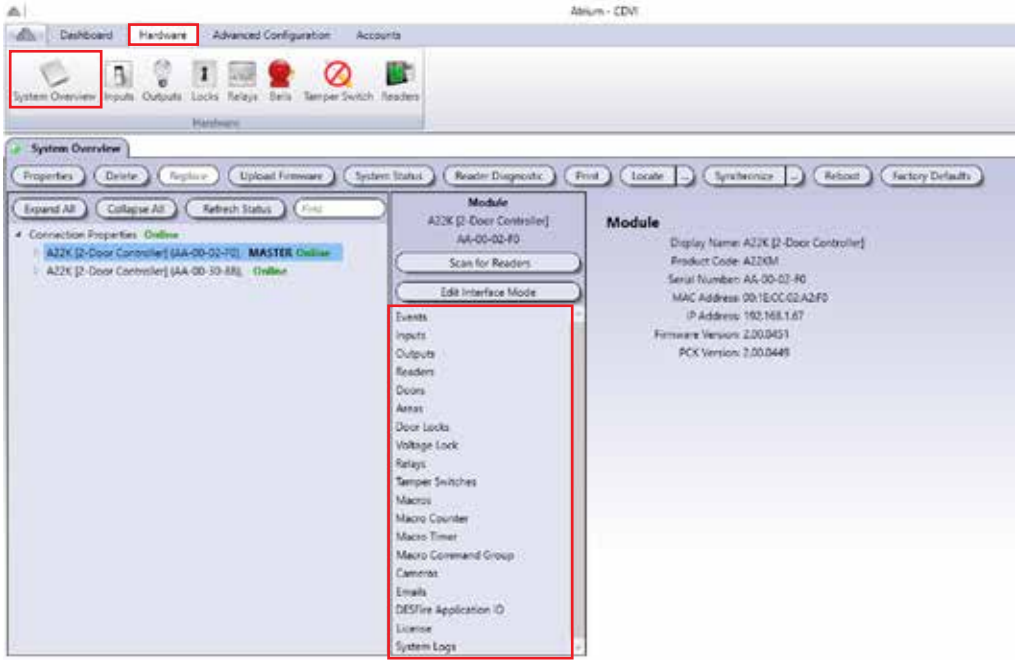
The report will be printed as the displayed result. It is possible to save the result of the report in different formats as well (Acrobat PDF, CSV, Excel 97-2003, Rich text-RTF, Tiff, Web archive-mhtml, XPS document are supported.)



SYSTEM OVERVIEW

The system overview displays and allows management of all ATRIUM modules within the access control system. From the system overview it is possible to see and control the inputs, outputs, readers, doors, areas, door locks, relays, bell and tamper switches. It also display system logs for each ATRIUM modules.

From the ***Hardware*** tab, click on the ***System Overview*** icon.

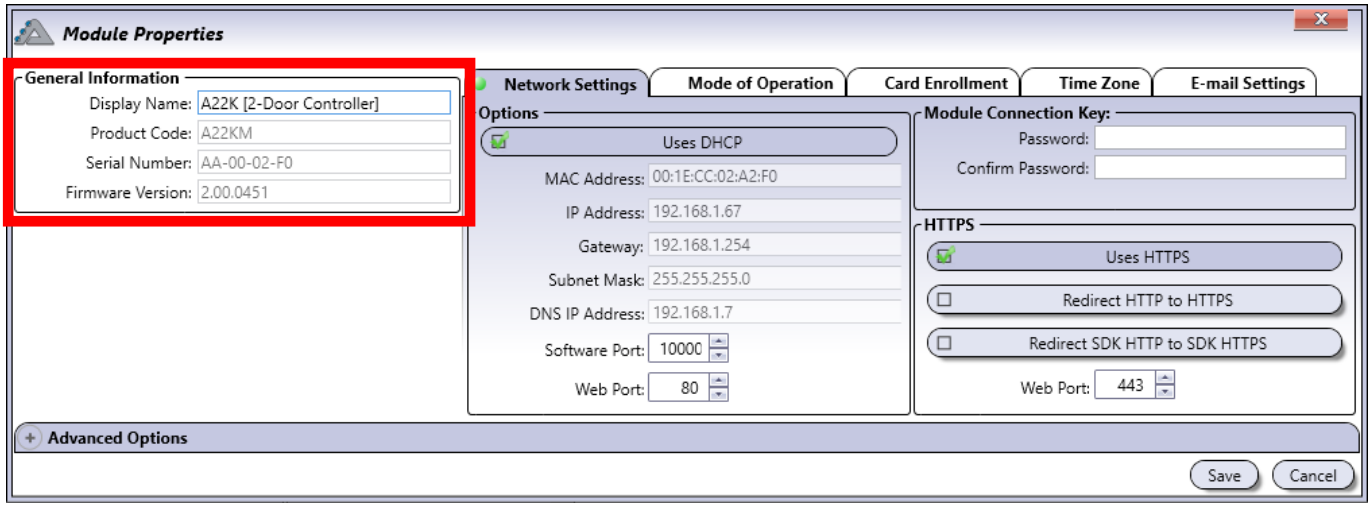


Under each controller and expander, the following information is available. Summary, status and control are available for each device or setting.

Device	Refer to
Events	“Events” on page 63
Inputs	“Inputs” on page 57
Outputs	“Outputs” on page 62
Readers	“Readers” on page 91
Doors	“Doors” on page 46.
Areas	“Areas” on page 39
Door Locks	“Door Lock” on page 85
Voltage Lock	
Relays	“Relays” on page 55
Bells **(AC22 only)**	“Bells” on page 87
Tamper Switches	“Tamper Switches” on page 90
Macros	“Macros” on page 93
Macro Counter	“Macro Counter” on page 91
Macro Timer	“Macro Timer” on page 93
Macro Command Group	“Macro Command Group” on page 100
Cameras	“Cameras” on page 105
Emails	“Emails” on page 103
DESFire Application ID	“DESFire Application ID and Readers” on page 108
Licence	“Licence” on page 77
System Logs	Reserved for technical support.

MODIFYING A CONTROLLER OR EXPANDER MODULE

From the ***Hardware*** tab, click on the ***System Overview*** icon, select a controller/expander module from the list and click on the ***Properties*** button.



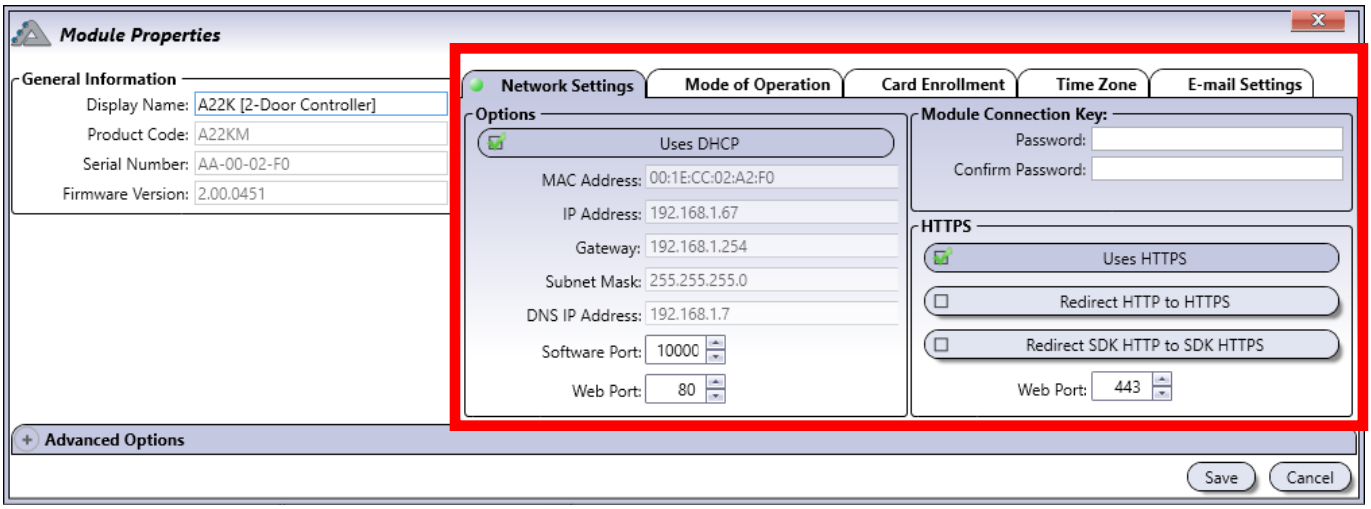
General Information

Allows to change the display name. All other information are read only.

- **Display Name:** Identifies the controller/expander throughout the ATRIUM software. We recommend using a name that is representative of the controller/expander module.
- **Product Code:** Indicates the module product code; AC22 for the ATRIUM 2-Door Controller, AX22 for the ATRIUM 2-Door Expander, etc.
- **Serial Number:** Indicates the serial number for the controller/expander module.
- **Firmware Version:** Indicates the current version of the module's firmware.

NETWORK SETTINGS (CONTROLLER ONLY)

Allows to define the 2-Door Controller's network communication settings.



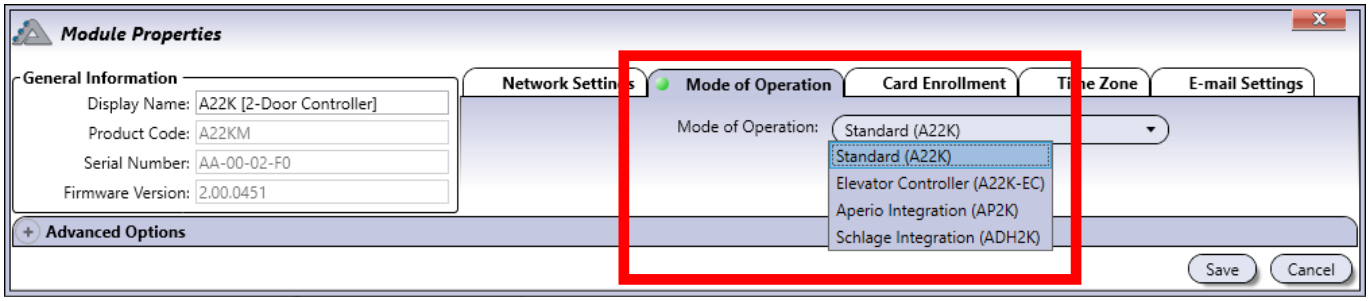
- **Uses DHCP:** When selected (default), the 2-Door Controller obtains an IP address automatically from the network's DHCP server.

The following parameters are only available when DHCP is **NOT** selected (manual setting entry).

- **MAC Address:** Indicates the MAC Address of the selected controller module. This field is read only.
- **IP Address:** Enter the IP Address of the controller module.
- **Gateway:** Enter the network Gateway address.
- **Subnet Mask:** Enter the network subnet mask.
- **DNS IP Address:** Enter the DNS IP address.
- **Software Port:** Select or enter the network software port number(Default= 10 000).
- **Web Port:** Select or enter the network web port number (Default= 80).
- **Module Password:** Enter module password. The default password is "admin".
- **Module Confirm Password:** Re-enter module password for confirmation.
- **Uses HTTPS:** All A22K controllers have HTTPS enabled by default. In order to have a valid HTTPS connection, all peripherals (desktop browser, tablet, smart phone, etc.) used to connect to the ATRIUM system must install the root certificate included in the USB key with the ATRIUM software or from the Download section of our website at: www.cdvi.ca. You may also install your own root certificate. Ensure your root certificate is installed on the **A22K "Master" controller** and all peripherals used to connect to the system. The root certificate can be installed on the **A22K "Master" controller** from the embedded ATRIUM web server.
- **Redirect HTTP to HTTPS:** This option will automatically redirect all HTTP connection to HTTPS secure connection. This feature works ONLY if an HTTPS connection is functional. See **"Uses HTTPS"** above on how to make an HTTPS secure connection.
- **Redirect SDK HTTP to SDK HTTPS:** Check this option if you are using a 3rd party application which uses the ATRIUM SDK and which supports HTTPS connections. It will will automatically redirect all HTTP connection to HTTPS secure connection. This feature works ONLY if an HTTPS connection is functional. See **"Uses HTTPS"** above on how to make an HTTPS secure connection.
- **Web Port:** Modify this option if the default HTTPS web port (443) is blocked. Contact your network administrator and / or your ISP (Internet Service Provider) to enter the correct HTTPS:// web port.

MODE OF OPERATION (A22K CONTROLLER ONLY)

The A22K controller includes all firmware bundled into one. You will be able to change the operating mode of the A22K from the same hardware (A22K firmware version 2.00.451 or higher). Note that whenever you change the operating mode of the A22K, it will force a reset to the module's factory default settings.

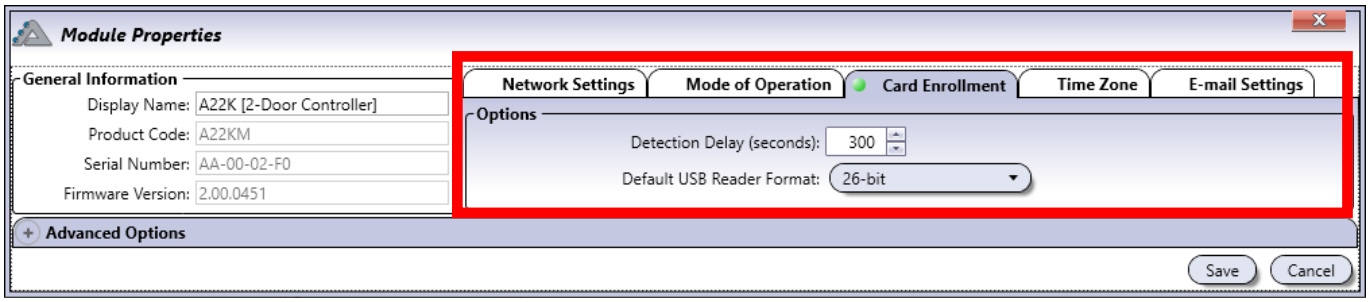


Operating modes supported (A22K firmware version 2.00.451 or higher):

- **A22K** 2-Door/4-Reader controller (default)
- **A22K-EC** Elevator controller
- **ADH2K** Schlage Integration, manage 2 door handles
- **AP2K** Aperio Integration, manage 2 door handles

CARD ENROLLMENT (CONTROLLER ONLY)

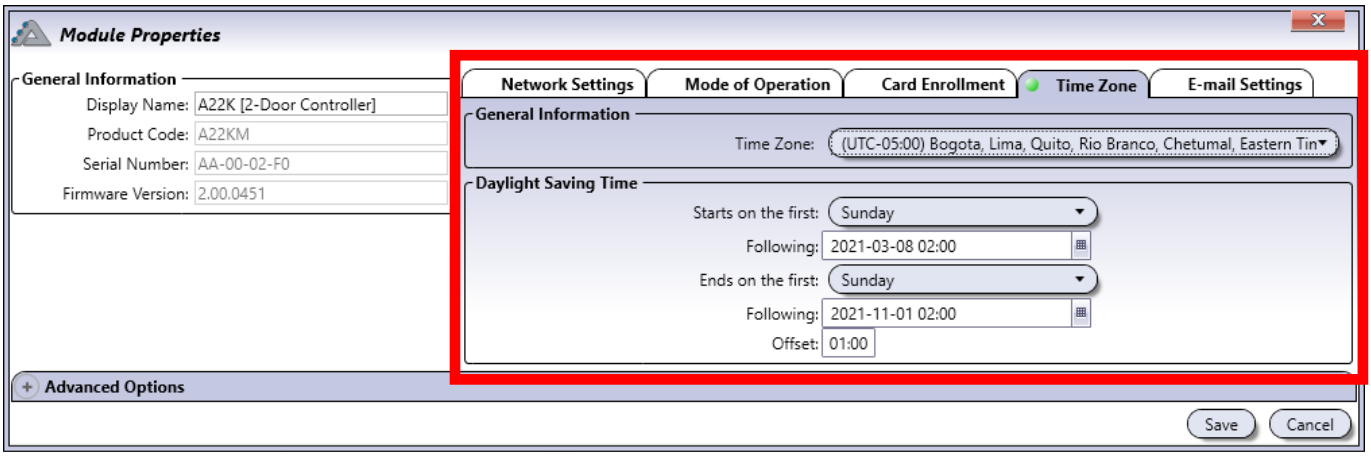
Defines the period within which a card must be presented to a reader to start adding/removing cards when using the 2-Door Controller's on-board card enrollment button (Refer to the 2-Door Controller instruction manual for more information). This time is also used to exit the enrollment mode when no more new cards are presented during this period.



- **Detection Delay (seconds):** Change the detection delay if required. The default setting is 300 seconds (5 minutes).
- **Default USB Reader Format:** Change the reader format if required. The default setting is 26-bit.

TIME ZONE (CONTROLLER ONLY)

Time zone configuration is used to tell the controller when to change its time for daylight saving. The time itself is automatically set whenever a PC connects; the module uses the PC's time and date.



General Information

- **Time Zone:** Select the time zone reference based on the UTC time and offset.

Daylight Saving Time

The following fields determine the start and end times of the daylight saving period.

Starts on the first: Select either ***<Fixed Date>*** or a "day of the week" the daylight saving period starts.

- ***<Fixed Date>*** is used when the daylight saving period starts the same date every year.
- ***Sunday to Saturday*** is used when the daylight saving period starts the same day of the week every year.

Following: Enter the date and time using the "yyyy:mm:dd hh:mm" format or click the icon on the right side of the field to select the following date and time.

- This date will be used to determine what will be the next date on the day selected in the "Start on the first" field. For example if the daylight saving starts the first Sunday of April at 2 o'clock in the morning, enter 2011/04/01 02:00. If the daylight saving starts the second Sunday of April at 2 o'clock in the morning, enter 2011/04/08 02:00.

Ends on the first: Select either a <Fixed Date> or a day of the week the daylight saving period ends.

- ***<Fixed Date>*** is used when the daylight saving period ends the same date every year.
- Sunday to Saturday is used when the daylight saving period ends the same day of the week every year.

Following: Enter the date and time using the "yyyy:mm:dd hh:mm" format or click the icon on the right side of the field to select the following date and time.

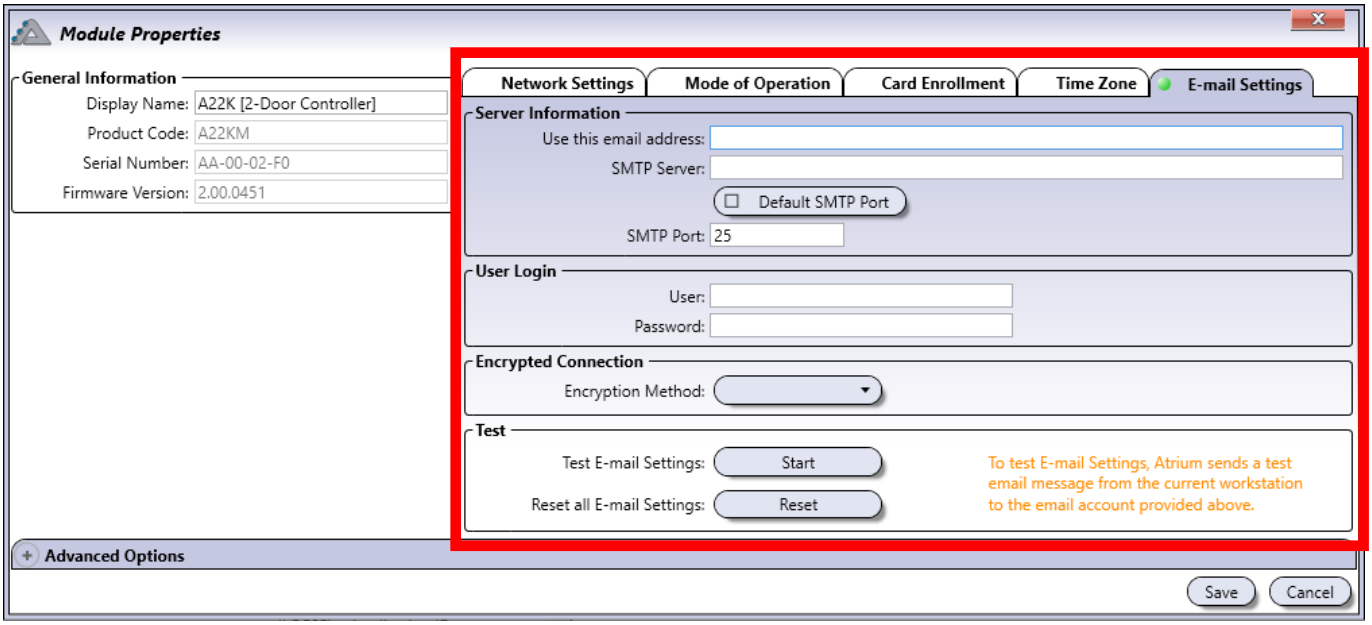
- This date will be used to determine what will be the next date on the day selected in the "Ends on the first" field. For example if the daylight saving ends the first Sunday of November at 2 o'clock in the morning, enter 2011/11/01 02:00. If the daylight saving ends the second Sunday of November at 2 o'clock in the morning, enter 2011/11/08 02:00.

Offset: Select the daylight offset time in hour and minute (hh:mm).

EMAIL SETTING (CONTROLLER ONLY)

Email setting configuration is used to tell the controller from which email will be send email notification.

See page 103 to configure email notification.



Server Information

- **Use this email address:** Enter the sender email
- **SMTP server:** Enter sender email SMTP server
- **Default SMTP Port:** The default SMTP port is 25 and works for most servers. Do not select when you enable encryption. Manually enter the SMTP port, see "SMTP port" below.
- **SMTP Port:** Uncheck "Use Default SMTP port" to enter manually a specific port number. When you enable encryption, in general, the required SMTP port will be 465 with SSL encryption and 587 with TLS encryption. Check with your email service provider to find out what type of encryption they use and on which port.

User Login

- **User:** Enter user login ID
- **Password:** Enter user login password. If your usual password doesn't work, your email service may require a new password and 2-step verification, check with your email service provider for details.

Encrypted Connection

- **Encryption Method:** SSL/TLS or STARTTLS

  Check if sender email use SSL/TLS or STARTTLS
  GMAIL SSL certificate is pre-loaded. (GMAIL default SSL port is 465 and TLS port is 587).

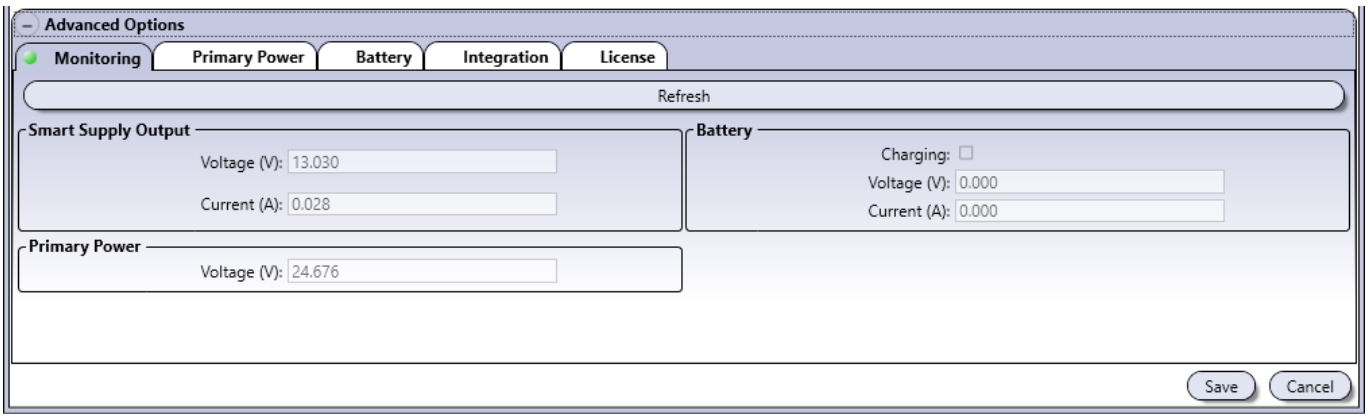
Test

- **Test E-mail Settings:** Click on "Start" to validate if the e-mail server information has been saved correctly.
- **Reset all E-mail Settings:** Click "Reset" to erase all e-mail server informations.

ADVANCED OPTIONS

Monitoring

Displays the monitored system's voltage and current values.

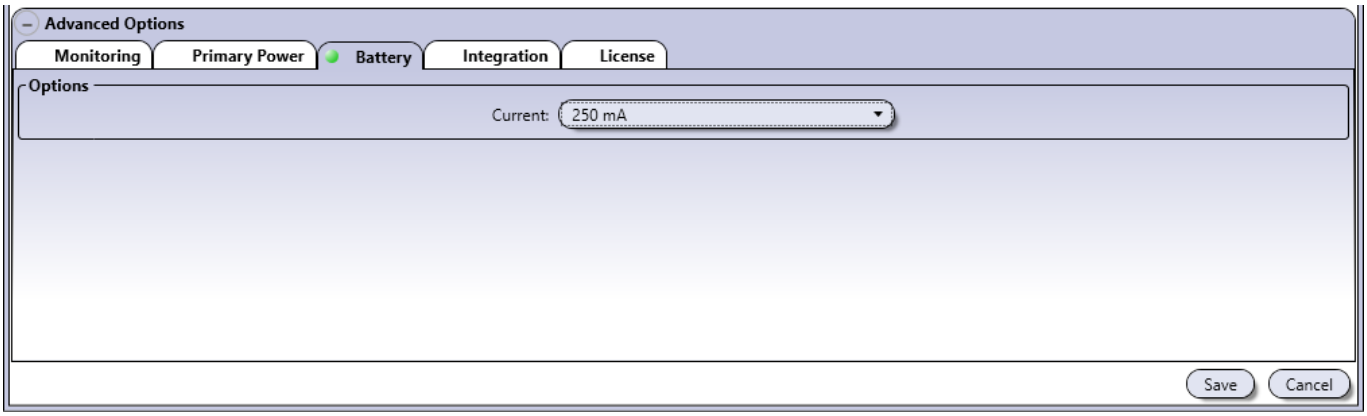


- **Refresh button:** Refreshes the voltage and current values.
- **Smart Supply Output** (Controller and Expander only)
  - **Voltage (V):** Indicates the voltage supplied to devices.
  - **Current (A):** Indicates the current used by the connected devices.
- **Battery** (Controller and Expander only)
  - **Charging:** Indicates, when the Charging check box is selected, that the battery is currently charging.
  - **Voltage (V):** Indicates the actual battery charging voltage.
  - **Current (A):** Indicates the actual charging current supplied to the battery
- **Primary Power** (Controller and Expander only)
  - **Voltage (V):** Indicates the voltage supplied to the module.

Primary Power

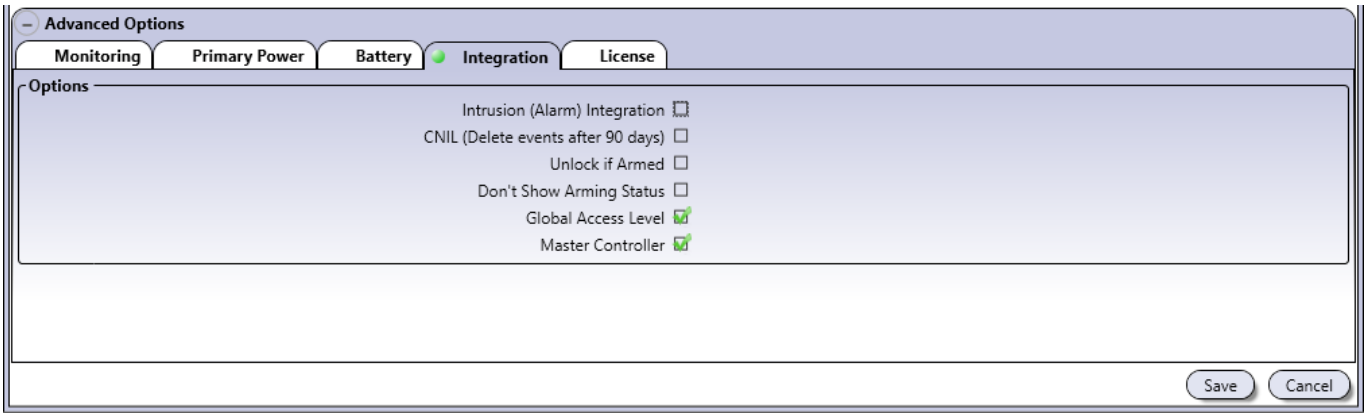
- **Fail Delay (minutes):** Value between 0 and 65534 minutes that represents the amount of time before sending power failure event message.
- **Restore Delay (minutes):** Value between 0 and 65534 minutes that represents the amount of time before sending power restore event message.

Battery



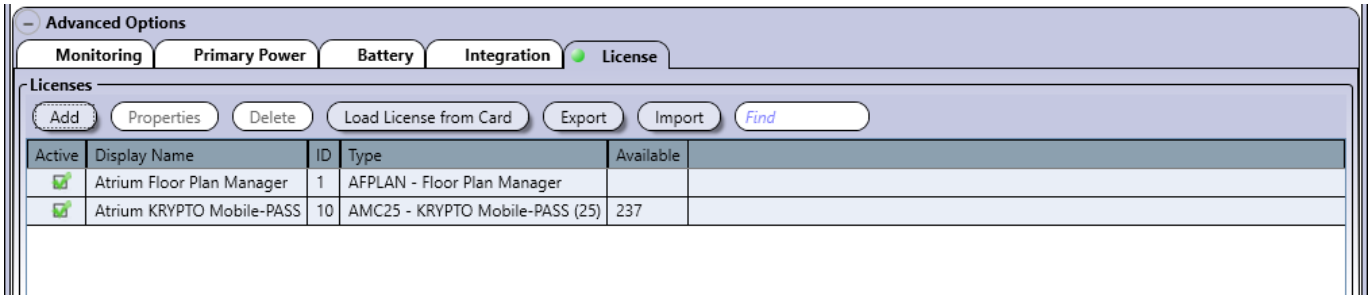
- **Options**
  - **Current:** Select the maximum current that will be used to charge the battery; 250mA (Default), 320mA, 500mA or 1A.

Integration



- **Options**
  - **Intrusion (Alarm) Integration:** When selected, activates the intrusion integration feature.
  - **CNIL (Delete events after 90 days):** When selected, the module will only keep record of the past 90 days
  - **Unlock if Armed:** When selected, the doors within the armed area can be unlocked if the user has permission (can arm/disarm)
  - **Don’t Show Arming Status:** When selected, the LED status of the readers within the armed area will return to normal, as to not indicate the armed status.
  - **Global Access Level:** The A22K uses Global Access Level system which improves the synchronization speed of the ATRIUM system. This option will be disabled automatically if the A22K controller is connected to an ATRIUM system that has an A22 as the master controller.
  - **Master Controller:** When selected, activates the controller to be “Master” controller. The ‘’Master’’ controller will manage the data (doors, users, schedules, etc.) among all sub-controllers and expansion modules.

License



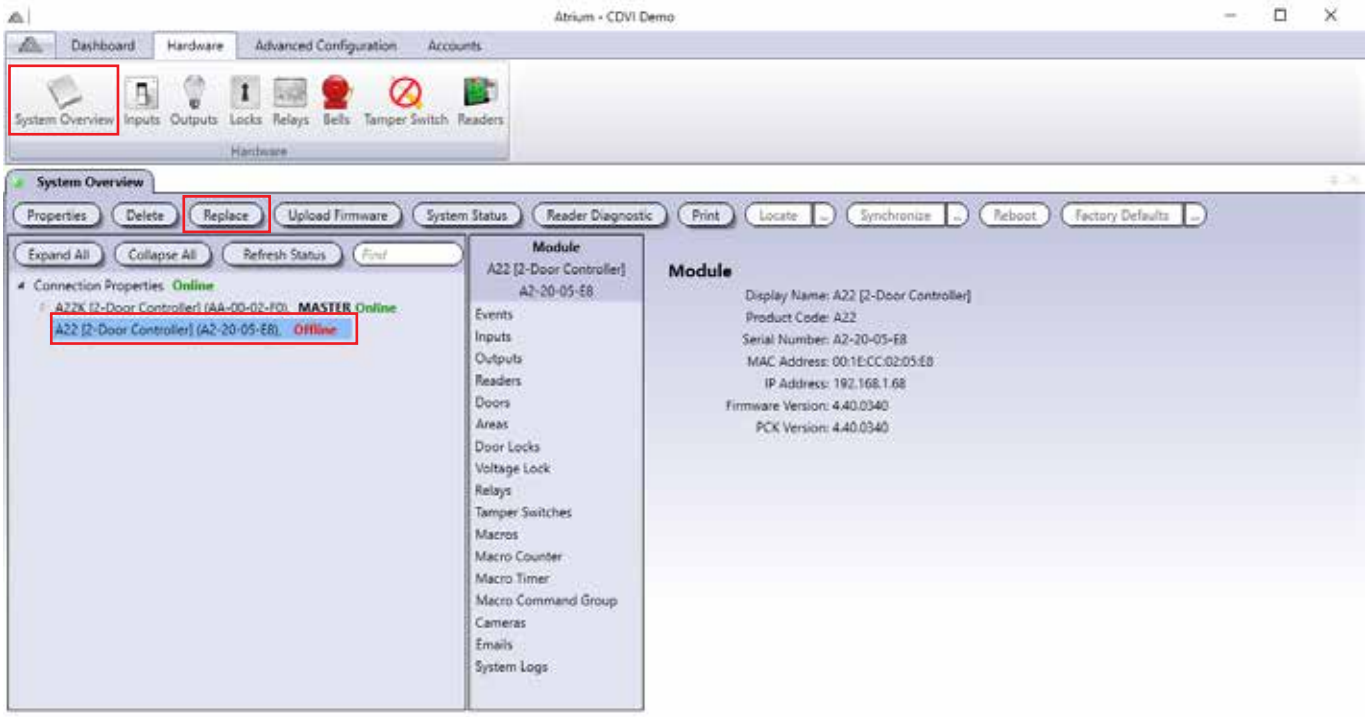
- **Add:** Click the ***"Add"*** button then copy/paste the provided license code in the field.
- **Properties:** Displays the code details of the license.
- **Delete:** It will delete the selected license file.
- **Load License from Card:** Click on the "Load license from card" button to add a license from a card. Select the KRYPTO reader where you will scan your license card. Present and hold the card close to the reader until it chirps and flashes green.
- **Export:** Future use
- **Import:** Future use

DELETING A MODULE

To delete a module, select the module from the list and click on the ***Delete*** button. Deleting a controller automatically deletes the controller itself as well as all attached expander modules. However, the distributed entities (users, cards, schedules, etc.) are not deleted. A dialogue box will appear requesting confirmation.

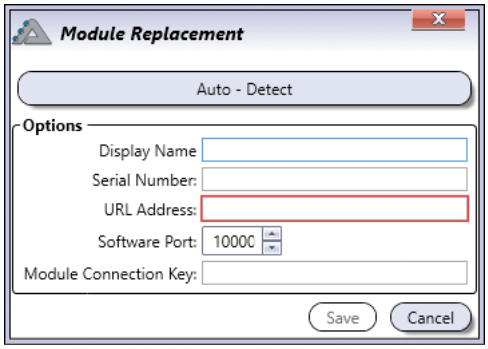
REPLACE

Replaces a defective and offline module that has been physically replaced. ***Only available for offline modules.***



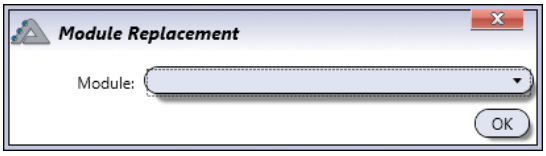
To replace a controller:

1. Make sure that the NEW controller is connected.
2. Select the controller that is defective from the list, "OFF LINE" and click on the ***"Replace"*** button.
3. The controller "Module Replacement" window will open, click on "Auto-Detect" to find new controller.
4. Select the new controller from the list and click OK.
5. The "Module Replacement" window will appear again, then enter "Module Connection Key" password. The default connection key password is "admin". Click ***OK***.
6. The new controller will synchronize automatically



To replace an expander module:

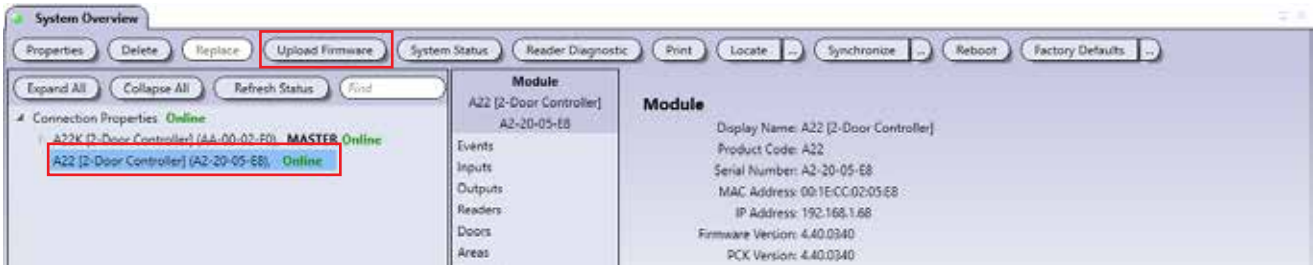
1. Make sure that the NEW expander is connected. The controller will detected automatically.
2. Select the defective expander ("OFF LINE") from the list and click on the ***"Replace"*** button.
3. The expander "Module Replacement" window will open.
4. Select the new expander from the drop down list and click OK.
5. The new expander will synchronize automatically



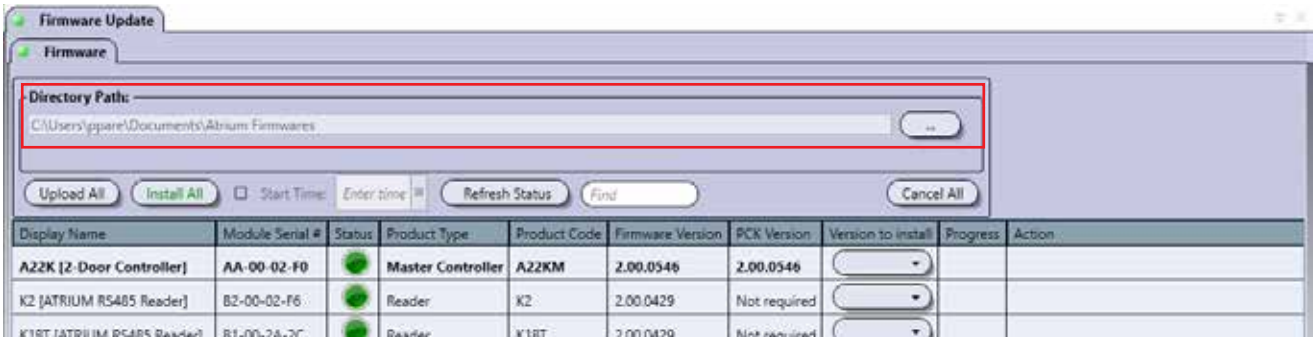
The configuration from the old module will be transferred to the new module, including the non distributed entities (inputs, outputs, areas, tamper switches, etc.).

UPLOAD FIRMWARE

Upgrades the selected controller or expander module with a new firmware.



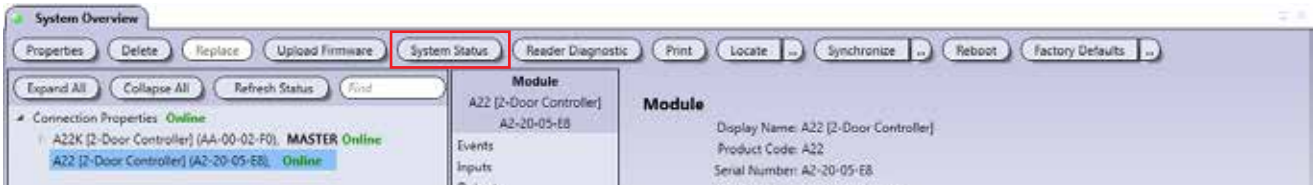
- Select one of the controller or expander module and click on ***Upload Firmware***.



- Save the new firmware file in the directory path folder or browse to locate where you saved it.
- Click on ***"Upload All"***, once upload done, click ***"Install All"*** to start updating all modules automatically.
- To update a module individually, select a "Version to Install" and click on ***Update***.
  When updating modules manually it is recommended to first update the expander(s), then sub-controller(s) and finally the master controller.

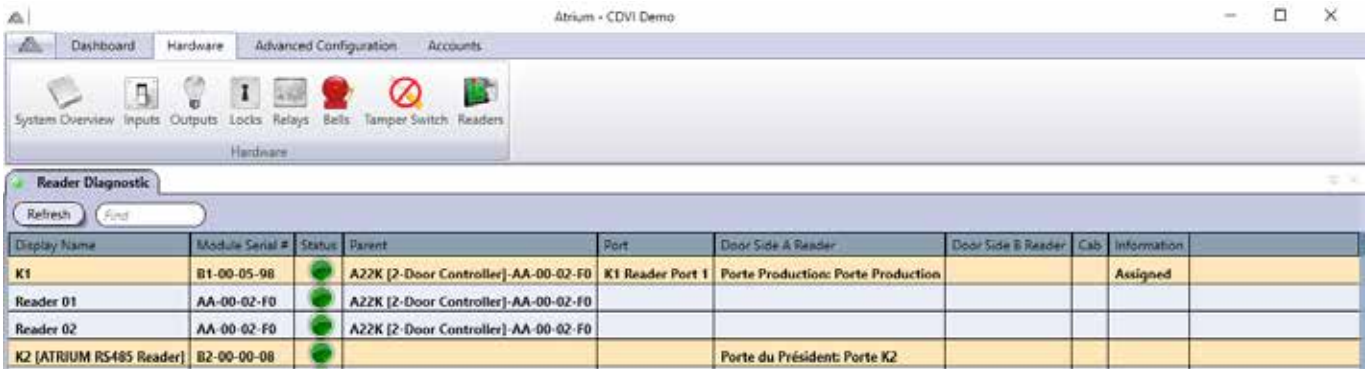
SYSTEM STATUS

Gives you an overview of all modules status. Such as; Is the module online or not, their input power supply, the battery voltage with charging current, the voltage outputs with their current consumption and tamper alarm.



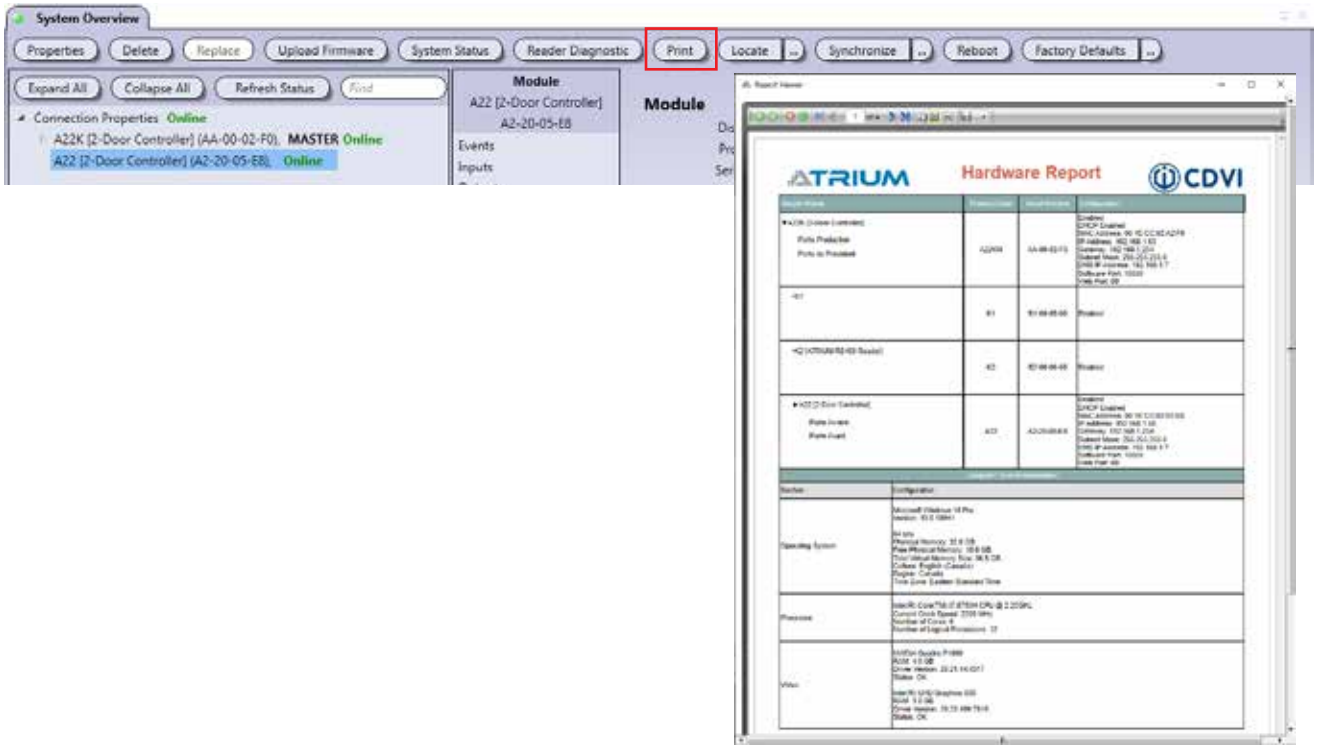
READER DIAGNOSTIC

Gives you an overview of all readers information's. Such as; reader serial number, Is the reader online or not, reader is connected to which module (parent), connected to which module port, connected on which side of the door, is it associate to cab and it is "Assigned" or not.



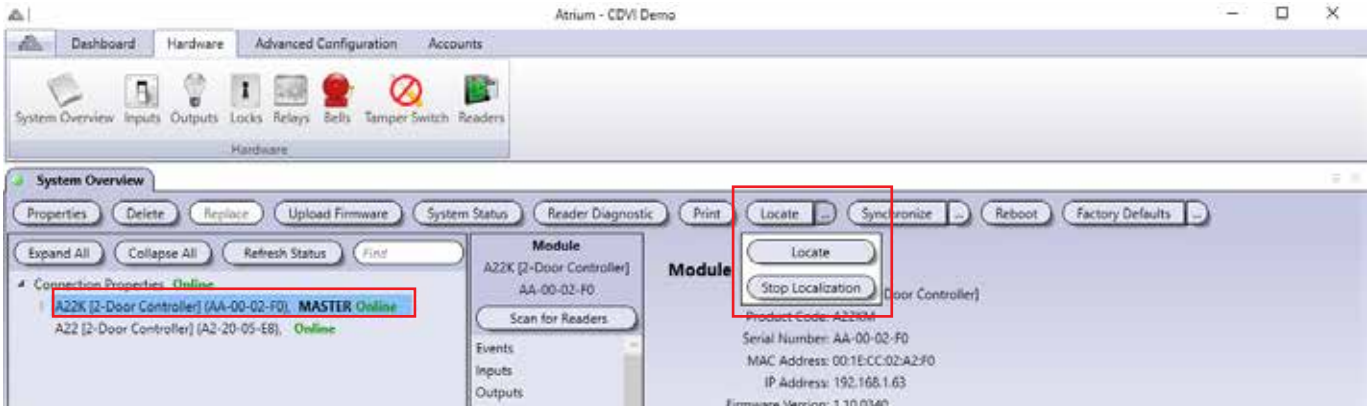
PRINT

Gives you a hardware report of all modules installed on a site. Information's such as; module serial number, MAC address, IP address, etc. It will also give many informations about the computer operating system (OS) where ATRIUM software is installed.



LOCATE

Allows to find a module when the serial number of the module has been removed or is not legible.

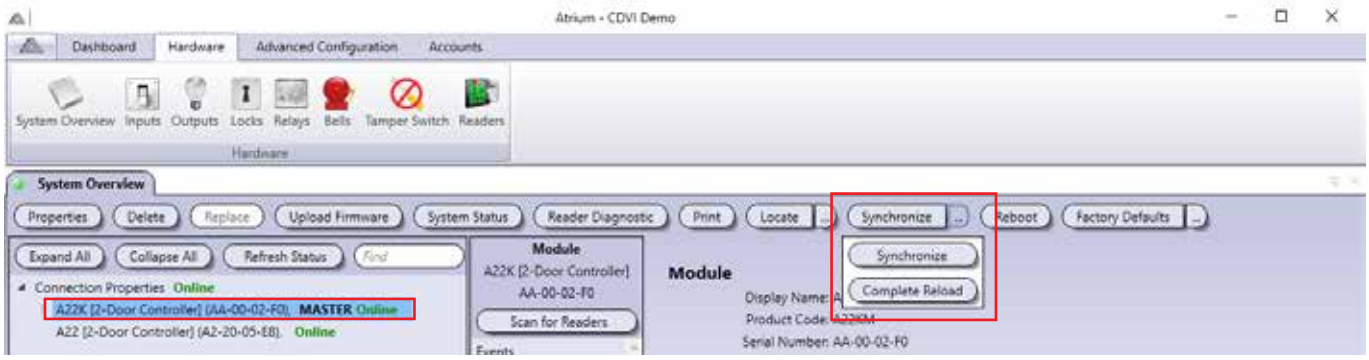


To locate a module:

1. Select the module to locate.
2. Click on the ***Locate*** button.
3. Open the door of each module's metal box, the corresponding module's GLOBAL -STAT LED will be flashing rapidly. Refer to the module instruction manual for more information.
4. Click on ***Stop Localization*** to exit the locate mode.

SYNCHRONIZE

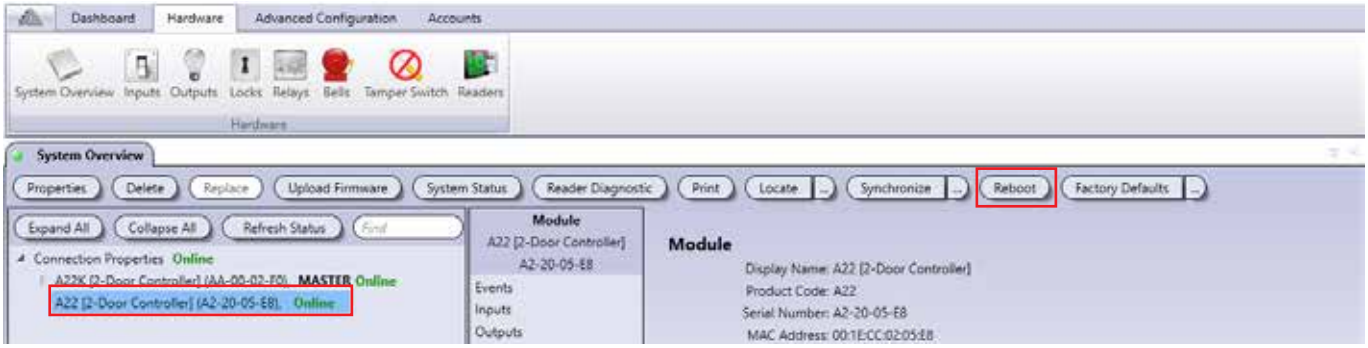
Synchronize the selected controller or expander module.



- **Synchronize:** Forces the system to synchronize the ATRIUM Controller database with the ATRIUM software database.
- **Complete Reload:** Forces the ATRIUM Controller database to overwrite the ATRIUM software database

REBOOT

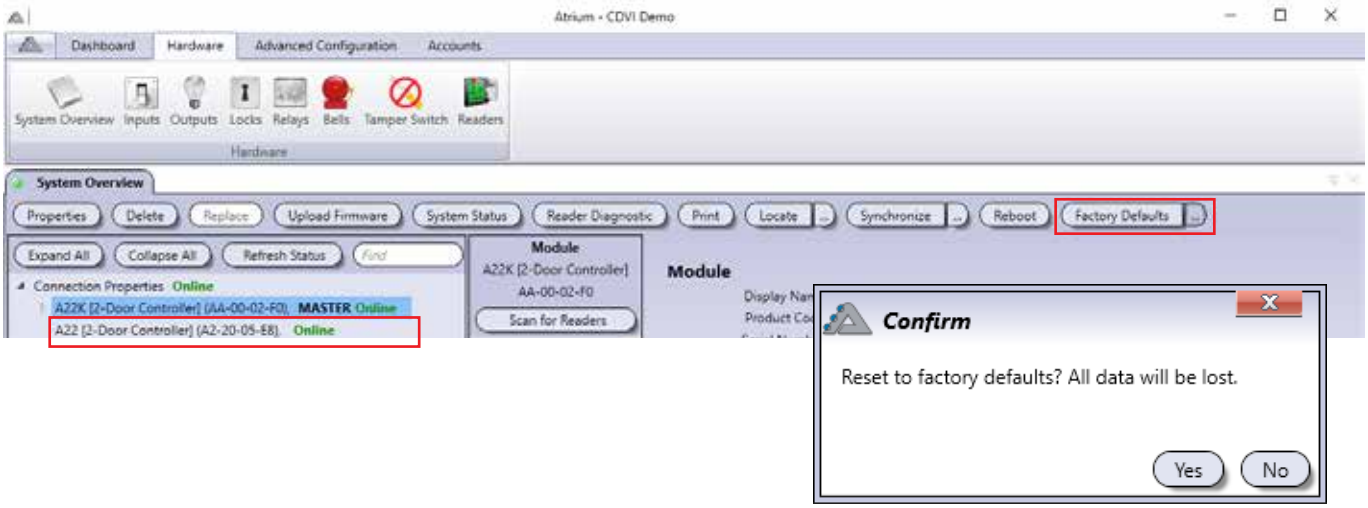
Shuts down and restarts the selected controller or expander module.



- Select the controller or expander module to be rebooted.
- Click on ***Reboot***.
- Click ***Yes*** to confirm.

RESTORE FACTORY DEFAULTS

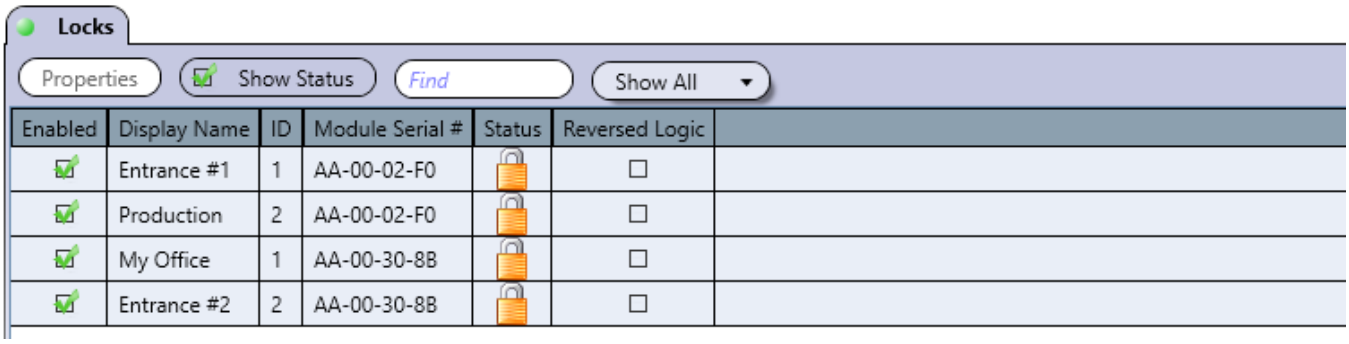
A "Factory Defaults" will erase all data but will keep the network settings in place to easily reconnect afterwards.



LOCKS

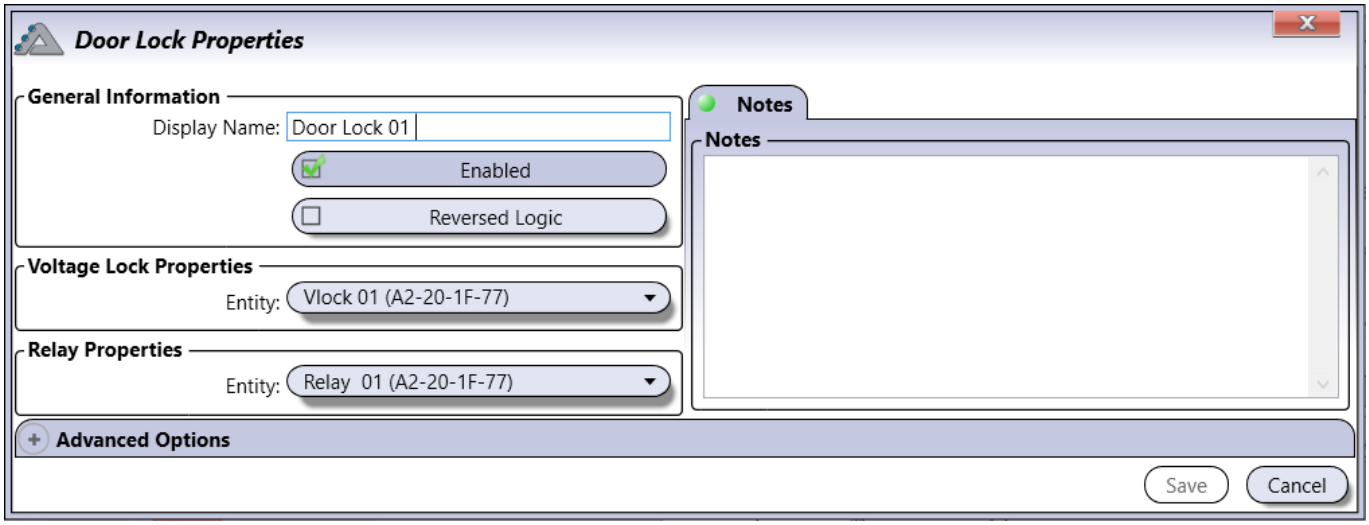
Typically, the locks are used to control the door lock devices such as door strike and electromagnetic devices.

Each controller includes two door locks and supports up to four 2-Door Expansion Modules which provide an additional 2 door locks each. Therefore, each controller can monitor the state of up to 10 door locks.



MODIFYING A DOOR LOCK

From the ***Hardware*** tab, click on the ***Locks*** icon, select a lock from the list and click on the ***Properties*** button.



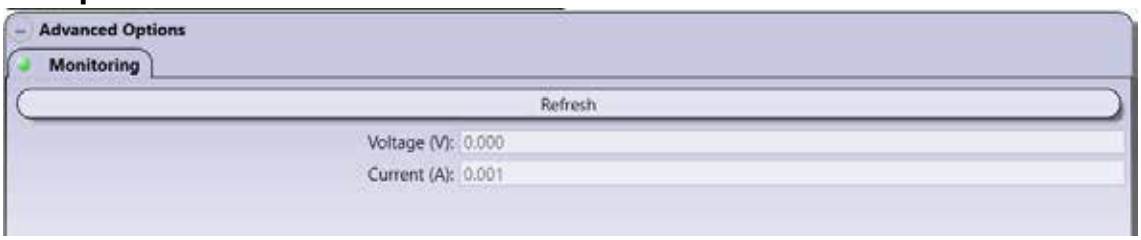
General Information

- **Display Name:** Identifies the door lock throughout the ATRIUM software. We recommend using a name that is representative of the door lock output.
- **Enabled:** When selected, activates the usage of this door lock.
- **Reversed Logic:** When selected, reverses the logic from either normally closed (N.C.) to normally open (N.O.) or vice-versa. Refer to Jumper Settings from the module instruction manual for more information on N.C. and N.O.
- **Voltage Lock Properties:** The voltage lock entity is set by default
- **Relay Properties:** By default the relay associated with the voltage lock is selected.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Advanced Options

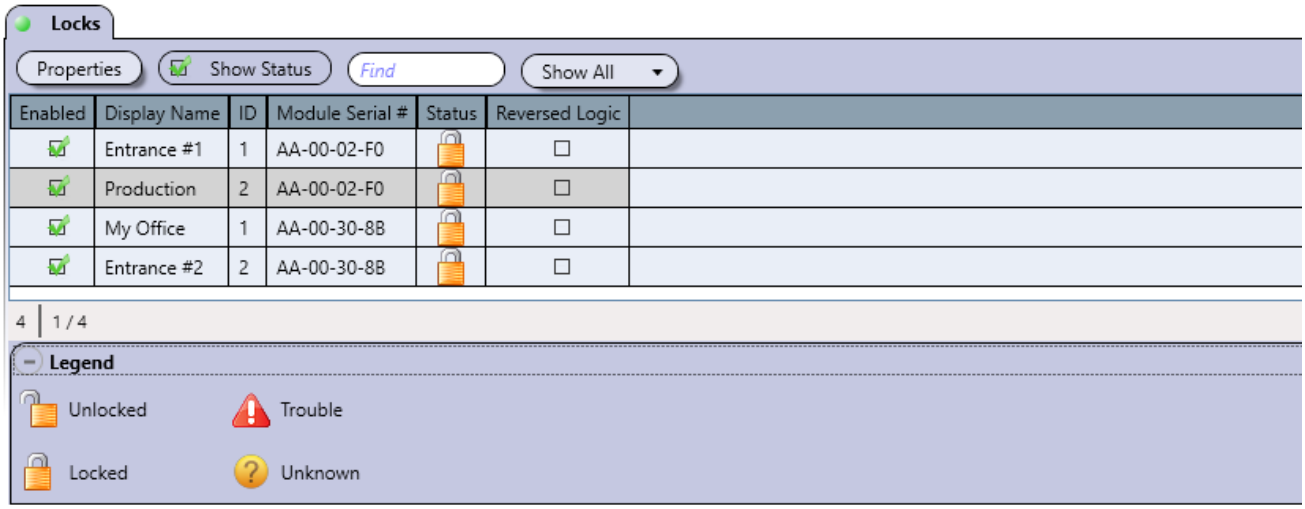


Monitoring

- **Refresh button:** Refreshes the voltage and current values.
  - **Voltage (V):** Indicates the voltage supplied to the door lock device.
  - **Current (A):** Indicates the current used by the connected lock device.

SHOW STATUS CHECK BOX

When enabled, displays the status of the door locks for a period of 5 minutes.



Legend

ICON	NAME	DESCRIPTION
	Unlocked	Indicates that the door lock is not activated.
	Locked	Indicates that the door lock is activated.
	Trouble	Indicates that the state of the door lock supply is short circuited or overloaded.
	Unknown	Indicates that either the module is not synchronized or the module has an older firmware version that is not compatible with the ATRIUM application.

Save Button

Use the ***save*** button to save changes.

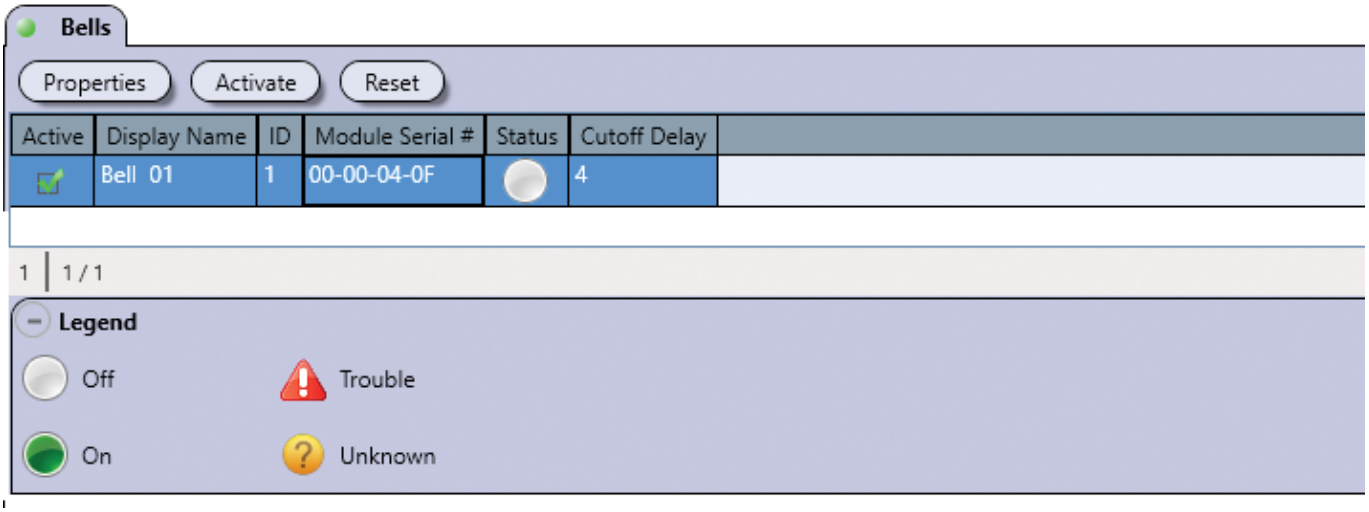
Cancel Button

Use the ***cancel*** button to ignore changes.

BELLS

The ATRIUM AC22 controller (first generation of controller) provides one bell output that can be used to drive one or several bells connected in parallel. Refer to the 2-Door Controller instruction manual for more information.

From the ***Hardware*** tab, click on the ***Bells*** icon.

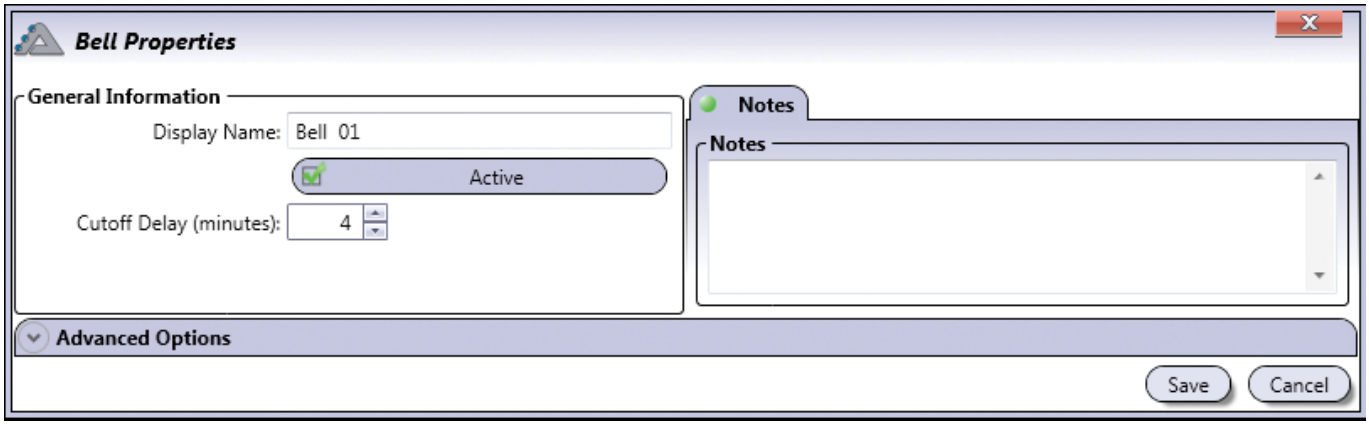


Legend

ICON	NAME	DESCRIPTION
	Off	Indicates that the bell is not activated.
	On	Indicates that the bell is activated.
	Trouble	Indicates that the state of the bell is either missing (absent), short circuited or overloaded
	Unknown	Indicates that either the module is not synchronized or the module has an older firmware version that is not compatible with the ATRIUM application.

MODIFYING THE BELL

From the ***Hardware*** tab, click on the ***Bells*** icon, select the bell from the list and click on the ***Properties*** button.



General Information

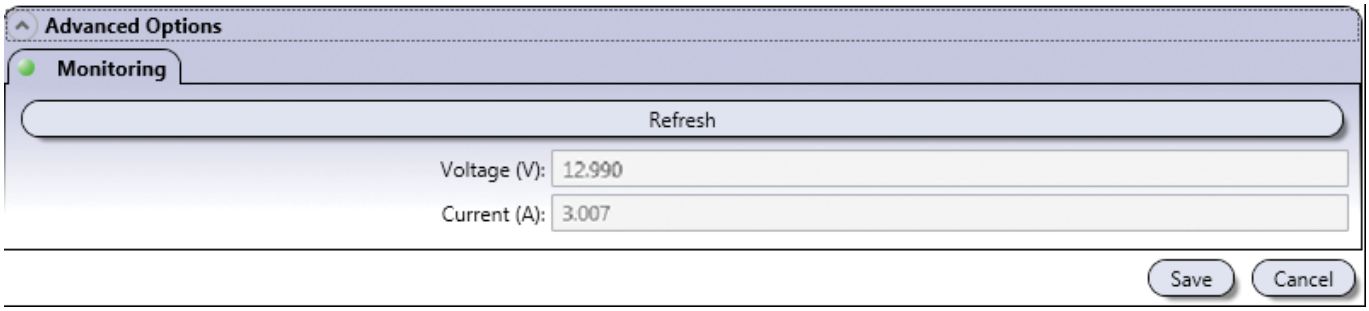
- **Display Name:** Identifies the bell/siren throughout the ATRIUM software. We recommend using a name that is representative of the bell/siren.
- **Enabled:** When selected, activates the usage of the bell/siren.
- **Cutoff Delay (minutes):** Type a value between 0 and 1000 minutes (Default: 4 minutes) that represents the amount of time the controller will maintain the bell active.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Advanced Options - Monitoring

Displays the monitored bell's voltage and current values.



Refresh button: Refreshes the voltage and current values.

- **Voltage (V):** Indicates the voltage supplied to the bell/siren device(s).
- **Current (A):** Indicates the current used by the connected bell/siren device(s).

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

RESET

Cancel the override bell control, returning the bell to its current scheduled or event state.

ACTIVATE

Manually activates the bell overriding the activation delay.

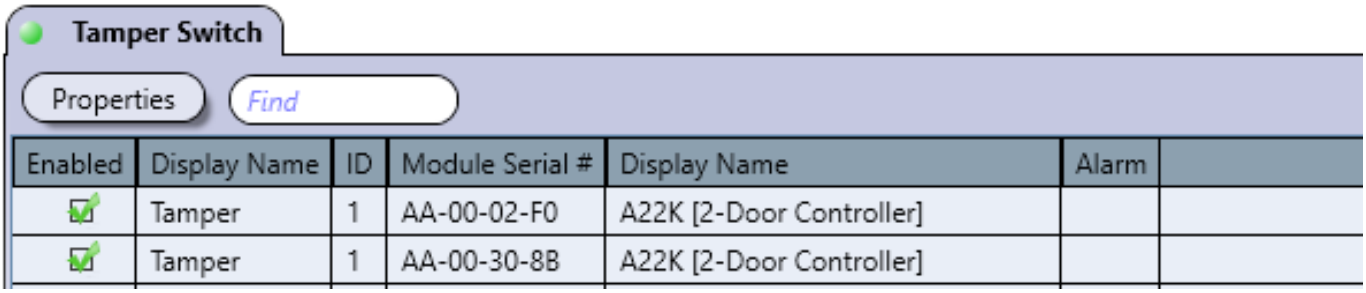
TAMPER SWITCH

Tamper switch detects when the cabinet door is opened or when the cabinet is removed from the wall.

Each controller and expander may have 2 tamper switches per cabinet, a wall and a door tamper switch.

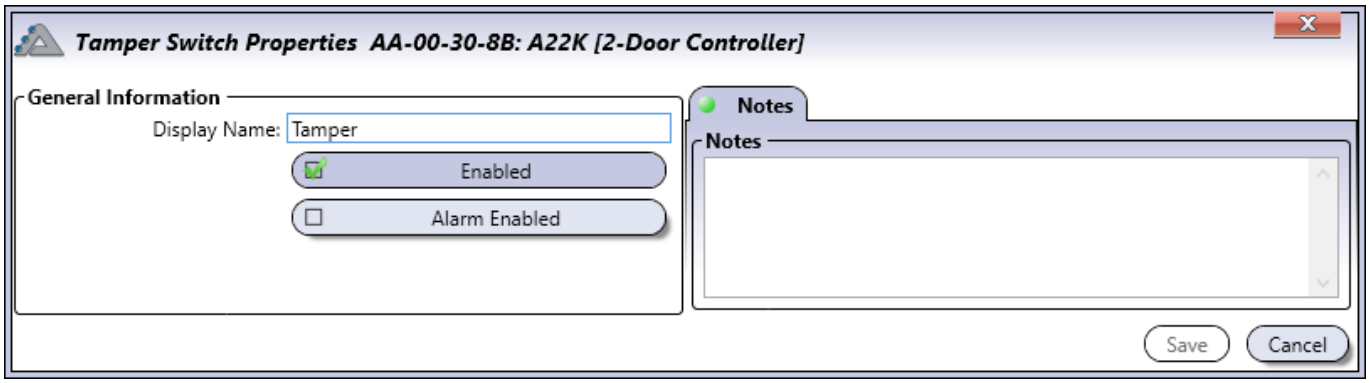
However, even when both are installed, only one tamper instance is monitored by the ATRIUM software per module box since they are connected in series.

From the ***Hardware*** tab, click on the ***Tamper Switch*** icon.



MODIFYING THE TAMPER SWITCH

From the ***Hardware*** tab, click on the ***Tamper Switch*** icon, select the tamper switch from the list and click on the ***Properties*** button.



General Information

- **Display Name:** Identifies the tamper switch throughout the ATRIUM software. We recommend using a name that is representative of the tamper switch.
- **Enabled:** When selected, operates normally but does not generate an alarm and restore automatically.
- **Alarm Enabled:** When selected, operates normally and will generate an alarm and must be manually restore. CDVI KRYPTO readers will delete the encryption keys.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

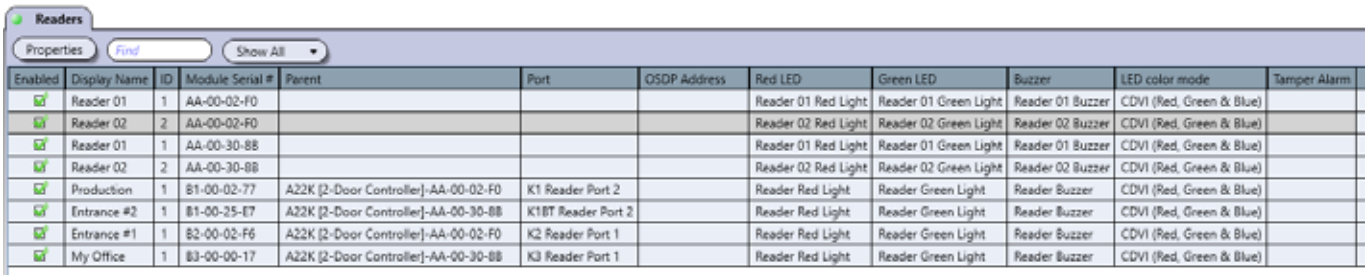
Use the ***cancel*** button to ignore changes.

READERS

Readers such as keypad and proximity readers are used to request access to an area via a door.

Each controller includes two readers and supports up to four 2-Door Expansion Modules which provide two readers each. Therefore, each controller can monitor the state of up to 10 readers.

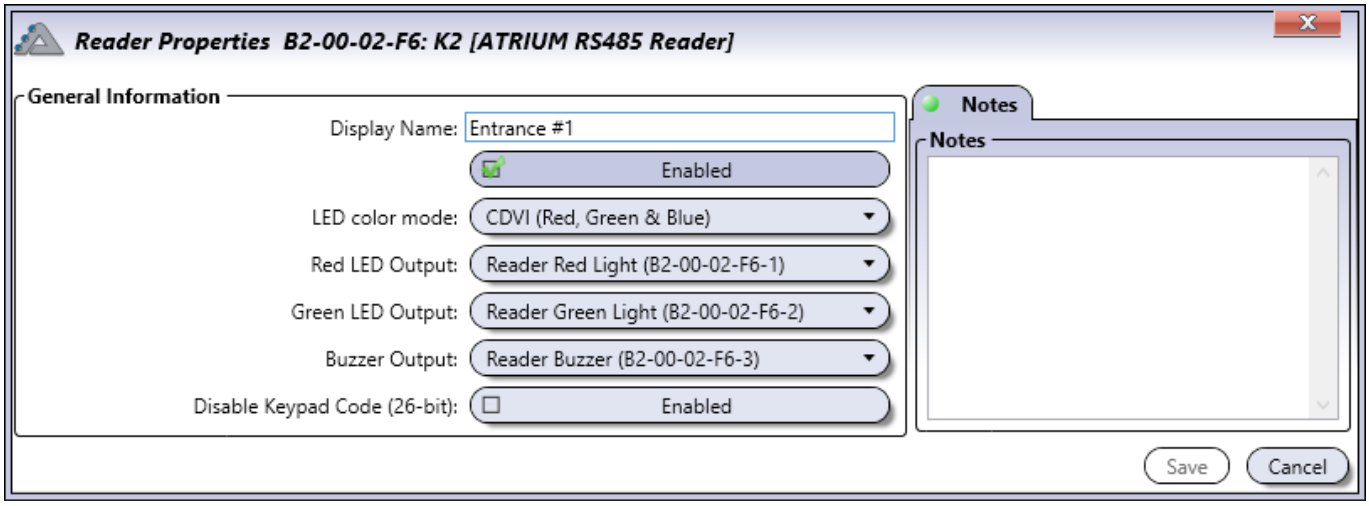
From the ***Hardware*** tab, click on the ***Readers*** icon.



Enabled	Display Name	ID	Module Serial #	Parent	Port	OSDP Address	Red LED	Green LED	Buzzer	LED color mode	Tamper Alarm
☑	Reader 01	1	AA-00-02-F0				Reader 01 Red Light	Reader 01 Green Light	Reader 01 Buzzer	CDVI (Red, Green & Blue)	
☑	Reader 02	2	AA-00-02-F0				Reader 02 Red Light	Reader 02 Green Light	Reader 02 Buzzer	CDVI (Red, Green & Blue)	
☑	Reader 01	1	AA-00-30-88				Reader 01 Red Light	Reader 01 Green Light	Reader 01 Buzzer	CDVI (Red, Green & Blue)	
☑	Reader 02	2	AA-00-30-88				Reader 02 Red Light	Reader 02 Green Light	Reader 02 Buzzer	CDVI (Red, Green & Blue)	
☑	Production	1	B1-00-02-77	A22K [2-Door Controller]-AA-00-02-F0	K1 Reader Port 2		Reader Red Light	Reader Green Light	Reader Buzzer	CDVI (Red, Green & Blue)	
☑	Entrance #2	1	B1-00-25-E7	A22K [2-Door Controller]-AA-00-30-88	K1BT Reader Port 2		Reader Red Light	Reader Green Light	Reader Buzzer	CDVI (Red, Green & Blue)	
☑	Entrance #1	1	B2-00-02-F6	A22K [2-Door Controller]-AA-00-02-F0	K2 Reader Port 1		Reader Red Light	Reader Green Light	Reader Buzzer	CDVI (Red, Green & Blue)	
☑	My Office	1	B3-00-00-17	A22K [2-Door Controller]-AA-00-30-88	K3 Reader Port 1		Reader Red Light	Reader Green Light	Reader Buzzer	CDVI (Red, Green & Blue)	

MODIFYING A READER

From the ***Hardware*** tab, click on the ***Readers*** icon, select a reader from the list and click on the ***Properties*** button.



General Information

- **Display Name:** Identifies the reader throughout the ATRIUM software. We recommend using a name that is representative of the reader.
- **Active:** When selected, activates the usage of this reader.
- **LED color mode:** Identifies if the reader has a 2 or 3-color LED. Choices are Generic (Red & Green), CDVI (Red, Green & Blue) and Digital-F (Feedback).
- **Red LED Output:** If there is a red LED associated to the door reader, select the red LED's output name, otherwise, leave it unassigned.
- **Green LED Output:** If there is a green LED associated to the door reader, select the green LED's output name, otherwise, leave it unassigned.
- **Buzzer Output:** If there is a buzzer associated to the door reader, select buzzer's output name, otherwise, leave it unassigned.
- **Disable Keypas Code (26-bit):** When enabled, it will bypass the keypad family codes (0 and 255). This is commonly used for cameras that have a 26-bit Wiegand output with SHA-1 generator for license plate recognition.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

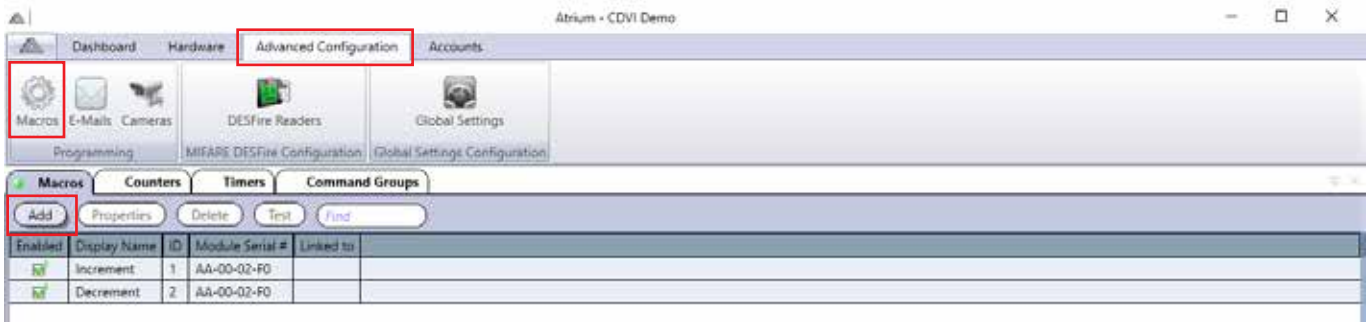
MACROS

Macros are used to cause an action on a device when triggering on an event. The macro instructs a device to perform a specific action like Activate Relay, Lock Door (Latched), etc.

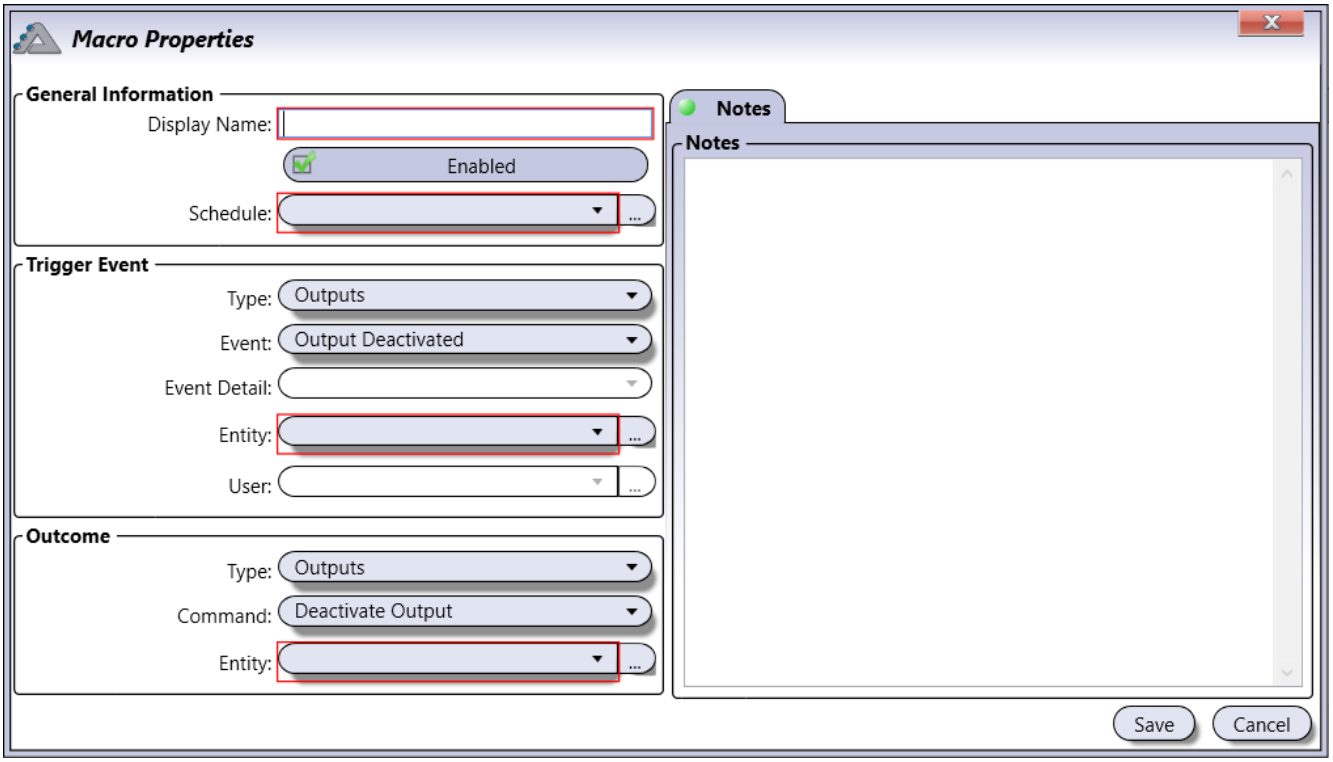
The ATRIUM application allows the creation of a macro by selecting the trigger event and the resulting command. Up to 100 macros can be created.

All macros of the ATRIUM access control system are saved on the 2-Door Controller module.

From the ***Advanced Configuration*** tab, click on the ***Macros*** icon.
Select the ***Macros tab*** and click on the ***Add*** button.



ADDING A MACRO



General Information

- **Display Name:** Identifies the macro throughout the ATRIUM software. We recommend using a name that is representative of the macro.
- **Enabled:** When selected, activates the usage of this macro.
- **Schedule:** Select the schedule which will define when the macro can be used.

Trigger Event (see "Trigger Event", page 95 for details on ''Trigger Event'')

- **Type:** Select the type of device/action with which the macro will be triggered.
- **Event:** Select by which event the selected type will trigger the macro. Empty means any event.
- **Event Detail:** Select by which event detail the selected event will trigger the macro. Empty means any event detail.
- **Entity:** Select by which entity of the selected type the macro will be triggered. Empty means any entity.
- **User:** Specify by which ''User'' the macro will be triggered. The "User" list is only available when the type "Area" and one of his event is selected (Access to area granted, access to area denied, user entered area and user exited area).

Outcome (see page 96 for details on ''Outcome'')

- **Type:** Select the type of device with which the macro will do a resulting command.
- **Command:** Selecte which command the selected type will do.
- **Entity:** Select the entity of the the selected type with which the macro will do a resulting command.

TRIGGER EVENT

Select the device type, the event and the entity that will be used as the trigger event. The entities are listed with the format "Module Serial #: Display Name".

Type	Event
Areas	Access Granted, Access Denied, Area accessed, Area Alarm Restored, Area Armed, Area Arming Request Sent, Area Disarmed, Area Disarming Request Sent, Area exited, Area Intrusion
Batteries	Added, Battery Absent, Battery Absent Restored, Deleted, Edited, Low Battery, Low Battery Restored
Card Enrollment	Deleted, Edited, Enrollment mode started via input alarm, Enrollment mode started via Programming Card, Enrollment mode started via controller button, Enrollment mode stopped, Enrollment mode stopped via Programming Card, Enrollment mode timeout
Doors	Added, Deleted, Door Alarm/Ajar, Door Alarm/Ajar restored, Door Bypassed by Emergency Input, Door Closed, Door Disabled, Door Enabled, Door Forced, Door Forced Restored, Door Lock, Door Locked, Door Open, Door Power Restored, Door Power Trouble, Door Pre-Alarm, Door Pre-Alarm Restored, Door Relocked (First Access/First Man in Cancelled), Door Restored by Emergency Input, Door Trouble (Contact), Door Trouble (Lock), Door Trouble Restored (Contact), Door Trouble Restored Lock, Door Unlocked, Door Unlocked by "First Access/First Man In", Door Unlocked by Operator, Edited, Lockdown access granted, Lockdown started, Lockdown stopped, PIN missing, User Entered using Door, User Exited using Door
Firmware	Added, Deleted, Edited, Firmware Update Completed, Firmware Update Started, Firmware Validation Completed, Web Page Update Started
Holidays	Added, Deleted, Edited, Holiday ended, Holiday started
Inputs	Added, Deleted, Edited, Input Closed, Input Opened
Lockdown	Added, Deleted, Edited, Lockdown started, Lockdown stopped
Locks	Added, Deleted, Door Lock Activated, Door Lock Bypassed by Emergency Input, Door Locked Deactivated, Door lock power restored, Door Lock Power Trouble, Door Lock Restored by Emergency Input, Edited
Login	Added, ATRIUM PC Service Logged In, ATRIUM SDK Logged In, Deleted, Edited, User Locked Out-Permitted login attempts exceeded, User login-ATRIUM software, User login-ATRIUM web page
Macro Counters	Added, Deleted, Edited,
Macro Timers	Added, Deleted, Edited, Macro Timer has been reloaded
Modules	Added, Deleted, Edited, Expander replaced, Module replaced
Outputs	Added, Deleted, Edited, Output Activated, Output deactivated
Primary Power	Added, Deleted, Edited, Primary Power Failure, Primary Power Failure Restored, Primary Power Trouble, Primary Power Trouble Restored
Readers	Added, Card Read, Deleted, Edited
Relays	Added, Deleted, Edited, Relay Activated, Relay deactivated, Relay pulse mode activated
Schedules	Added, Deleted, Edited, Schedule ended, Schedule started
Smart Supply Outputs	Added, Deleted, Edited, Smart Supply Trouble, Smart Supply Trouble Restored
Sub-Controllers	Module Missing, Module Reconnected
Tamper Switch	Added, Deleted, Edited, Tamper Restored, Tamper Trouble
User	Added, Deleted, Edited, User counter has been decremented, User counter has been set, User counter has reached zero

OUTCOME

Select the device type and the command then select the entity on which the command will be applied. The entities are listed with the format "Module Serial #: Display Name".

Type	Command
Areas	Arm, Disarm
Doors	Disable access (reader), Enable access (reader), Grant Access, Lock Door (permanent), Reset Door, Timed Unlock, Unlock Door (Latched)
Inputs	Bypass, Unbypass
Lockdown	Start, Stop
Outputs	Activate Output, Deactivate Output, Timed Activation
Relays	Activate Relay, Deactivate Relay, Timed Activation

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING A MACRO

Select a macro from the list and click on the ***Properties*** button. See "Adding a Macro" on page 88 for more information.

DELETING A MACRO

Select the macro from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

ADVANCED MACROS

Atrium now offers Advanced Macros, with these, you can program functions to be performed on any event in real time.

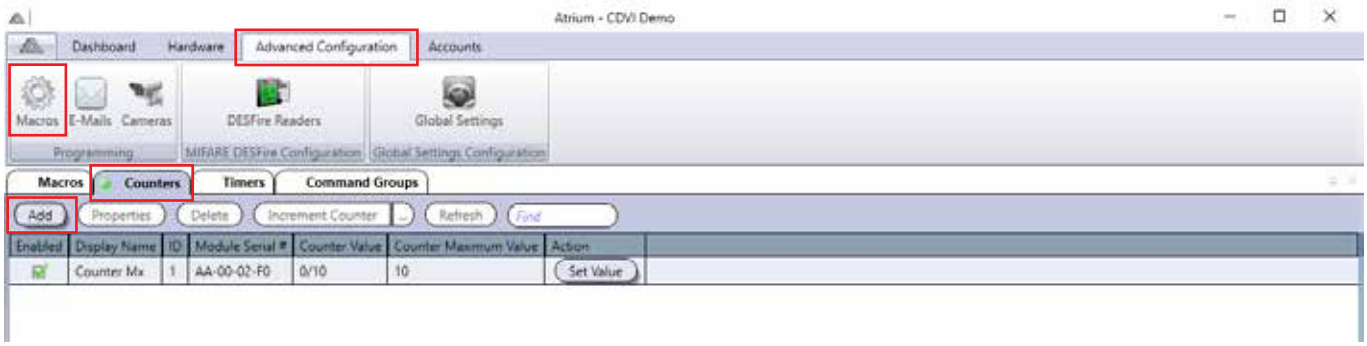
The event must be generated on the module itself (locally). If the event is from another controller, you must program the Macro for that controller. Each controller can manage 100 macros. The resulting command can be executed/run on the same or any other controller.

MACRO COUNTER

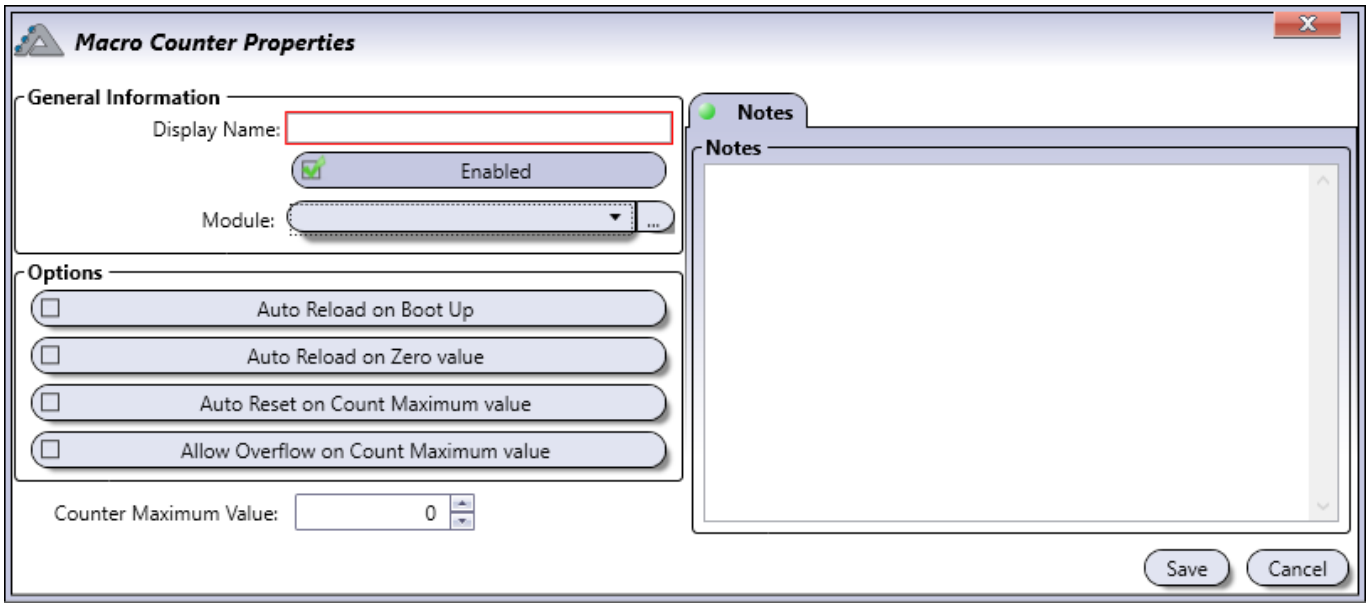
Generic, power and flexible counters allow you to tally and manage occupancy in real time.

Examples for a macro counter application include parking lot management and user group management (limiting the number of people in a fitness center or on a production floor).

From the ***Advanced Configuration*** tab, click on the ***Macros*** icon. Select the ***Counters*** tab and click on the ***Add*** button.



ADDING A MACRO COUNTER



General Information

- **Display Name:** Identifies the macro counter throughout the ATRIUM software. We recommend using a name that is representative of the macro counter.
- **Enabled:** When selected, activates the usage of this macro counter.
- **Module:** Select which module the macro counter will be saved on.

Options

- **Auto Reload on Boot Up:** When selected, the counter will reset to the Max value after the board is rebooted (due to power failure or service).
- **Auto Reload on Zero Value:** When selected, the counter will reload to the maximum value once the count reaches zero.
- **Auto Reset on Count Maximum value:** When selected, the counter will reset to zero when the count reaches maximum value.
- **Auto Overflow on Count Maximum value:** When selected, this allows to count to exceed the maximum value.
- **Counter Maximum Value:** Set the counter's maximum value.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING A MACRO COUNTER

Select a macro counter from the list and click on the ***Properties*** button. See "Adding a Macro Counter" on page 93 for more information.

DELETING A MACRO COUNTER

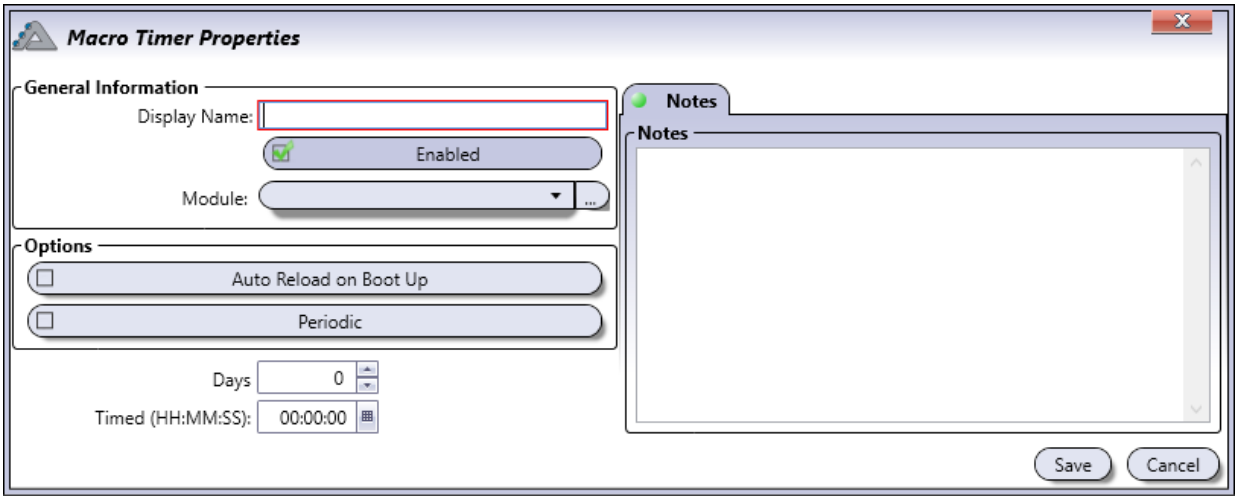
Select the macro counter from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

MACRO TIMER

Macro Timers add the flexibility of timed actions to a macro.

From the ***Advanced Configuration*** tab, click on the ***Macros*** icon. Select the ***Timers*** tab and click on the ***Add*** button.

ADDING A MACRO TIMER



General Information

- **Display Name:** Identifies the macro timer throughout the ATRIUM software. We recommend using a name that is representative of the macro timer.
- **Enabled:** When selected, activates the usage of this macro timer.
- **Module:** Select which module the macro timer will be saved on.

Options

- **Auto Reload on Boot Up:** When selected, the timer will restart after a system reboot.
- **Periodic:** When selected, the timer will repeat.
- **Days:** Set the amount of days the action will be performed.
- **Timed (HH:MM:SS):** Set the amount of time (hours:minutes:seconds) the action will be performed. Which will be added to the day if applicable.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING A MACRO TIMER

Select a macro timer from the list and click on the ***Properties*** button. See “Adding a Macro Timer” on page 95 for more information.

DELETING A MACRO TIMER

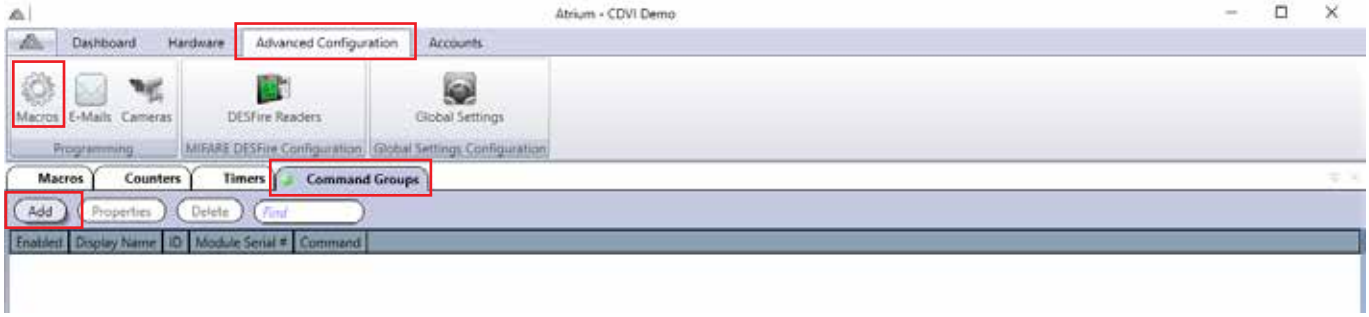
Select the macro timer from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

MACRO COMMAND GROUP

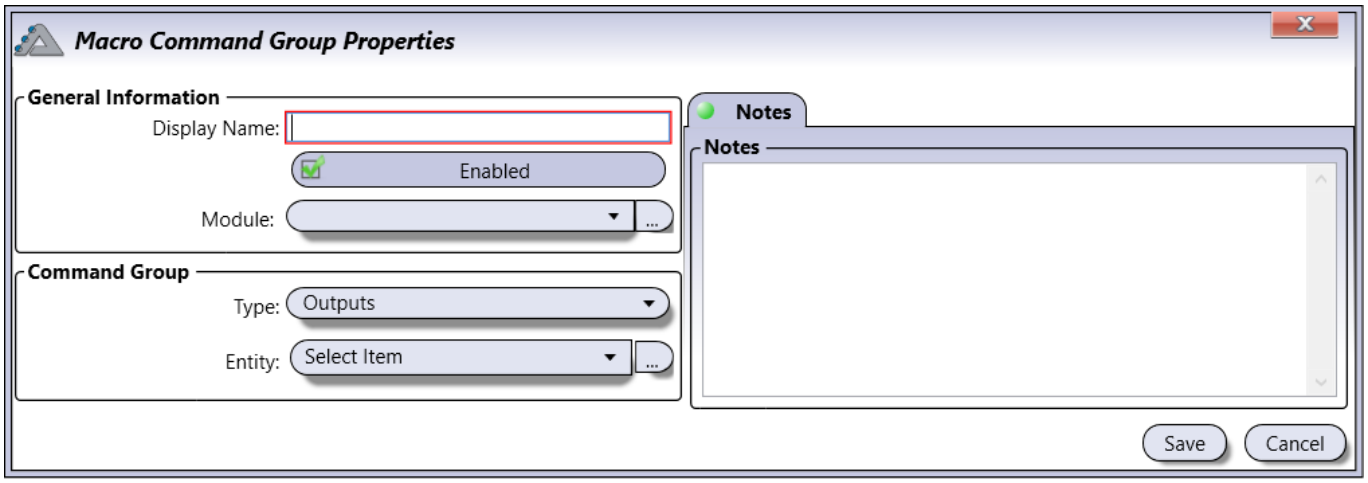
Macro Command Groups permit the creation of multiple doors, inputs,relays, outputs and areas.

Grouped objects are managed in Macro Commands. (see Macro Commands p.92)

From the ***Advanced Configuration*** tab, click on the ***Macros*** icon. Select the ***Command Groups*** tab and click on the ***Add*** button.



ADDING A COMMAND GROUP



General Information

- **Display Name:** Identifies the command group throughout the ATRIUM software. We recommend using a name that is representative of the macro command group.
- **Enabled:** When selected, activates the usage of this macro command group.
- **Module:** Select which module the macro command group will be saved on.

Command Group

- **Type:** Select the type of device/action with which the command group will be triggered.
- **Entity:** Select by which entity of the selected type the command group will be triggered.

Notes Tab

Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

Save Button

Use the ***save*** button to save changes.

Cancel Button

Use the ***cancel*** button to ignore changes.

MODIFYING A COMMAND GROUP

Select a command group from the list and click on the ***Properties*** button. See “Adding a Command Group” on page 97 for more information.

DELETING A COMMAND GROUP

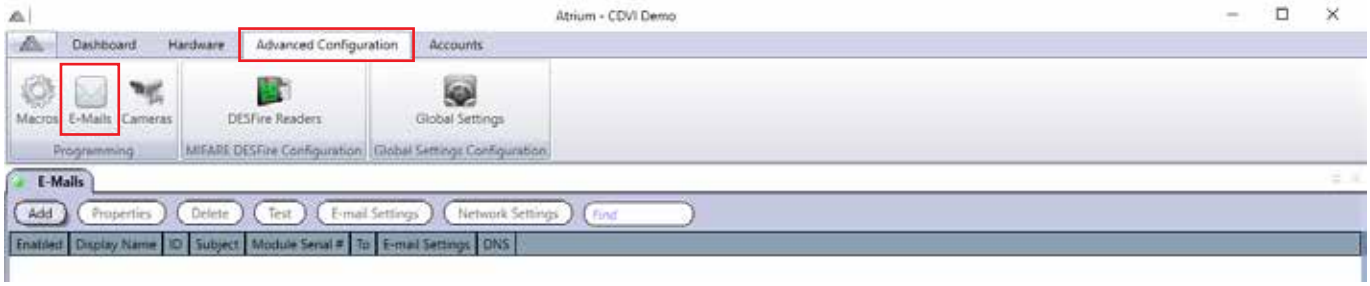
Select the comannd group from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

EMAIL NOTIFICATIONS

Email notifications are used to notify the recipient of this e-mail on the status of the system. You can choose which schedule, the type of entity and any specific event you wish to receive email notification. You must configure the email setting, see page 75, for the email notification option to work correctly.

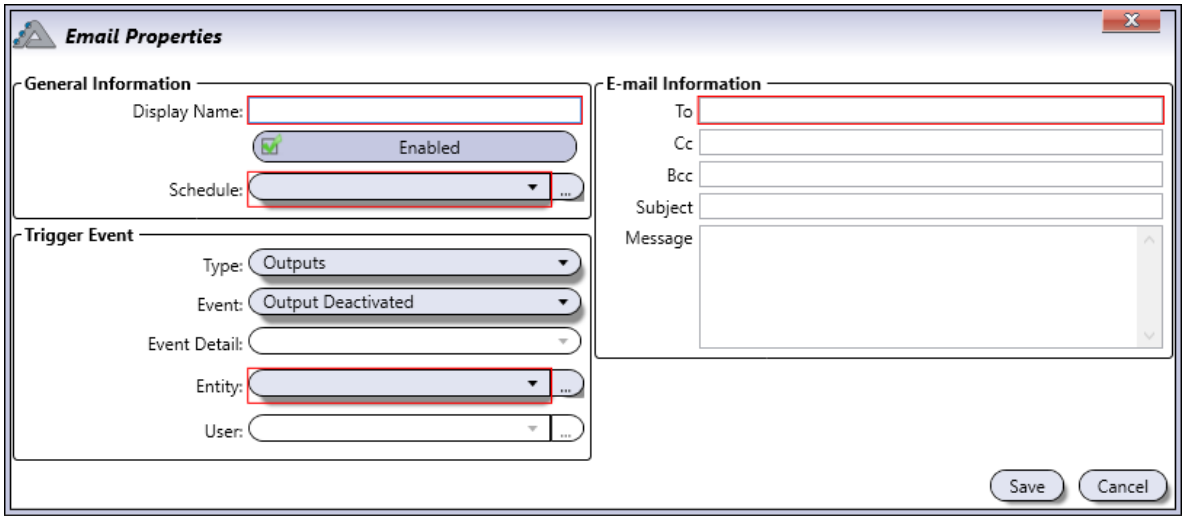
You must add the email notification on the module to which the entity type selected was connected.

From the ***Advanced Configuration*** tab, click on the ***Emails*** icon.



ADDING AN EMAIL NOTIFICATION

Click on the ***Add*** button. The following window will pop up.



General Information

- **Display Name:** Identifies the email notification display name
- **Enabled:** When selected, activates the email notification.
- **Schedule:** Select the schedule which will define when the email will be send.

Trigger Event

- **Type:** Select by which type of device/action email function will be activated.
- **Event:** Select on which specific event email function will be activated.
- **Event Detail:** Select on which specific event detail email function will be activated.
- **Entity:** Select by which entity of the selected type email function will be activated.
- **User:** Specify by which ''User'' the email will be triggered. The "User" list is only available when the type "Areas" and one of his event is selected (Access to area granted, access to area denied, user entered area and user exited area).

E-mail Information

- **To:** Enter email receiver
- **Cc:** Enter carbon copy email receiver.
- **Bcc:** Enter blind carbon copy email receiver. (other email receiver won't see is email address)
- **Subject:** Enter email subject.
- **Message:** Enter any relative message of sending email.

MODIFYING AN EMAIL NOTIFICATION

Select an email notification from the list and click on the ***Properties*** button.

DELETING AN EMAIL NOTIFICATION

Select the email notification from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation.

TESTING AN EMAIL NOTIFICATION

Select the email notification from the list and click on the ***Test*** button. An email will be sent to the specified address in the notification email.

CAMERAS

See who is at the door and what is happening within ATRIUM's web page. Up to ten IP cameras can be associated to a controller and expanders. Configuring the camera is done via ATRIUM's software or web page.

Supported IP cameras:

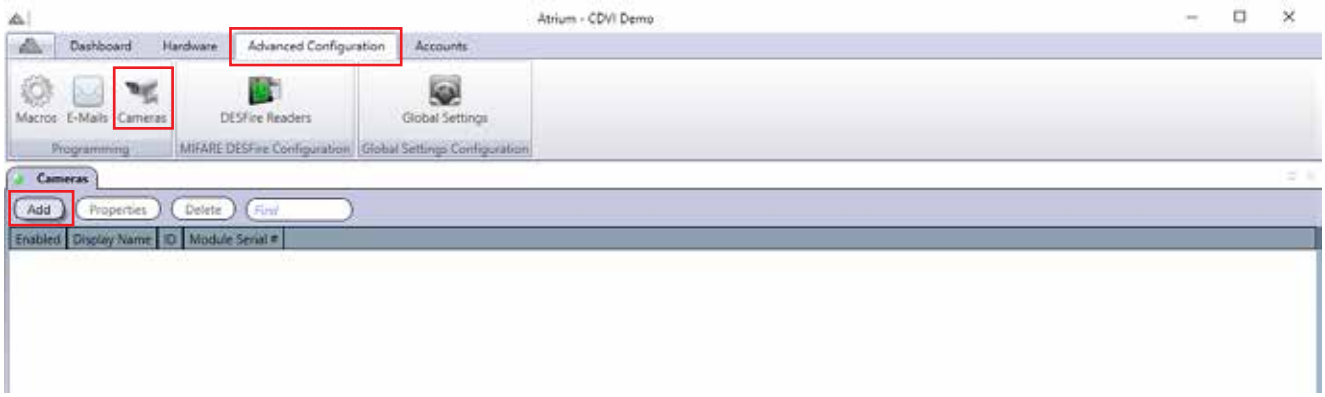
- AXIS P3304
- Vivotek FD8162

Supported formats:

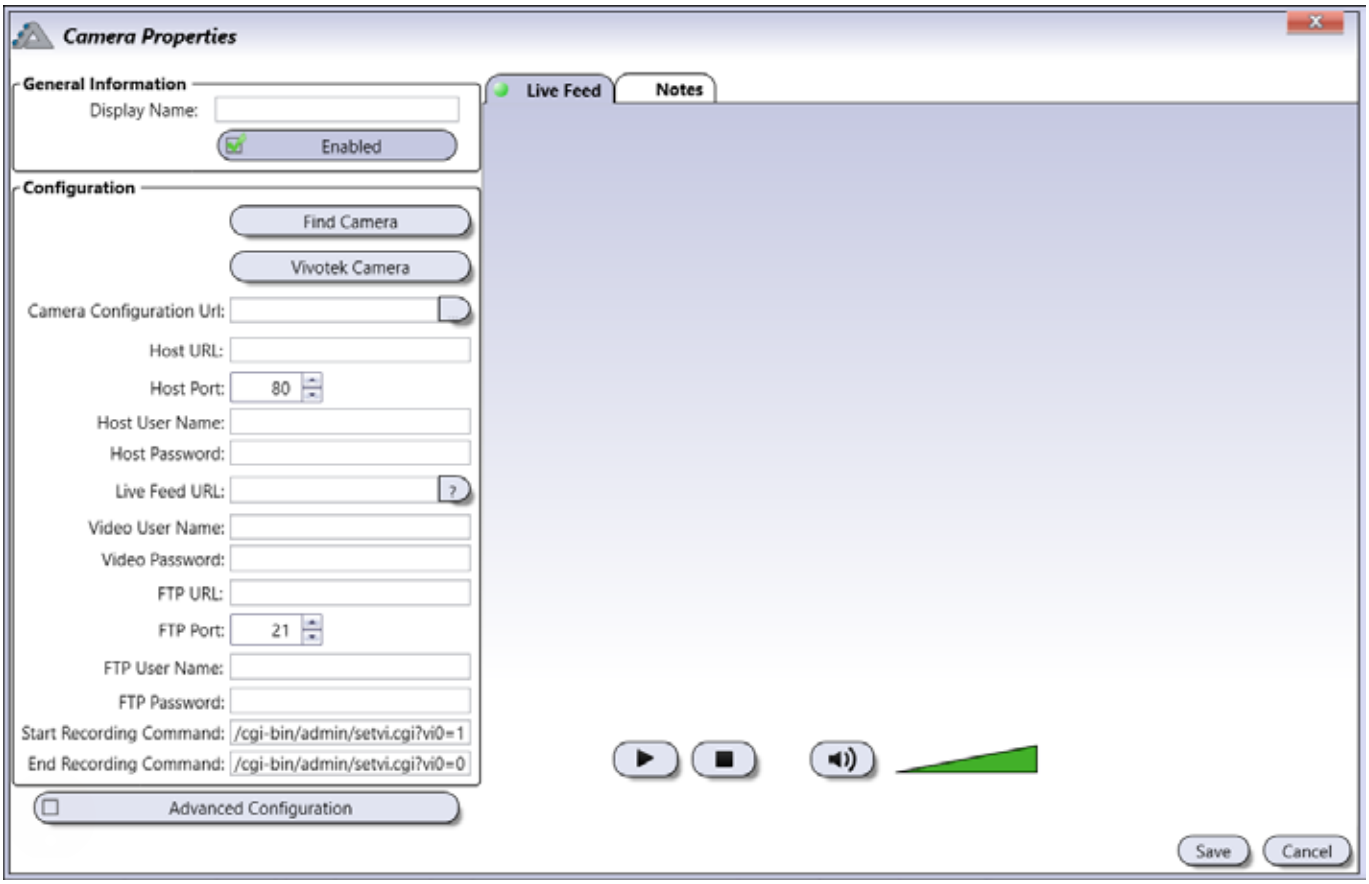
- MJPEG

From the ***Advanced Configuration*** tab, click on the ***Cameras*** icon. Then, click on the ***Add*** button.

A maximum of 10 cameras may be assigned per controller.



ADDING A CAMERA



General Information

- **Display Name:** Enter the camera display name. This name will appear in the list of cameras added to the system.
- **Enabled:** When selected, activates the camera.

Configuration

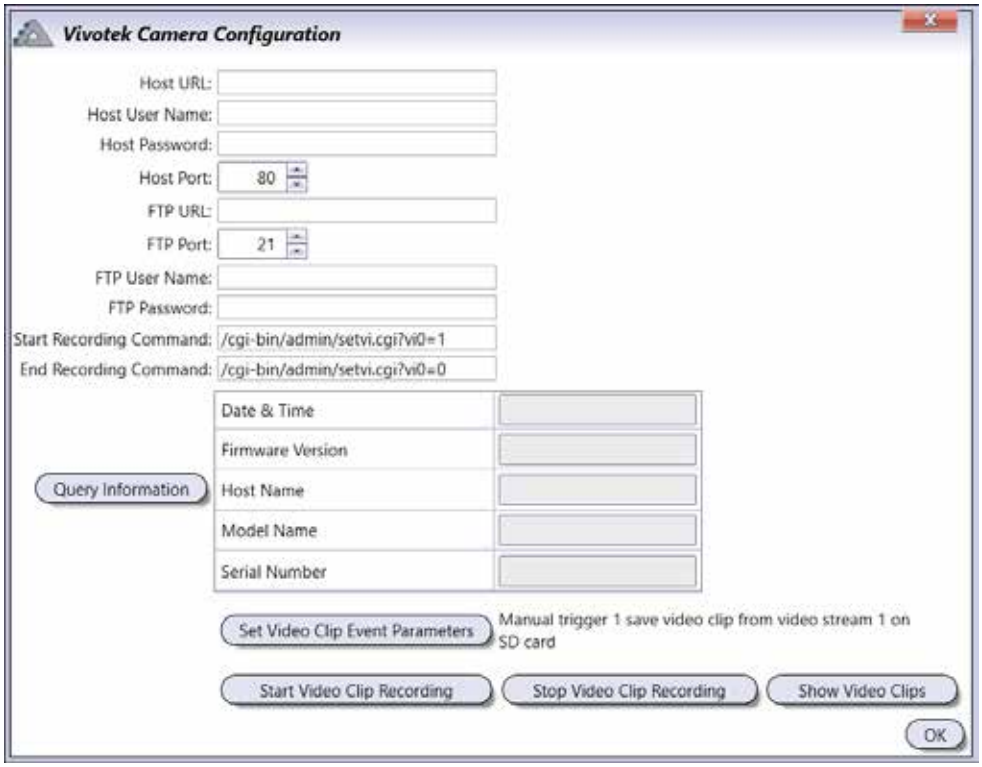
Before configuring camera, refer to the camera's manual, web page or network administrator to obtain camera IP address and port setting. Vivotek model FD8162 has been pre-configured in ATRIUM software. Other VIVOTEK models may also work.

- **Find Camera:** Click the ***Refresh*** button to find the camera(s) on the network. Once selected fill out the fields accordingly.

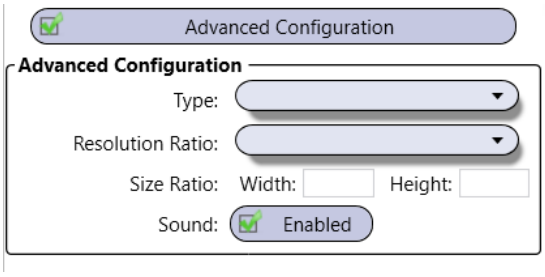
When you fill out the field "Video User Name" and "Video Password", this will automate the login process when viewing the camera in ATRIUM's web page. If this information is omitted, the camera will request the username and password every time you view it.

- **Vivotek Camera:**

  When choosing "Vivotek": The "VIVOTEK Properties" window will appear asking to fill out general settings and set desired parameters:



Advanced Configuration



- **Type:** Select one of the stream types.
- **Resolution Ratio:** Select one of the resolution ratio.
- **Size Ratio:** Manually enter the width and height of the screen.
- **Sound:** If the camera has a microphone, enable the Sound selection.

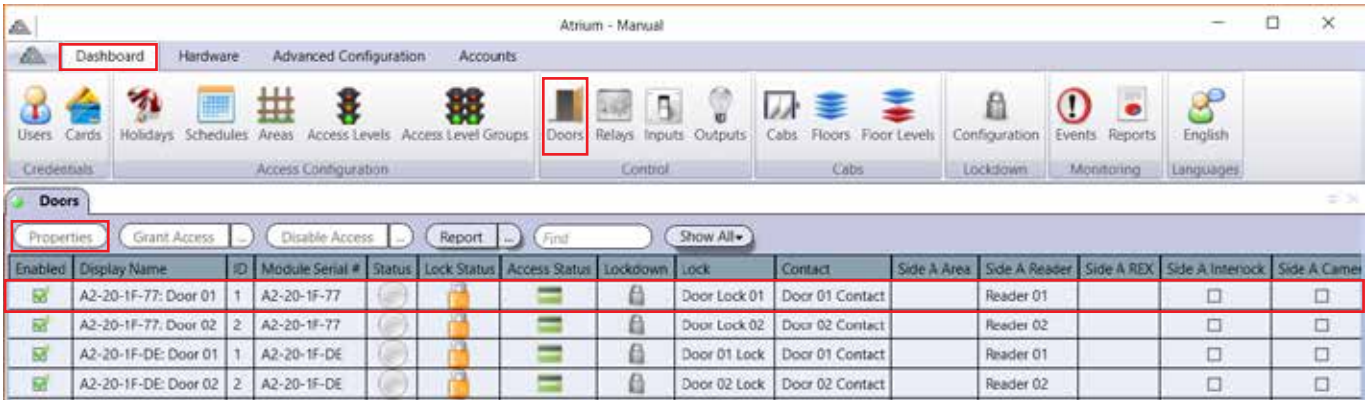
The "Type", "Resolution Ratio", and "Size Ratio" fields may be used if the Stream profile selected needs to be fine tuned. This is usually not required. It is easier to select an alternative Stream profile to obtain the best results.

Live Feed Tab: The live feed of the camera can be viewed in the Live Feed Tab.

Notes Tab: Use the Notes text field to record any additional notes that may be required. We recommend that you keep a log of what settings were changed and when they were changed.

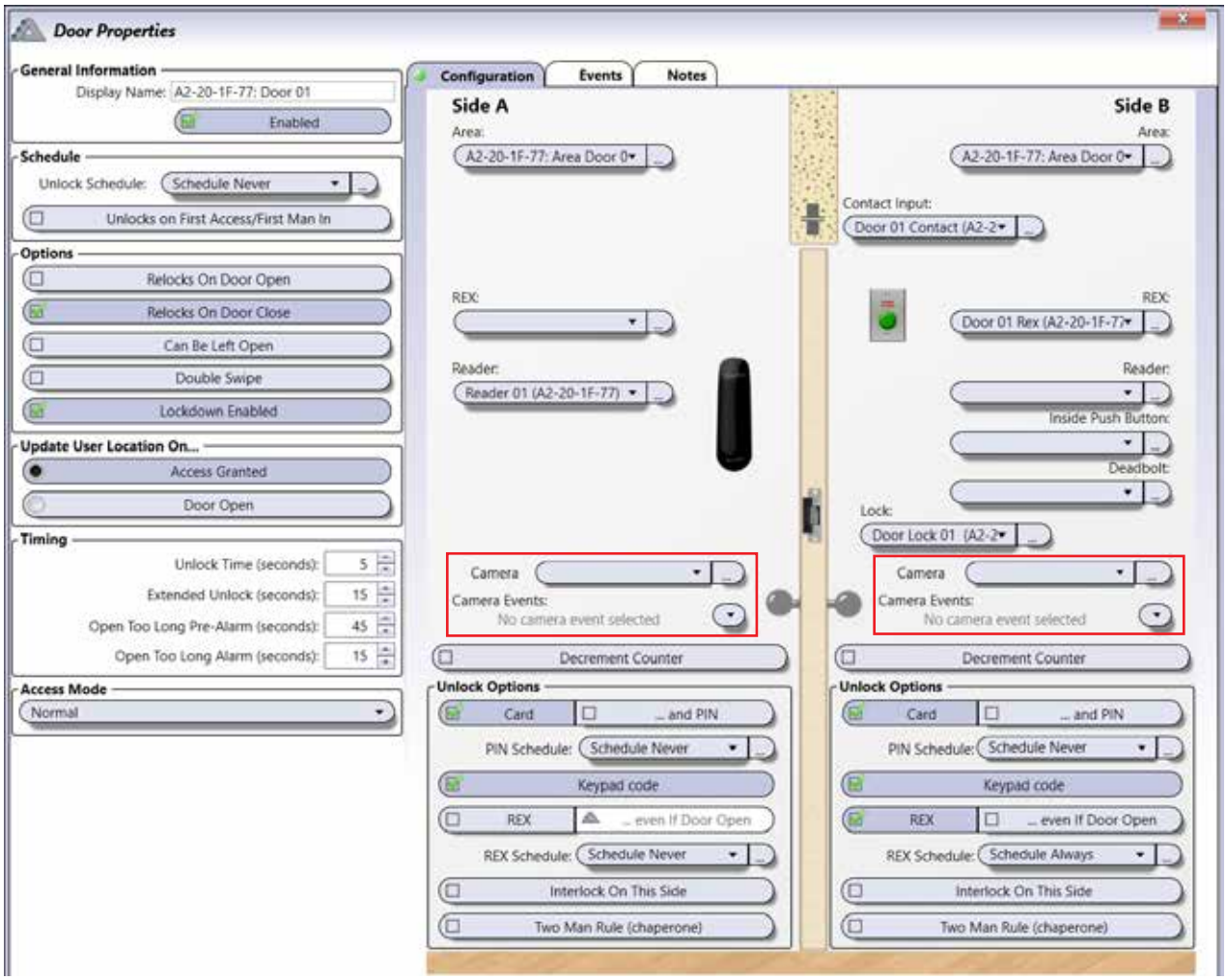
ASSOCIATE THE CAMERA TO A DOOR

From the Dashboard tab, click on the ***Doors*** icon, select/highlight a door in the list and click the ***Properties*** button.



In Advanced view, associate the camera to the door by selecting it in the Camera field.

You can assign 2 cameras to one door. Simply assign a camera to both sides (Side A – Side B) of the door. A maximum of 10 cameras may be assigned per controller.

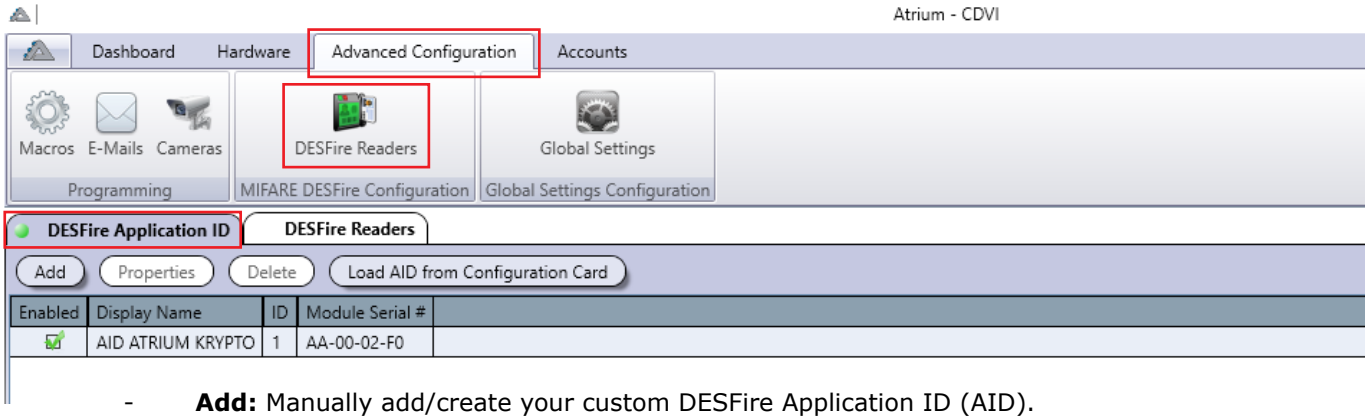


DESFIRE APPLICATION ID AND READERS

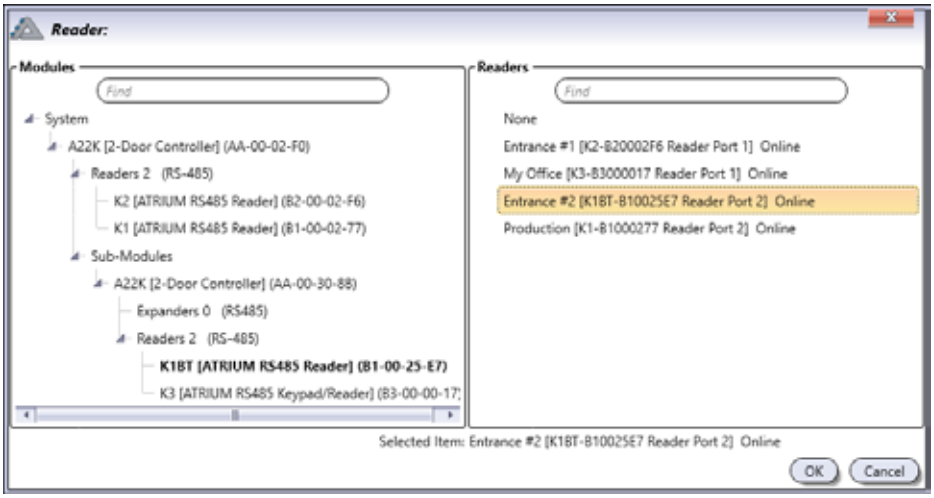
DESFIRE APPLICATION ID

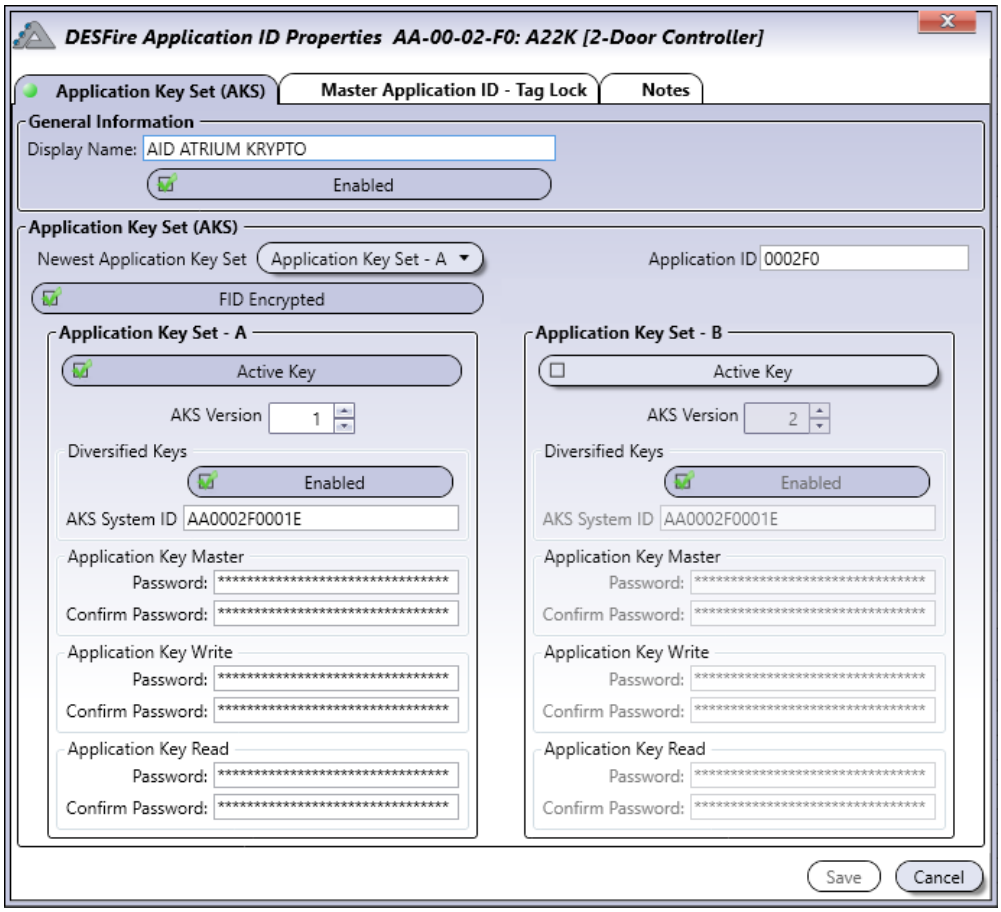
ATRIUM's KRYPTO system automatically generates a unique DesFire Application ID (AID) and associated key sets. This site-specific AID is identified as "AID ATRIUM KRYPTO" in the system. This unique, site-specific ATRIUM KRYPTO AID is automatically uploaded to the KRYPTO readers by the A22K KRYPTO controller. No programming app or external intervention at the readers by the service technician is required. Optionally, the ATRIUM KRYPTO system operator can create a "custom" AID if preferred. Simply click the "ADD" button to create a custom AID. Whether you choose the automatically generated ATRIUM KRYTPO AID or create a custom AID, it is strongly recommended to create a Configuration Card containing your system's AID for disaster recovery purposes. The Configuration Card is required to initialize the reader with your AID upon original implementation of the system (for a custom AID) , after a power failure, reader tamper alarm or when replacing system controller hardware (ATRIUM KRYPTO or custom AID). Store this Configuration Card in a secure place for future retrieval as necessary.

From the ***Advanced Configuration*** tab, click on the ***DESFire Readers*** icon. Double click on the default AID to modify or click on the ***Add*** button, to add a new one.



- **Add:** Manually add/create your custom DESFire Application ID (AID).
- **Properties:** Displays all the relevant key set information of the selected AID.
- **Delete:** Removes the selected AID from the system.
- **Load AID from Configuration Card:** Select the most conveniently located KRYTPO reader to scan your Configuration Card containing your custom AID.





General Information

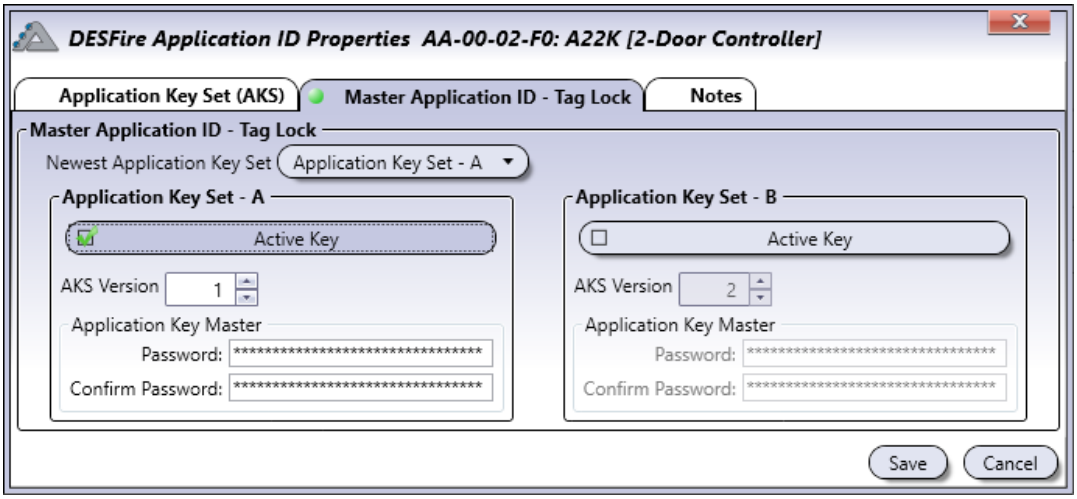
- **Display Name:** Identifies the application ID (AID) display name
- **Enabled:** When selected, activates the application ID (AID).

Application Ket Set (AKS)

- **Newest Application Key Set:** Each DESFire application has two key sets, A and B. This is in order to allow a smooth transition from existing key sets to new ones. By default the ***"Application Key Set - A"*** is active.
- **Application ID (AID):** This identifies the application (AID) installed and used by the system. Must be a 6-digit hexadecimal between 0-F (3 bytes).
- **FID Encrypted (File IDentification):** When activated, adds an extra layer of secure communication between reader and tag for File read/write manipulation. A 32-bit CRC (Cyclic Redundancy Check) is calculated over the stream and attached to the transmitted data. The stream is then encrypted with AES128 cryptogram.

Application Ket Set - A or B

- **Active Key:** When selected, activates the application key set.
- **AKS Version:** Tracks key set version changes. Application key sets A and B must be different otherwise the key set transition from A to B will not be possible. Must be a decimal number from 1 to 255.
- **Diversified keys:** Diversified keys enhance security even further. Activating this option ensures a unique key set is assigned to each individual DESFire EV2 TAG on site. This is accomplished using the tag's unique number (CSN) and other encryption factors. If de-activated, a single, secure and unique site-generated key set is assigned to all the DESFire EV2 tags used on site.
- **AKS System ID:** Used with Diversified keys. This is the seed value used in the key diversification process. Must be a 12-digit hexadecimal number containing letters A to F and numbers 0 to 9 (6 bytes).
- **Application Key Master:** The application key "Master" manages file creation and deletion. You need to authenticate with this key to be able to create and delete files inside the application on the DESFire credential. Must be a 32-digit hexadecimal number containing letters A to F and numbers 0 to 9 (16 bytes).
- **Application Key Write:** The application key "Write" manages file writing. You need to authenticate with this key to be able write to the files inside the application on the DESFire credential. Must be a 32-digit hexadecimal number containing letters A to F and numbers 0 to 9 (16 bytes).
- **Application Key Read:** The application key "Read" manages the file read. You need to authenticate with this key to read from the files inside the application on the DESFire credential. Must be a 32-digit hexadecimal number containing letters A to F and numbers 0 to 9 (16 bytes).

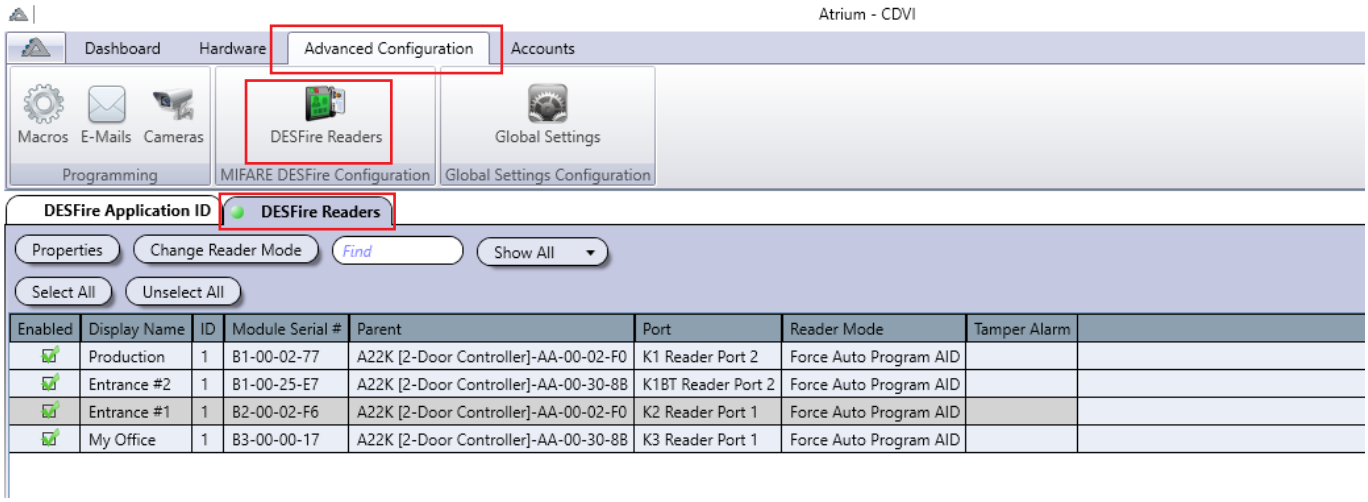


Master Application ID - Tag Lock

- **Master Application ID - Tag Lock:** This key is the master key of the PICC (Proximity Integrated Circuit Chip). By default, CDVI DESFire EV2 credentials use the default NXP mifare DESFire master keys which are all 0 (32 digits). This allows the CDVI site application (AID) to be installed on CDVI's DESFire EV2 card. The CDVI's DESFire EV2 credential will allow the installation and deletion of other applications on the credential. You can prevent other application providers from using CDVI DESFire credential by changing the default master key. The card will then be locked for other application providers. Only the owner of the "Tag Lock" will be able to add or remove applications on the DESFire credential. Must be a 32-digit hexadecimal number containing letters A to F and numbers 0 to 9 (16 bytes).

DESFIRE READERS

The DESFire reader tab is the place to change the operating mode of a KRYPTO card reader. You can also convert any of the KRYPTO card readers as a programmer. The DESFire card programmer is a card management tool used to; enroll a card, enroll a card with a custom number, read a card number, format a card, create a DESFire configuration card or create an OSDP installation card.



Properties: Opens the properties menu of the selected DESFire reader. The selected reader will be used for the following operations/commands:

- **Create a New Card (recommended):** Will generate a card number and register it in the card with the programmer's selected DESFire application. The card can be read by KRYPTO readers having the same DESFire application and added, as usual, by the administrator into the ATRIUM system.

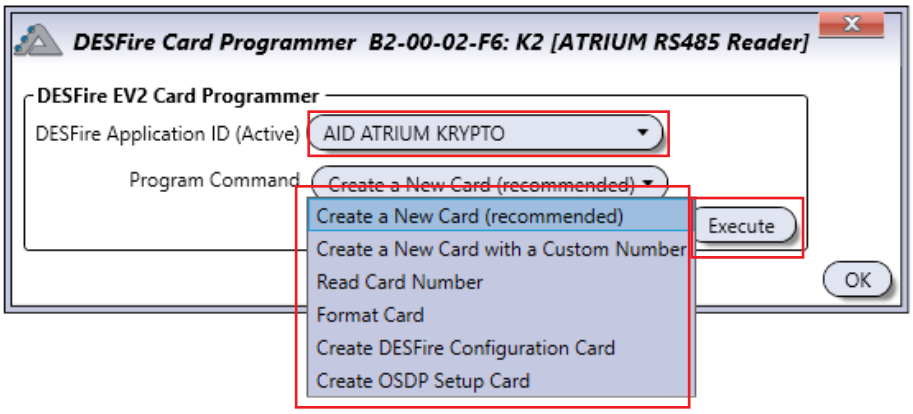
- **Create a New Card with a Custom Number:** You will be able to add a custom number and register it in the card with the DESFire application selected from the programmer. The card can be read by KRYPTO readers having the same DESFire application and added, as usual, by the administrator into the ATRIUM system.

- **Read Card Number:** Reads and displays the card number that is written on the card.

- **Format Card:** Deletes all DESFire applications installed on the DESFire card except for the CDVI "Master" application.

- **Create DESFire Configuration Card:** Saves the key sets and settings of the selected DESFire application to a card. This in case of major forces like; building bruning down, irreversible vandalism of the ATRIUM system, etc. You will be able to reinstall the same DESFire application in a new ATRIUM system and users will be able to keep the same cards.

- **Create OSDP Setup Card:** Creates an OSDP setup card. This same card can be used for all OSDP installations.

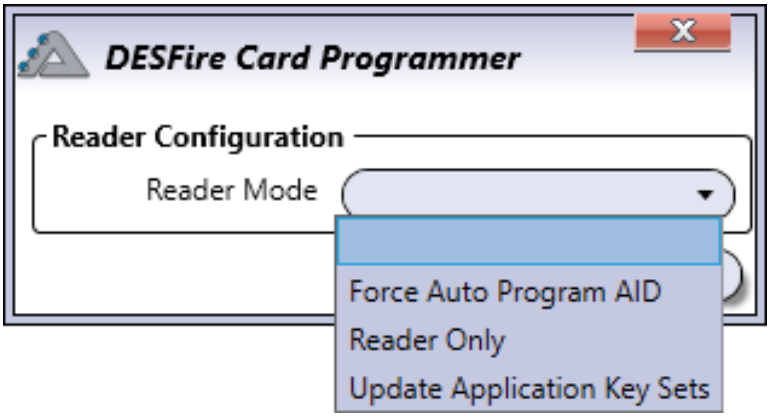


Select from which **"DESFire Application ID"** the programmer will execute command. Choose a **"Command"** from the drop down list, click **"Execute"**.

The selected KRYPTO card reader will start flashing green and red. A constant 2 second green LED confirms success, a constant 2 second red LED confirms failure. The reader times out after 30 sec.

Change Reader Mode: KRYPTO reader operating modes:

You can change the operating mode of one KRYPTO reader at a time or several KRYPTO readers at the same time. Use “Select All” and “Unselect All” button.



- **Force Auto-Program AID (Default Mode):** This is the default mode for all KRYPTO readers and allows you to install the active DESFire application of a site on any DESFire EV2 credentials from CDVI. The DESFire Application will automatically be transferred to the CDVI DESFire EV2 credential once presented to the KRYPTO card reader. CDVI’s DESFire EV2 credential can be added to the ATRIUM system as usual thereafter. It will also allow the update of the key set (A or B) of the active DESFire Application in the ATRIUM system.

The **“Master”** controller of each ATRIUM installation generates a unique DESFire application and its key set per site.

- **Update Application Key Sets:** This mode is used to update the key set (A or B) of the active DESFire Application in the ATRIUM system. While in this mode no other DESFire applications can be installed on the credential. The DESFire application key set will automatically be updated once the DESFire credential is presented to the reader (A to B or B to A).

- **Reader Only:** This mode allows the reading of cards with the DESFire application installed and active in the ATRIUM KRYPTO system. While in this mode no other DESFire applications can be installed and no key set updates can be made on the credentials. The DESFire application can be installed on each new card using the “DESFire EV2 Card Programmer” of the ATRIUM system. See chapter 5, “DESFire Card Programmer” to know how to manually program a DESFire card.

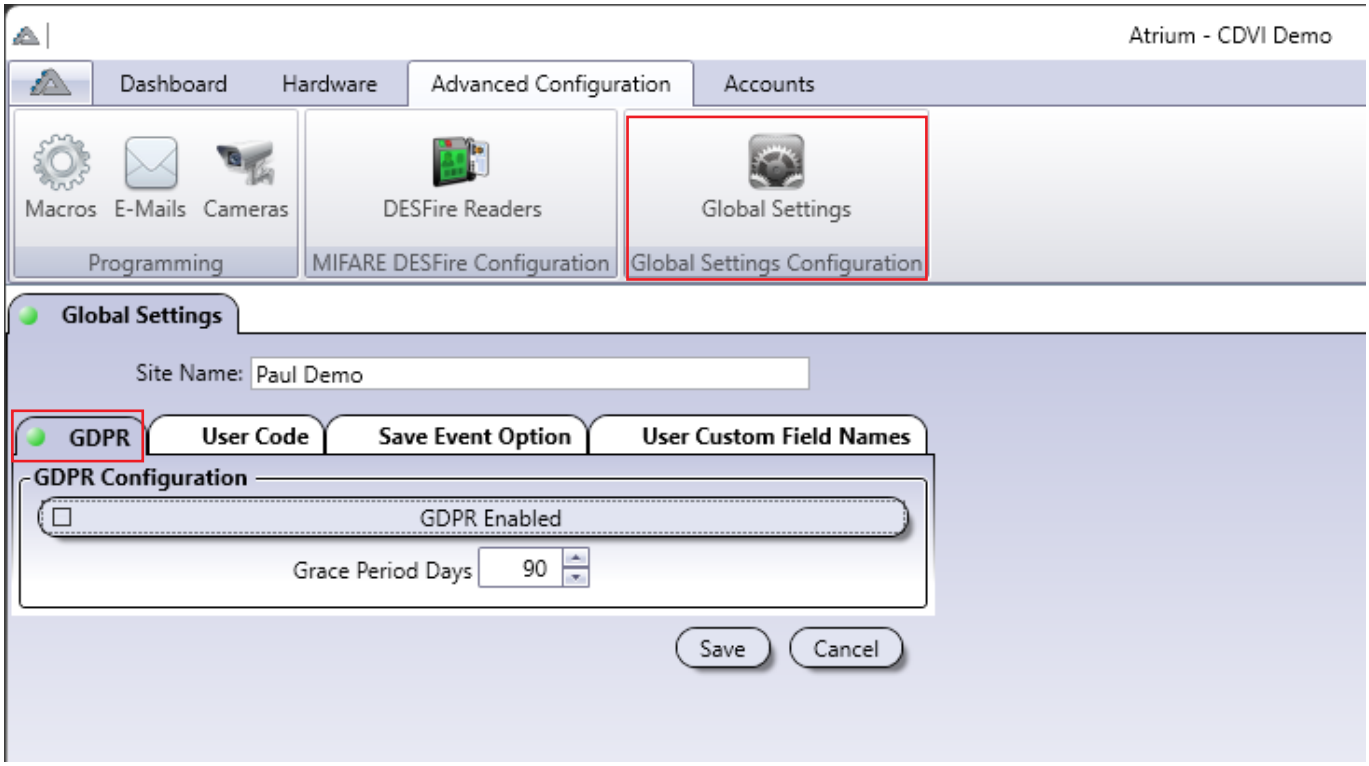
GLOBAL SETTINGS

Global configurations will be applied on the entire ATRIUM system site. Here are some applications:

GDPR Configuration (General Data Protection Regulation)

In many countries, companies must ensure they're in compliance with General Data Protection Regulation (GDPR). Controllers and processors of personal data must put in place appropriate technical and organizational measures to implement the data protection principles.

Click on ***"Save"*** after each change.

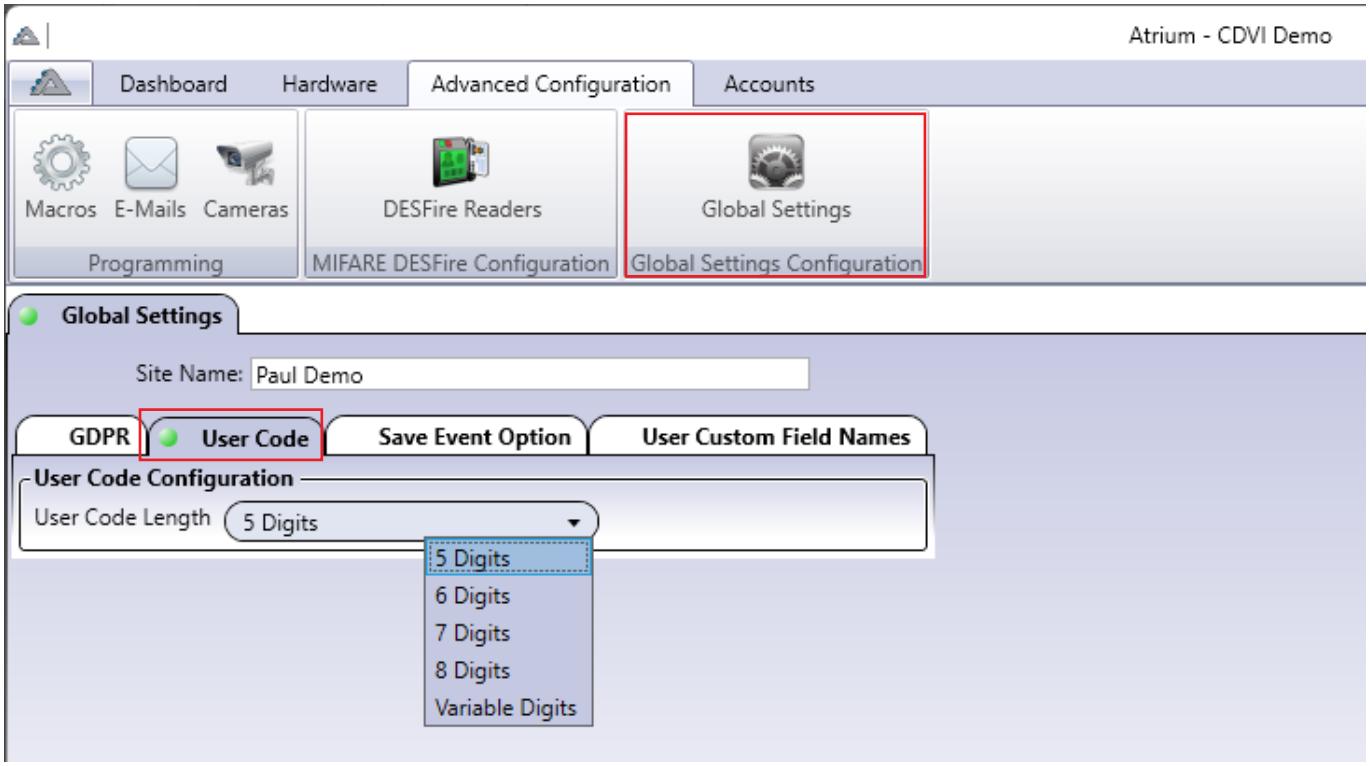


- **Site Name:** Enter the name of the site that will be displayed in the ATRIUM BT application.
- **GDPR Enabled:** When selected, activates the CNIL (GDPR) feature.
- **Grace Period Days:** Will keep personal data for the period chosen, by default, 90 days. After this period has elapsed, no personal events will be displayed or stored.

User Code

By default the keypad code length is 5-digits (between 00001 and 99999). It can be changed ONLY if you have the ***"Installer"*** User rights. The code length can be changed from 5 to 8 digits or variable (between 1 and 8 digits). In variable digits mode you must type "#" or "B" on CDVI keypad after the sequence in order to activate the command.

Click on ***"Save"*** after each change.

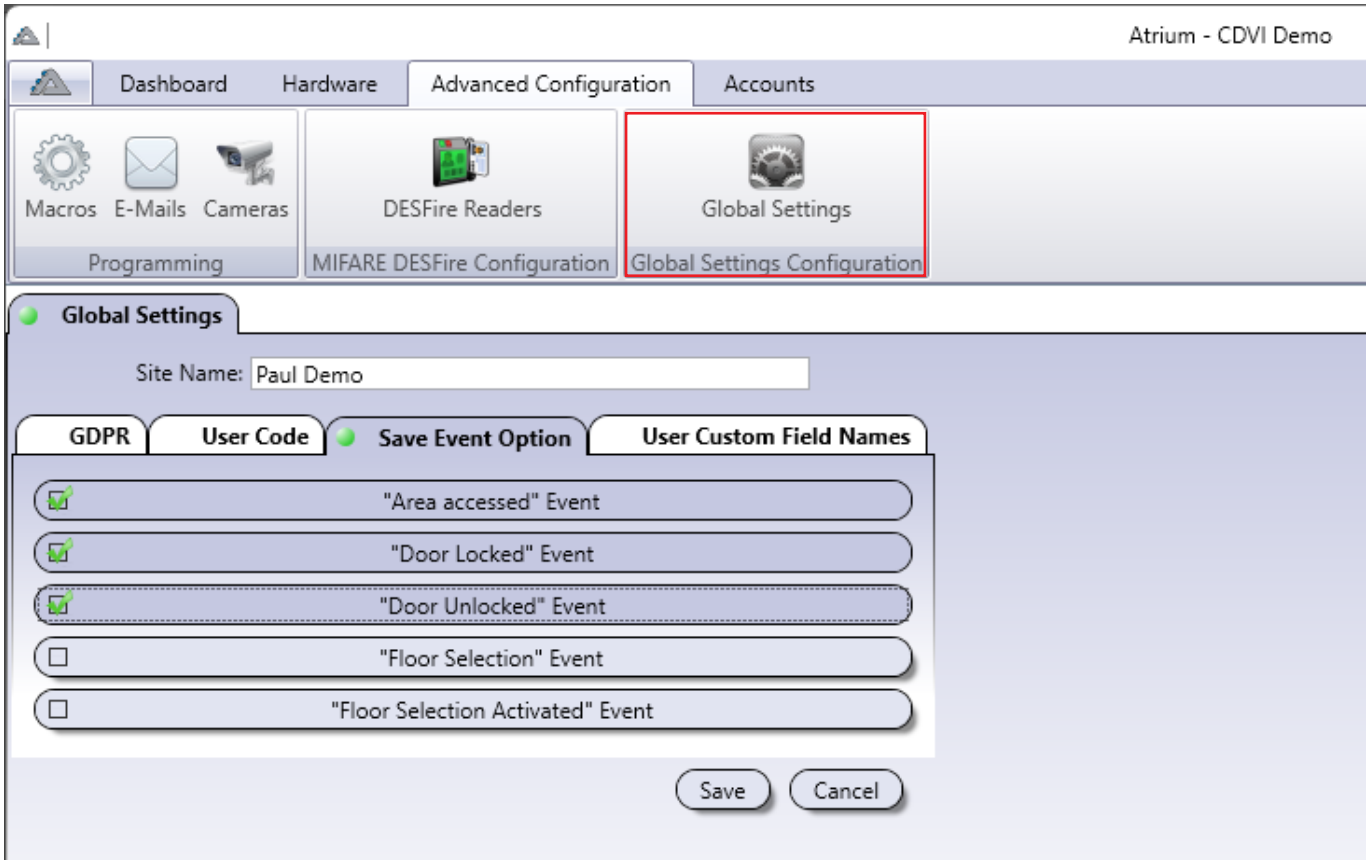


Save Event Option

Access granted will generate up to 4 events per access granted (Access Granted, Area Accessed, Door Unlocked and Door Locked). In some cases, it is not critical to record all of these events in the ATRIUM system. You could save buffer space by unchecking events that you no longer want to save in the ATRIUM system.

This option is ONLY available if you have ***"Installer"*** user rights.

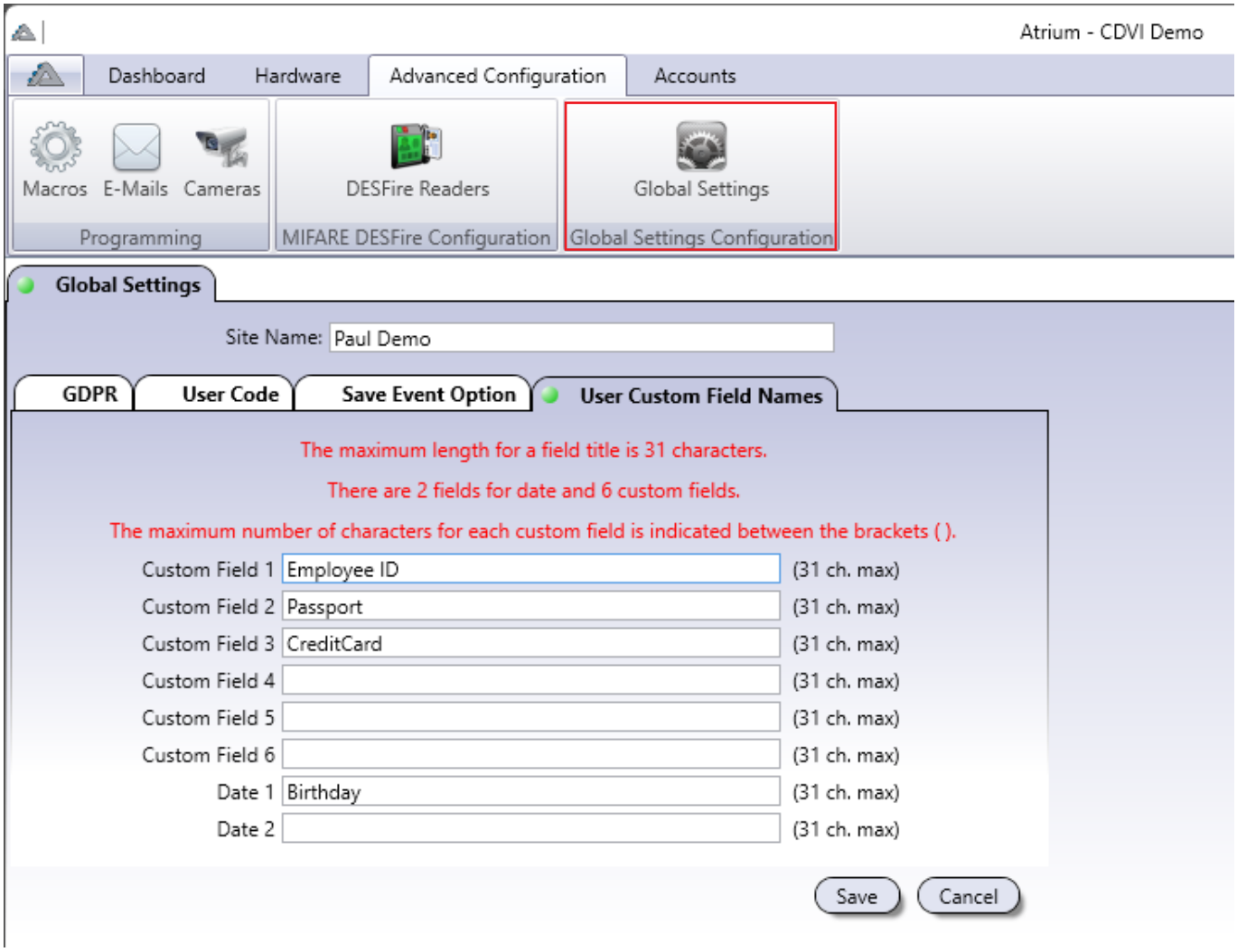
Click on ***"Save"*** after each change.



User Custom Field Names

You can name 8 custom user fields (6 alphanumeric fields and 2 date fields). These custom user fields will be available to all users and can be used for passport number, employee number, birthday or anything else as needed for your users.

Click on ***"Save"*** after each change.



INTRUSION (ALARM) INTEGRATION

Arm/disarm an intrusion detection system (burglar alarm) with a card The intrusion detection system must support key switch arming.

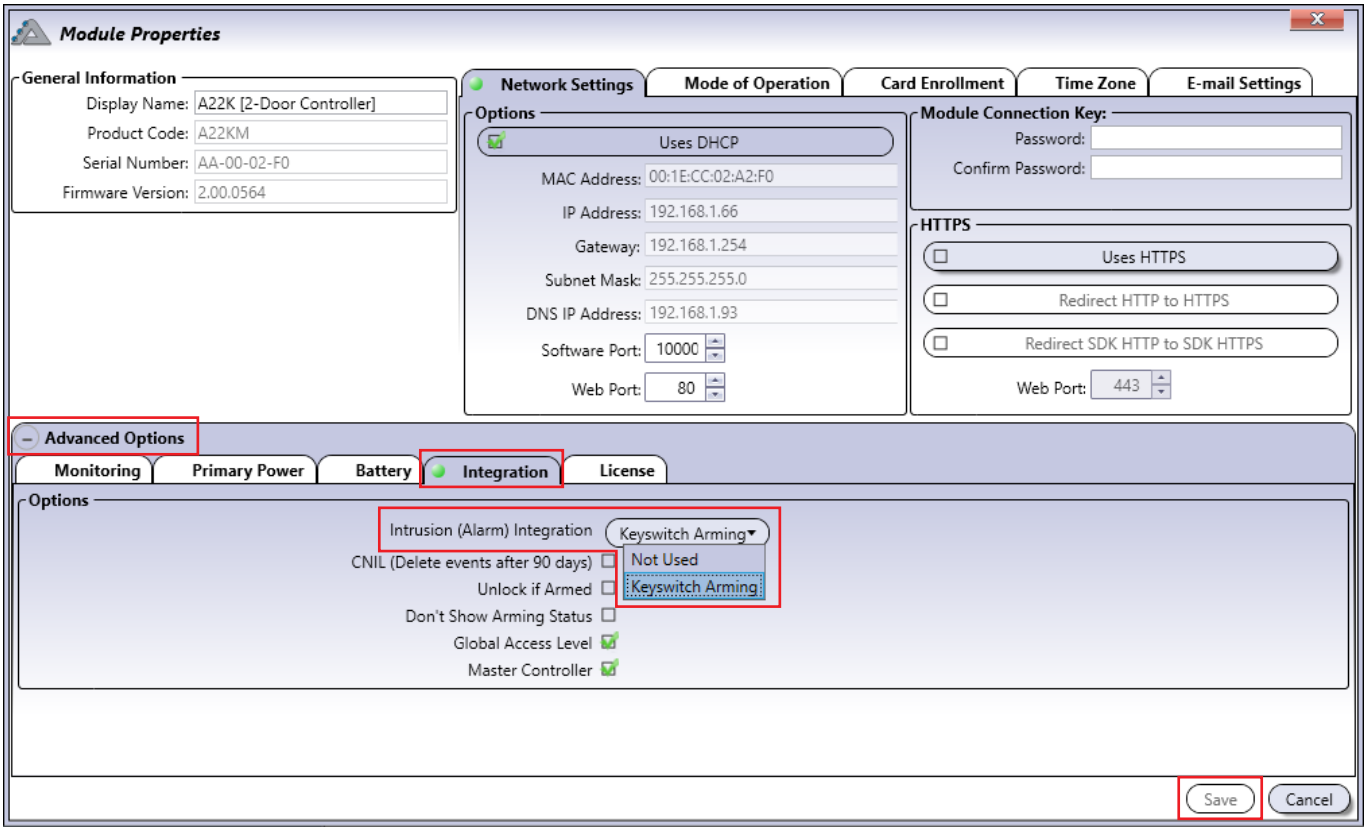
These are the options and advantages when you implement this feature:

- Select which cards have this capability.
    - Some cards may have the capability to arm and disarm.
    - Some cards may only arm.
    - Some cards may only disarm.
- Present the card to the reader 2 consecutive times (double-swipe) to arm.
- Present the card once (single-swipe) to disarm.
- View the armed or disarmed status in real time within the ATRIUM software or web page.
- Arm or disarm the intrusion (alarm) system from your smart phone, tablet or any web-enabled devise.
- Use a simple mouse click to arm or disarm in the ATRIUM software.
- Monitor the alarm condition of the intrusion (alarm) system when it is armed.
- Let ATRIUM send an email when an intrusion (alarm) is detected.

ENABLING INTRUSION (ALARM) INTEGRATION

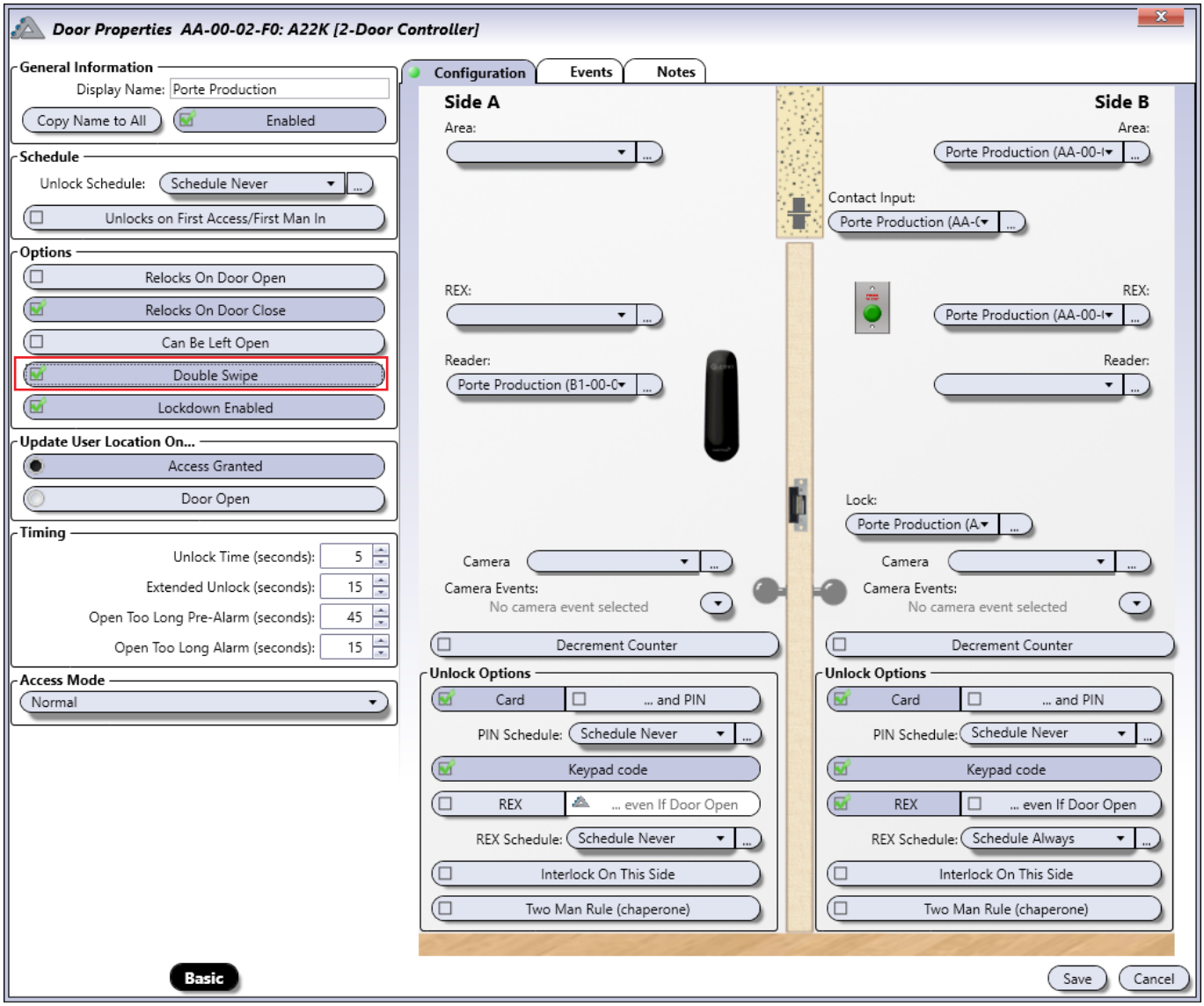
From the ***Hardware*** tab, click on the ***System Overview*** icon.
Select the Master controller from the list and click on the ***Properties*** button.

From the ***Module Properties*** window, expand the ***Advanced Options*** tab.
Select the ***Integration*** tab and check/enable ***Intrusion (Alarm) Integration***. Click the ***Save*** button



You can arm an alarm system by double-swiping the card to the reader. You must enable the "Double Swipe" option for each door to which you want to apply this option.

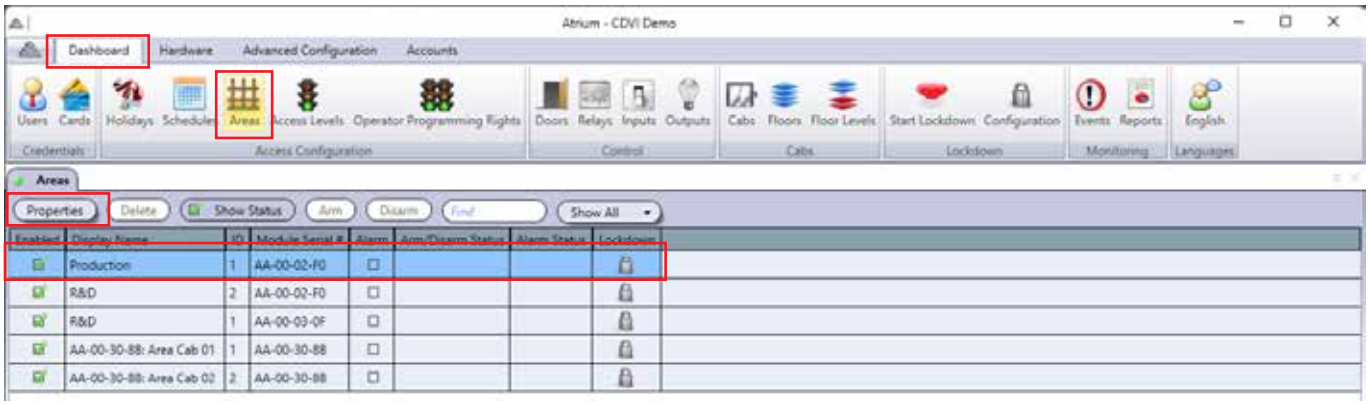
From the ***Door Properties*** window (display basic view by default), click the ***Advanced*** button.
Check/enable ***Double Swipe*** then click the ***Save*** button. Repeat for each door you want to activate "Double Swipe" arming.



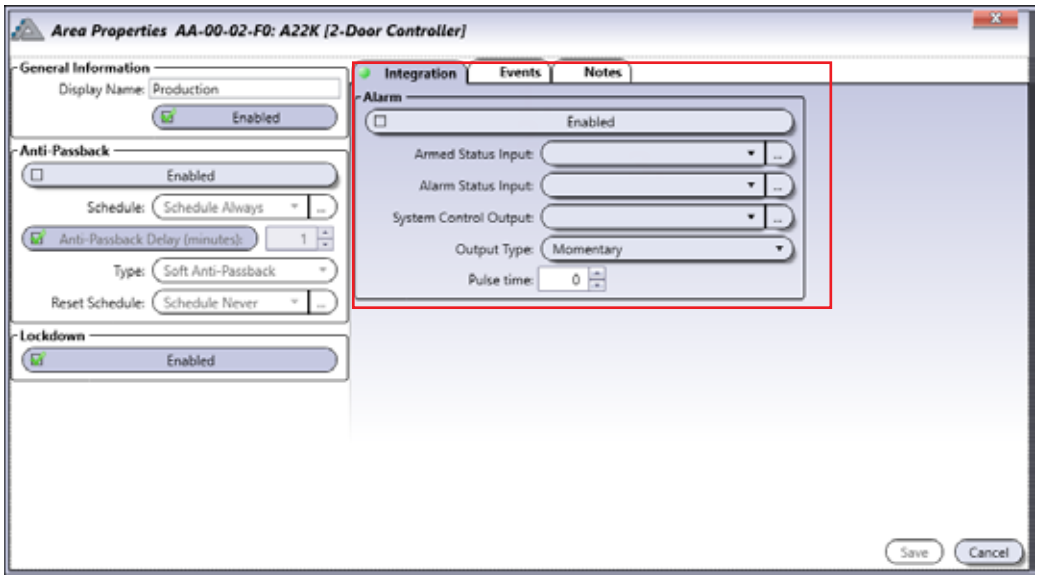
SETTING AREA

Any readers associated to an area, can be used to arm and disarm the intrusion alarm system.

From the ***Dashboard*** tab, click on the ***Areas*** icon.
Select an area from the list and click on the ***Properties*** button.



From ***Area Properties*** window. Select ***Integration*** tab



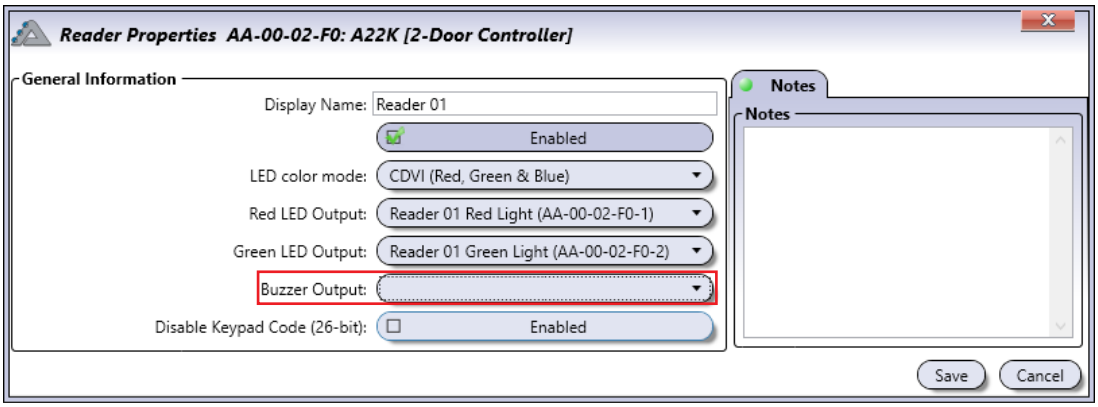
Integration

- **Enabled:** Check Active to activate this area to arm and disarm the intrusion (alarm) system.
- **Armed Status Input:** Select an ATRIUM input that will monitor the "armed" or "disarmed" status of the intrusion (alarm) system. ATRIUM will send an arming request to the intrusion (alarm) system only if the Arm Status Input state is in "disarmed" condition. The intrusion (alarm) system must be configured to activate a programmable (pgm) output when it is armed. Connect an external dry contact relay to the programmable (pgm) output and the selected ATRIUM input. Refer to page 125 to view the connections.

Integration (continued)

- **Alarm Status Input:** Select an ATRIUM input that will monitor the alarm status of the intrusion (alarm) system. The intrusion (alarm) system must be configured to activate a programmable (pgm) output when it detects an alarm condition. Connect an external dry contact relay to the programmable (pgm) output and the selected ATRIUM input. RRefer to page 125 to view the connections.

- **System Control Output:** Options include either the dry contact relays (RLY1/RLY2 on the controller) or any of the reader outputs.
    - If a reader output is selected, you must de-activate (leave the output field blank) its default settings in the Reader Properties menu. See page 91 to view the reader output configuration settings.



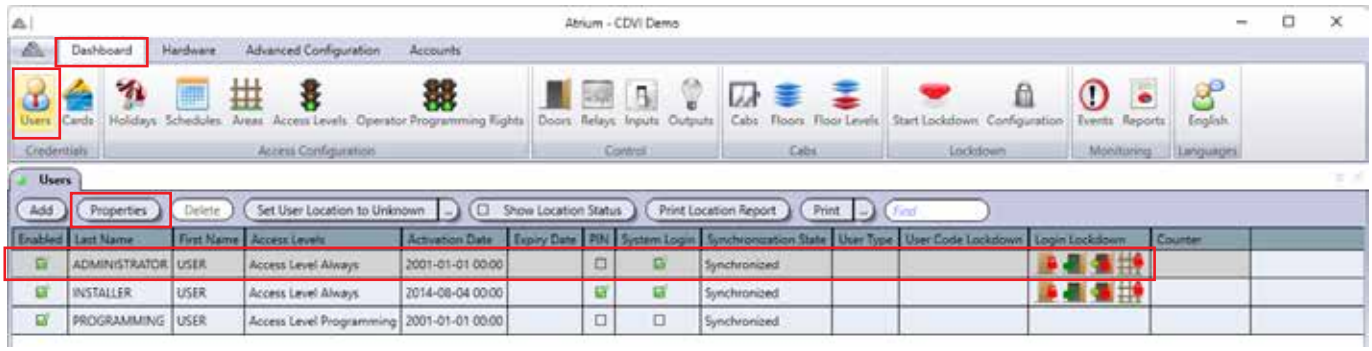
    - An external 12V relay must be connected to the selected reader output terminal. The external relay is then connected to the key switch arming input.

- **Output Type:** Maintained or Momentary
    - Maintained:
        - o The output will activate and remain activated when a valid double-swipe is detected.
        - o The output will de-activate when a valid swipe is detected.
    - Momentary:
        - o The output will activate for the amount of time defined in the Pulse Delay field and de-activate when the time expires.

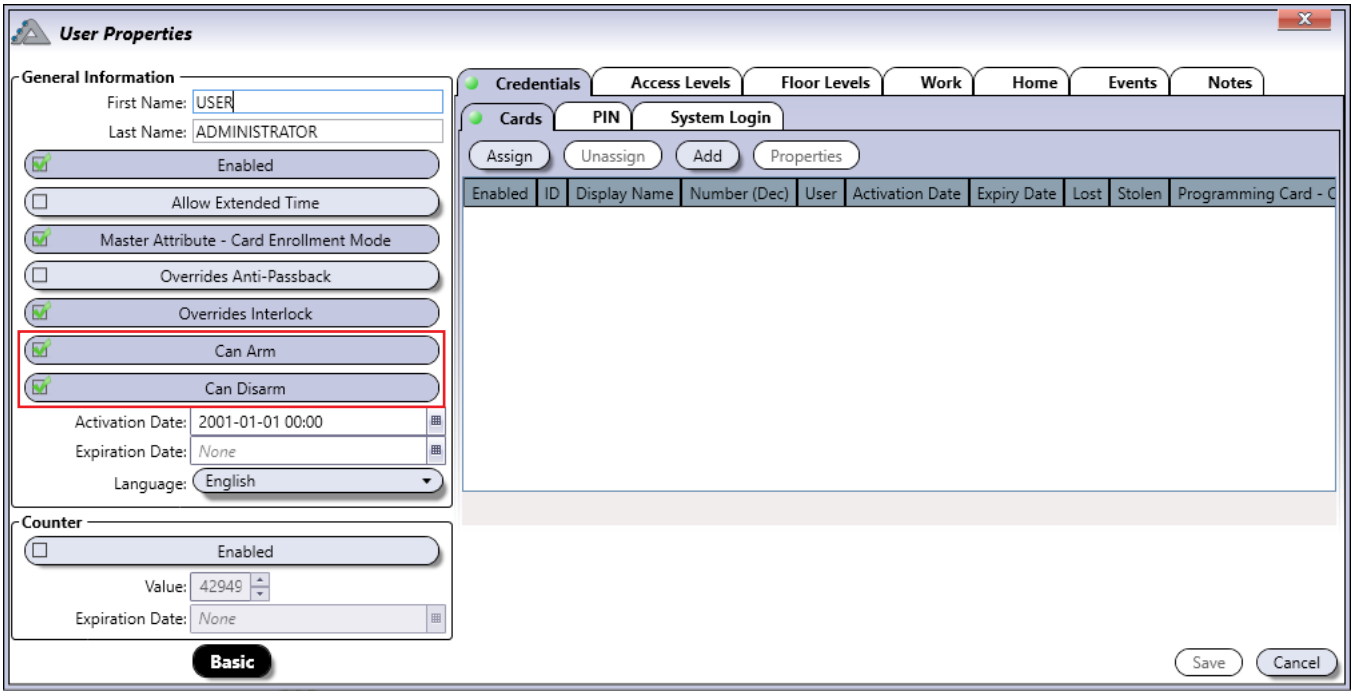
- **Pulse Time:** Amount of time, in seconds, the selected control output will activate.

ENABLING A USER TO ARM/DISARM.

From the ***Dashboard*** tab, click on the ***Users*** icon.
Select a user from the list and click on the ***Properties*** button.



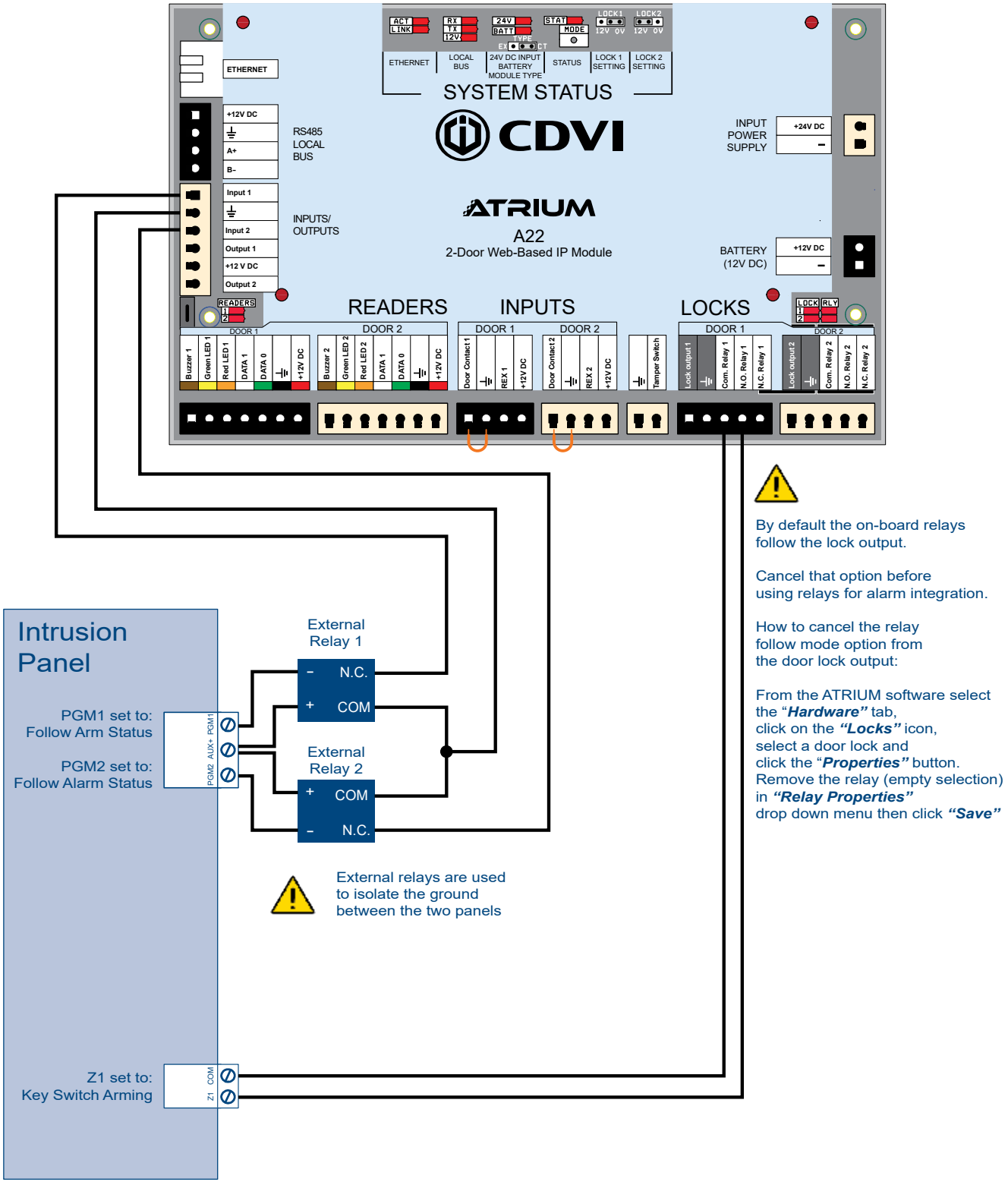
From ***User Properties*** window, select Advanced View.



Check ***Can Arm*** to activate the selected user to arm the intrusion alarm system

Check ***Can Disarm*** to activate the selected user to disarm the intrusion alarm system. Save your modifications.

WIRING DIAGRAM



ELEVATOR INTEGRATION

ATRIUM's elevator control integration allows you to manage up to 256 floors per account. The 256 floors can be divided in different ways. For instance; 1 building of 256 floors, 4 buildings of 64 floors or 8 buildings of 32 floors each. It could also be 1 building with 8 elevator cabs of 32 floors each.

Let's take the example of 4 buildings of 64 floors, each floor should be named similar as following;

Building 1 - Floor 1	Building 1 - Floor 2	Building 1 - Floor 3	Building 1 - Floor 4
Building 2 - Floor 1	Building 2 - Floor 2	Building 2 - Floor 3	Building 2 - Floor 4
Building 3 - Floor 1	Building 3 - Floor 2	Building 3 - Floor 3	Building 3 - Floor 4
Building 4 - Floor 1	Building 4 - Floor 2	Building 4 - Floor 3	Building 4 - Floor 4

etc.

Once you have named each floor, the next step is to determine how many cabs would be used. Note that each A22K EC can manage two cabs and two card readers (one per cab). Each A22K EC controller manages 128 floors (64 floors per cab). So if you have to manage 8 cabs, you would need four (4) A22K EC controllers.

Once the number of floors and the number of cabs to be managed has been determined, the floor buttons for each cab needs to be configured. Each cab button should be associated with a CA-A480-A relay. Each the CA-A480-A manages 16 relays. So let's take the example of a 16-floor building with four (4) cabs, you will need two (2) A22K EC controllers with two cab readers(2) CA-A480-A connected to each A22K EC controller.

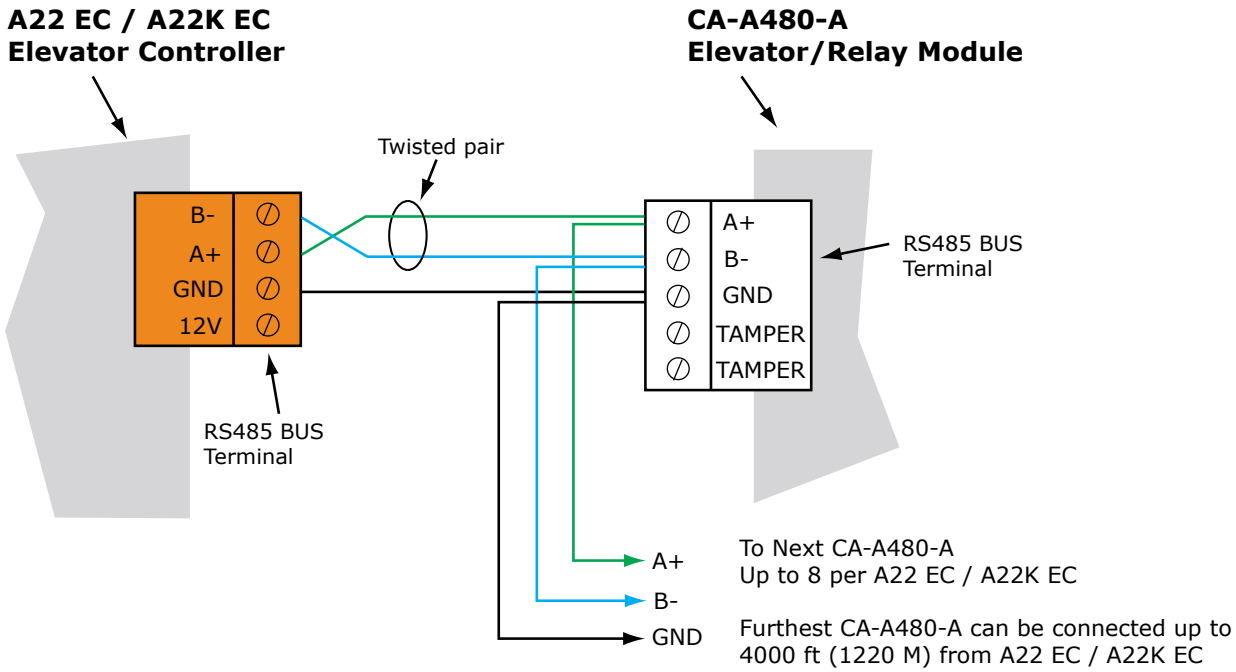
Follow the next steps to know how to connect and configure the ATRIUM system elevator management solution.

To convert an A22K to A22K EC, simply change the controller's operating mode. Follow the instructions in the A22K manual on how to change the operating mode.

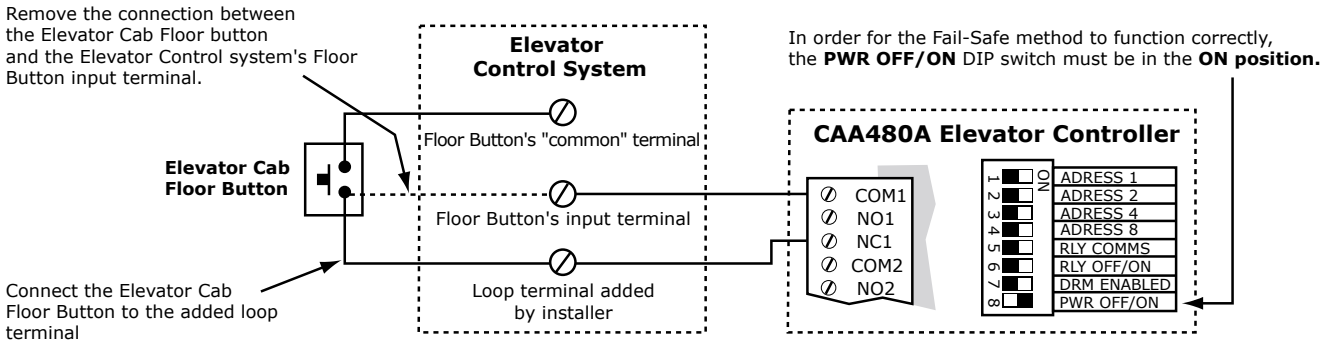
New elevator integration features require ATRIUM software version 7.0.1.268 or higher with A22K firmware version 3.00 or higher. A22 controller or older/legacy A22K firmware also support elevator control but do not support new added features.

CONNECTING AN A22 EC/A22K EC CONTROLLER TO A CA-A480-A ELEVATOR/RELAY MODULE

The "daisy chain" wiring from an A22 EC/A22K EC to a CA-A480-A, to the next CA-A480-A (if used) is shown below.

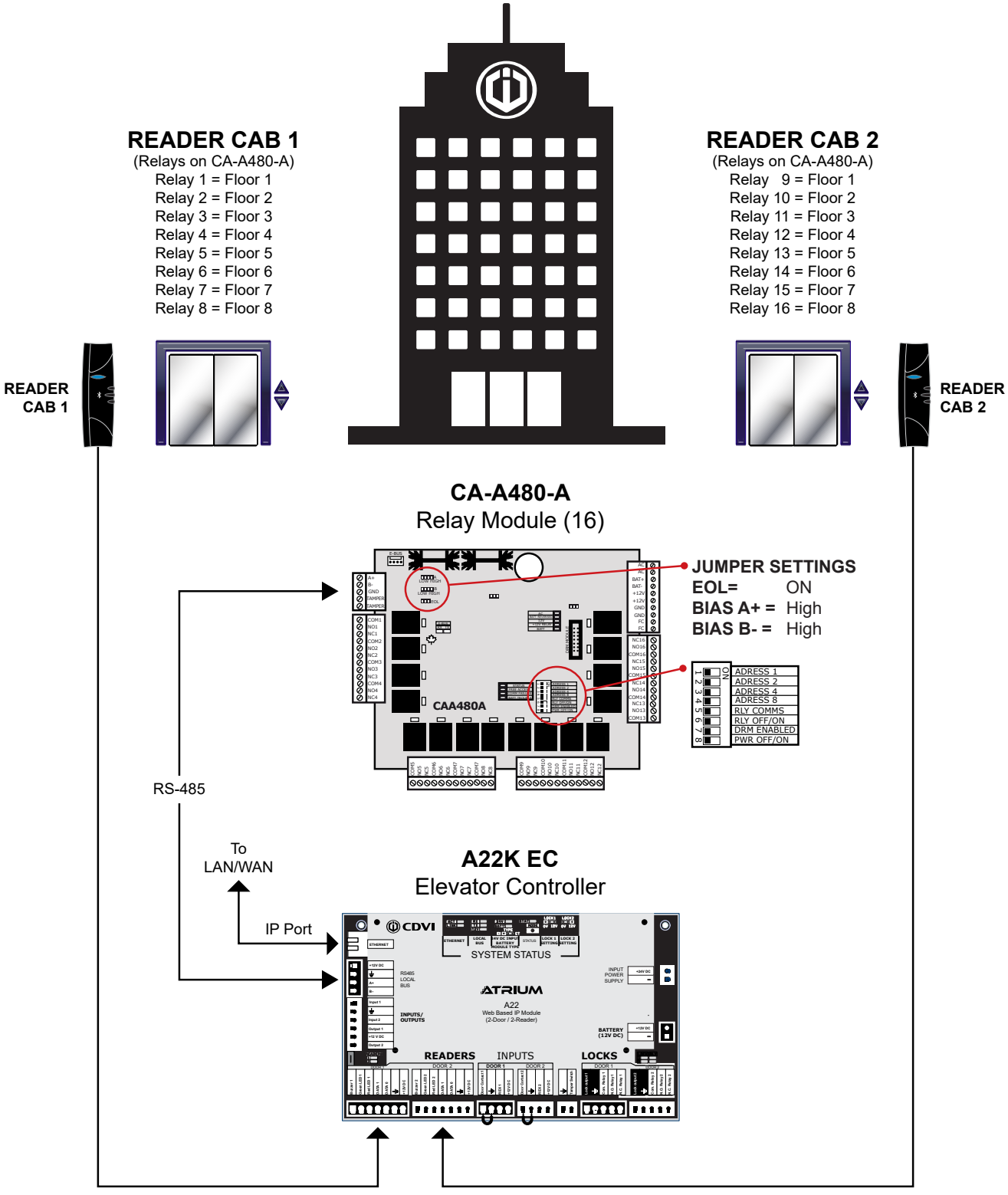


CONNECTING A CA-A480-A ELEVATOR/RELAY MODULE TO AN ELEVATOR SYSTEM

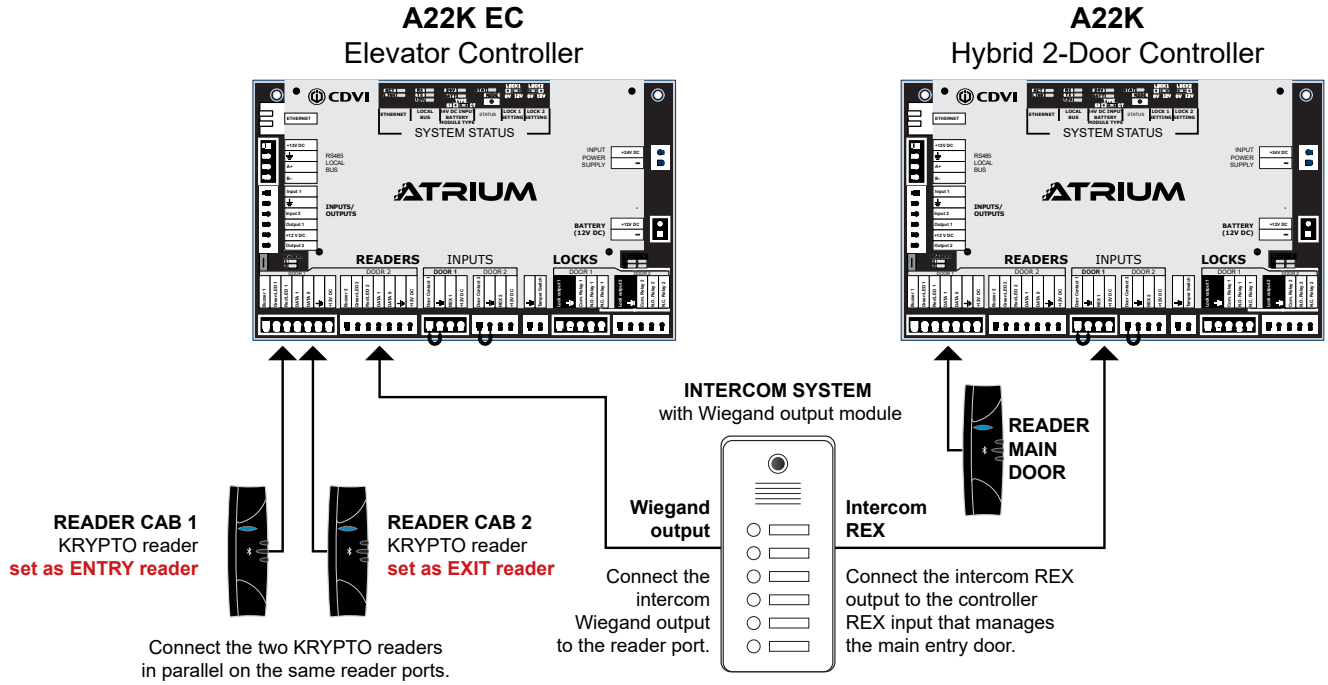


The diagrams on p.125 to 128 shows the connection of the A22-EC/A22K-EC to a CA-A480-A and the cab readers and floors that they manage. It also shows the jumper settings that can be used across all CA-A480-As, the dipswitch settings for floor addressing and the DRM connection diagram. For more information on specific settings, consult the CA-A480-A manual.

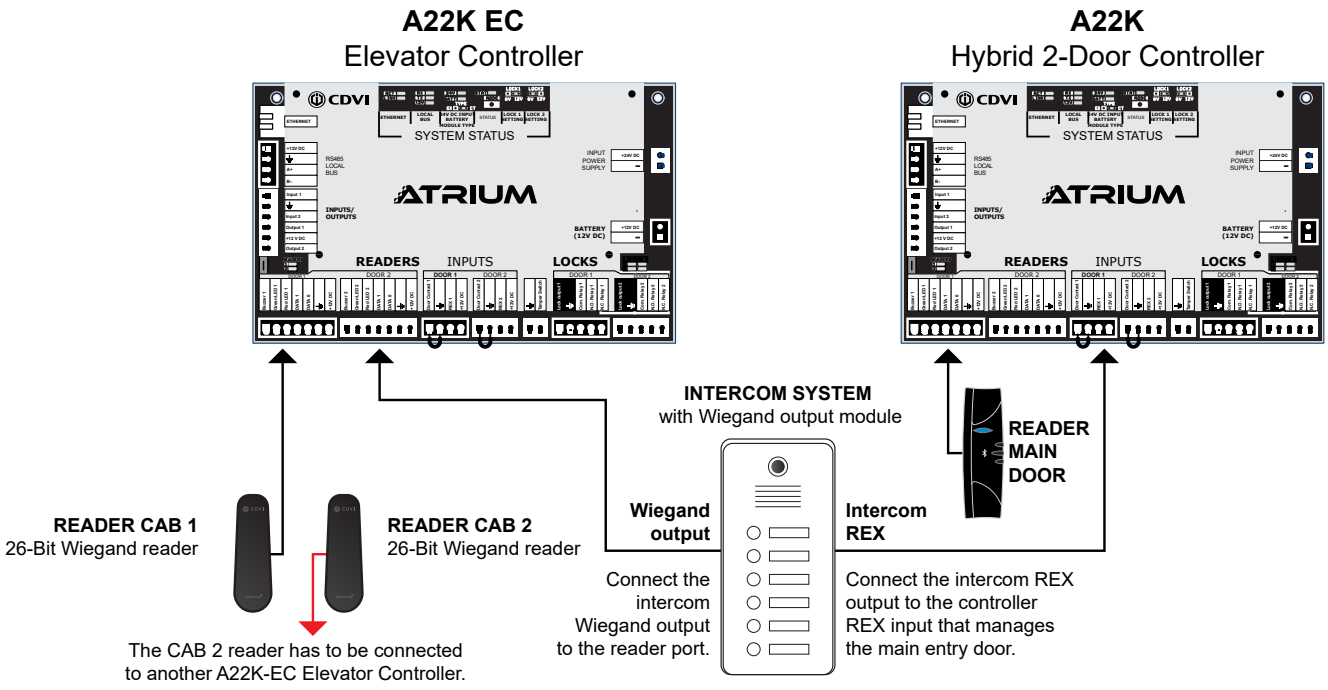
CONNECTING AN A22K-EC ELEVATOR CONTROLLER TO A BUILDING OF 8 FLOORS AND 2 CABINS.



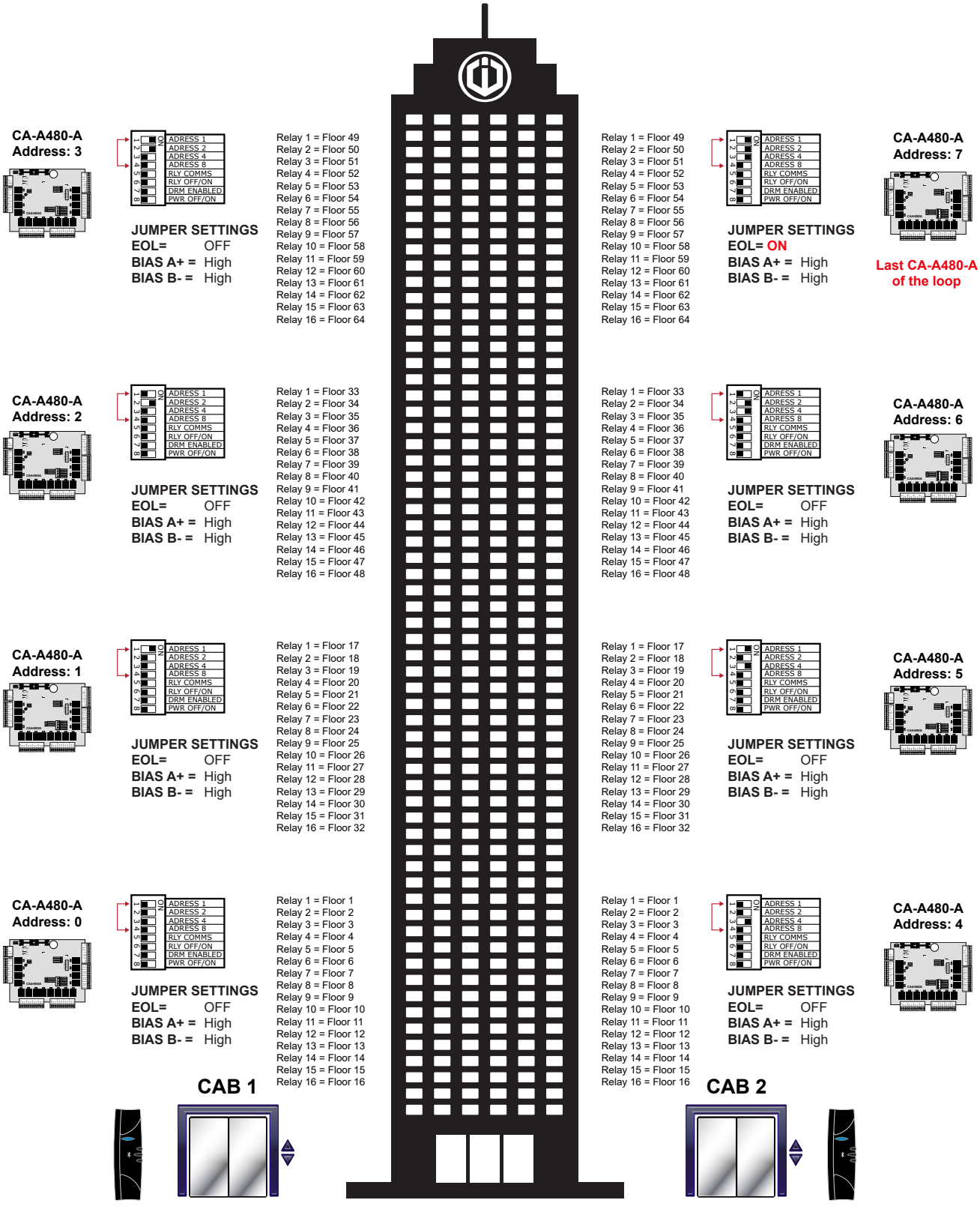
HOW TO CONNECT THE ATRIUM SYSTEM TO AN INTERCOM SYSTEM USING KRYPTO READERS



HOW TO CONNECT THE ATRIUM SYSTEM TO AN INTERCOM SYSTEM USING STANDARD WIEGAND READERS

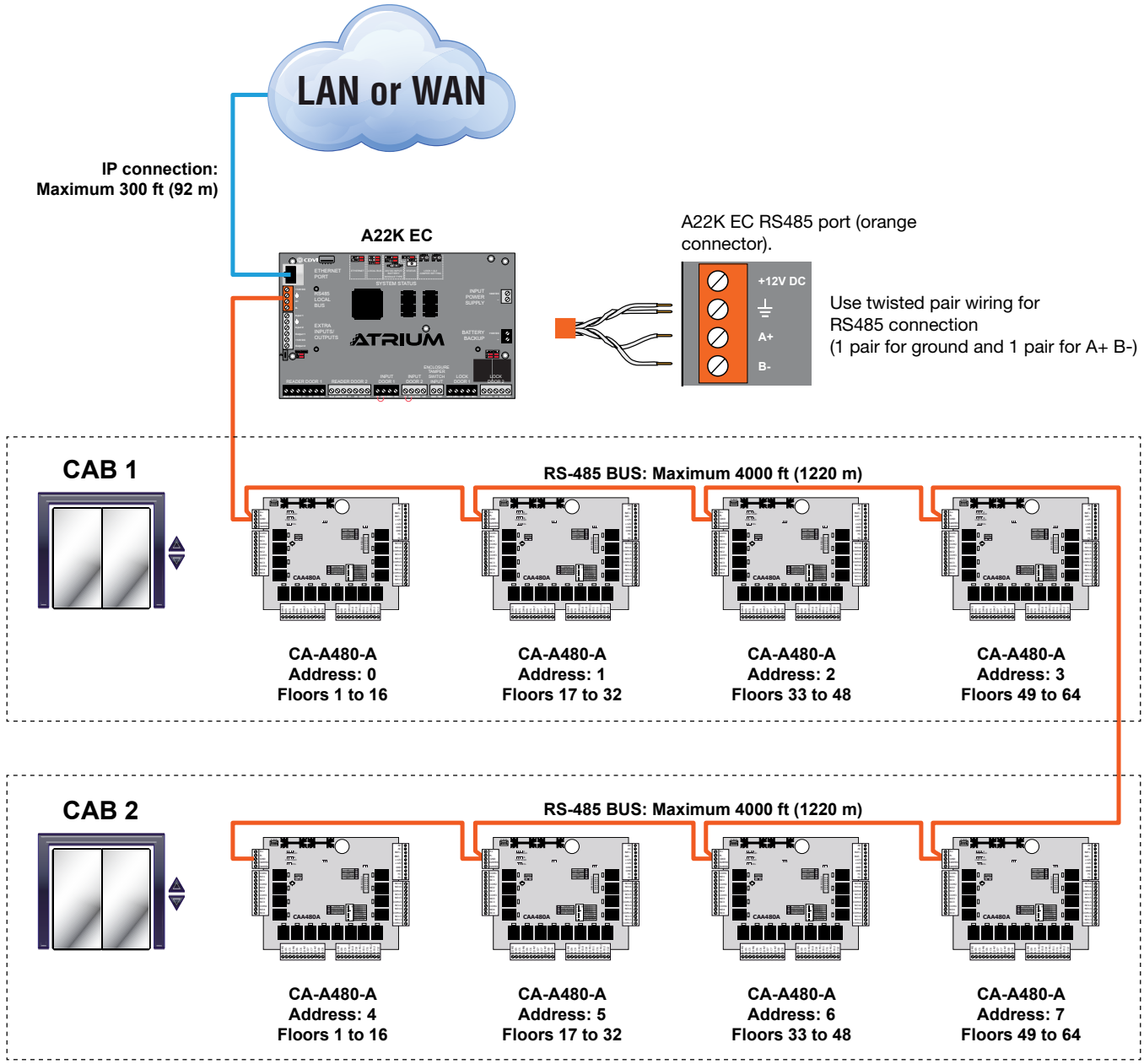


Example of a 64-floor building with 2 cabs (CA-A480-A DIP switch addressing)



RS485 WIRING DIAGRAM

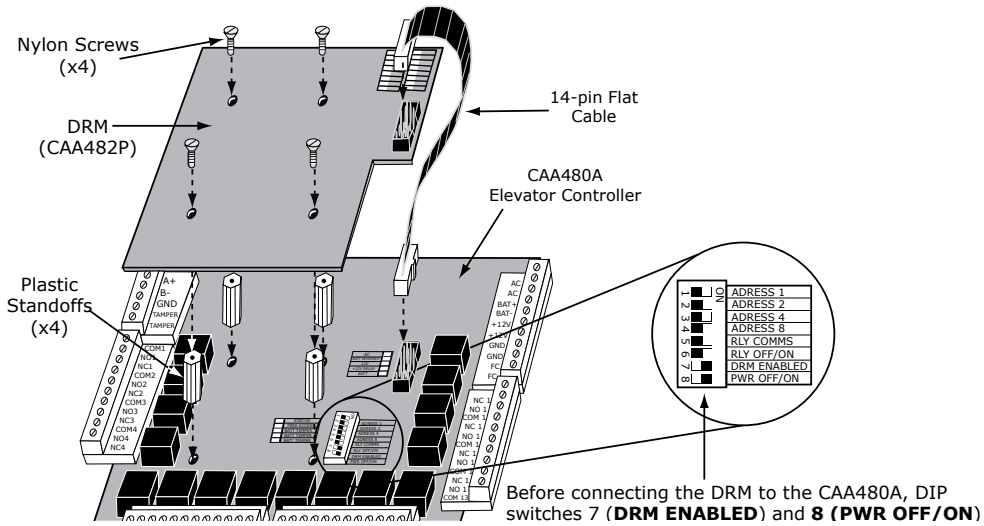
An K EC can manage 128 floors, 64 floors per cab. A maximum of 8 CA-A480-A elevator/relay modules can be connected to the RS-485 BUS of the A22K EC. The illustration below shows a configuration with 2 cabs of 64 floors each for a total of 128 floors per A22K EC. Add an A22K EC for additional floor management.



USING THE CA-A482-P DESTINATION REPORTING MODULE (DRM)

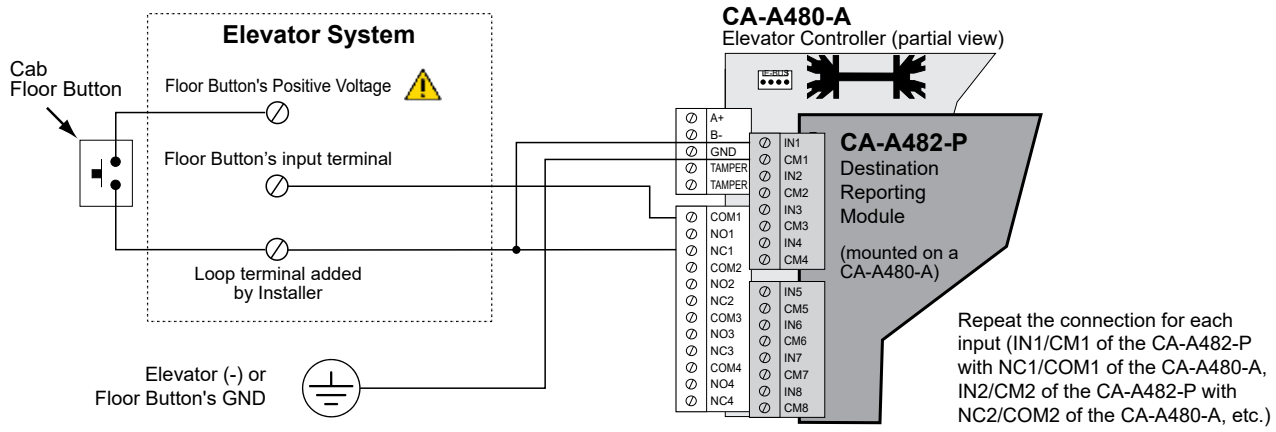
The CA-A482-P Destination Reporting Module adds the ability to:

- Floor selection confirmation. Depending on your floor level, an access gives you permission to select one floor among several.
- Toggle floor commands on double swipe of a card.
- Use the "Unlock on First Access" for floor public access option (Floor Properties).
- Provide extra floor unlock time for visitors (intercom).



WIRING DIAGRAM

(CA-A480-A elevator controller and CA-A482-P Destination Reporting Module)

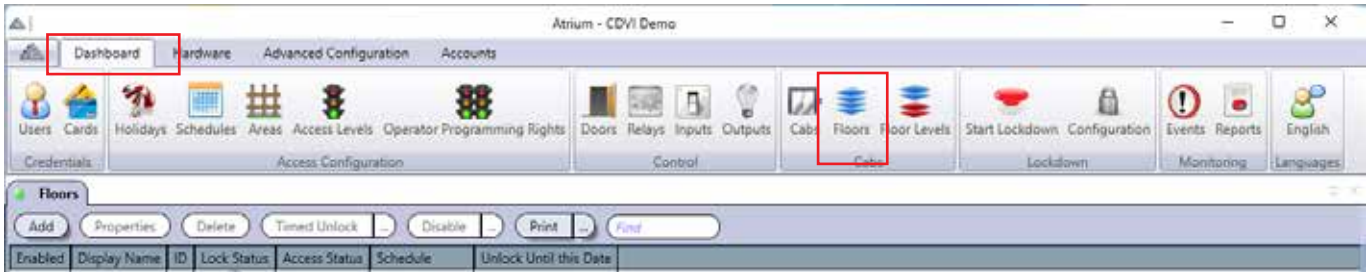


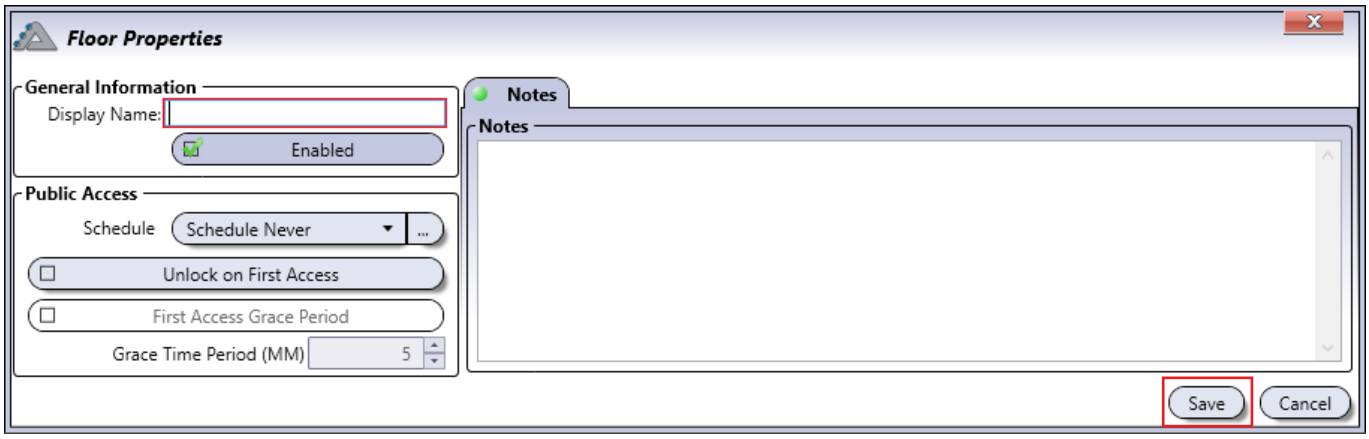
The elevator control system may provide a positive or negative button control voltage.
The appropriate floor selection input will need to be wired to reflect this.
The above diagram shows it wired for a positive button control input.

FLOORS

Floors can be located within the same building or distributed between different buildings. The total number of ***Floors*** in the account will be listed from 1 to a maximim of 256. If any ***Floors*** are located in other buildings, you can rename the ***Floors*** to identify/find them easier (ex. Building A - Floor 1, Building B - Floor 1, etc.).

From the ***Dashboard*** tab, click on ***Floors***, then ***Add*** to open the **Floor Properties** menu and add a new floor.





General Information

- **Display Name:** Enter a display name for the floor.
- **Enabled:** Enable (checked) or Disable (unchecked) the Floor.

Public Access

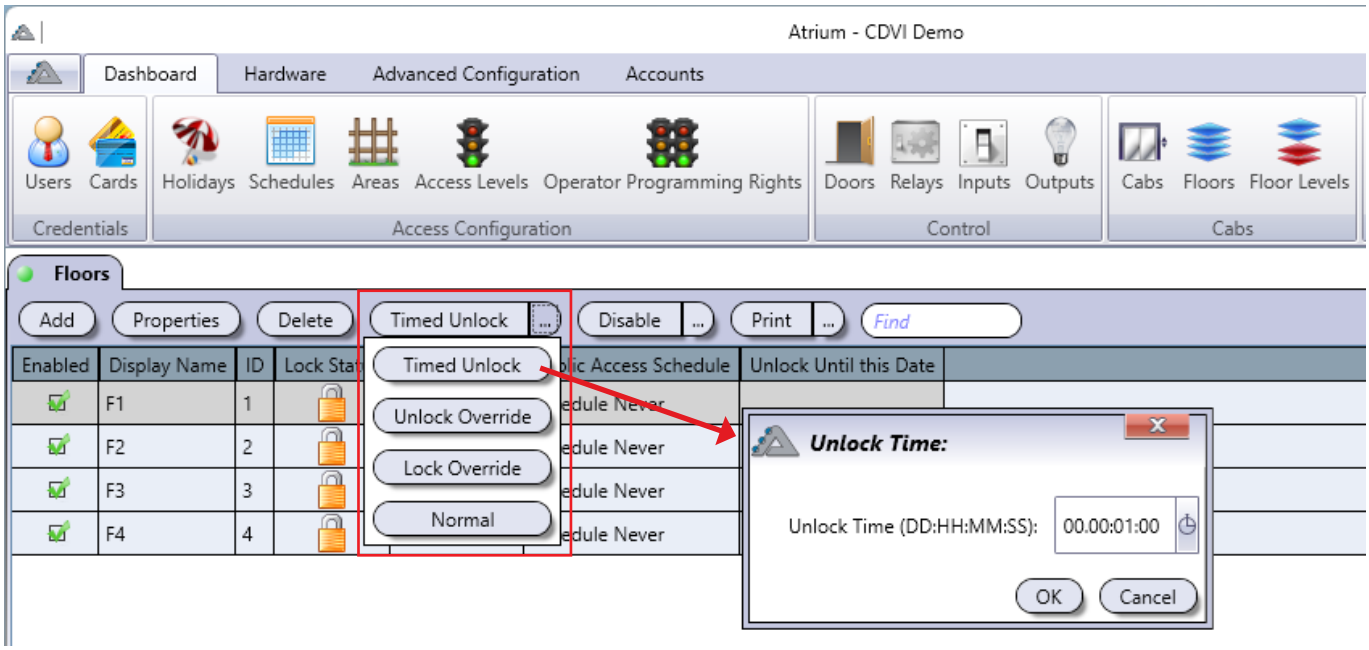
- **Schedule:** Select a schedule to specify when users will have free access.
- **Unlock on First Access:** The public access schedule will not begin until an access granted is generated after the start of the chosen schedule.
- **First Access Grace Period:** This option is enable only if "Unlock on first Access" is checked/enable. It will allow the schedule to open at starting time if a valid access have been done during the period determined before the beginning of the schedule.
- **Grace Time Period (MM):** Enter grace time period in minutes, two digits.
- **Notes (tab):** Click anywhere inside the box to add notes.

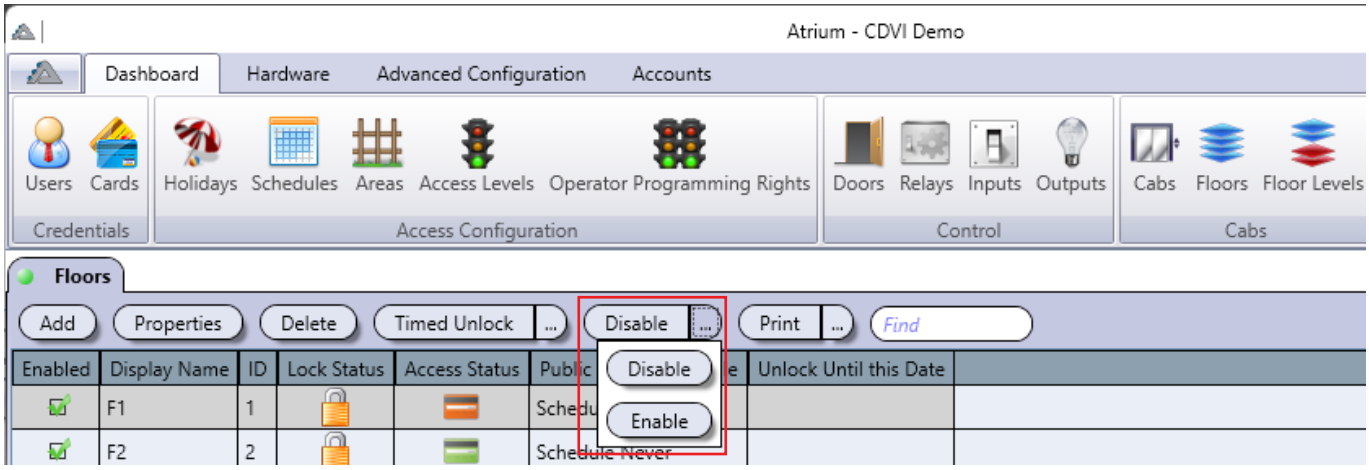
Click ***Save*** to keep any changes.

FLOOR COMMANDS

There are commands you can apply to one or more floor selections at once. You will be able to:

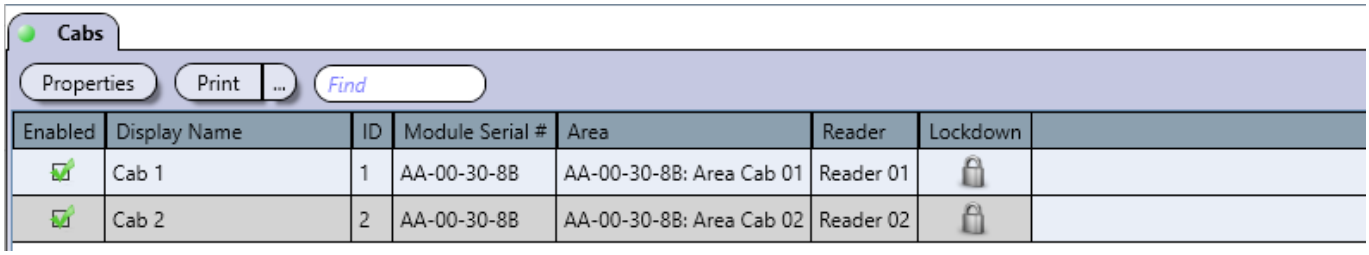
- **Timed Unlock:** The command will unlock the selected floor(s) manually without passing the card. It will unlock the cab buttons that have this floor programmed. A window will open to enter a time in day, hour, minute and second. This command will override any other pre-programmed command.
- **Unlock Override:** Select to unlock the selected floor(s) permanently. This command will override any other pre-programmed command. Click "Normal" command to put back the floor to its pre-programmed state.
- **Lock Override:** Select to lock the selected floor(s) permanently. This command will override any other pre-programmed command. Click "Normal" command to put back the floor to its pre-programmed state.
- **Normal:** Select to return the selected floor(s) to the normal pre-programmed system state.
- **Disable:** Select the "Disable" command to manually revokes the access for the selected floor(s) but will not disable pre-programmed public access.
- **Enable:** Select the "Enable" command to manually restore access to the selected floor(s).

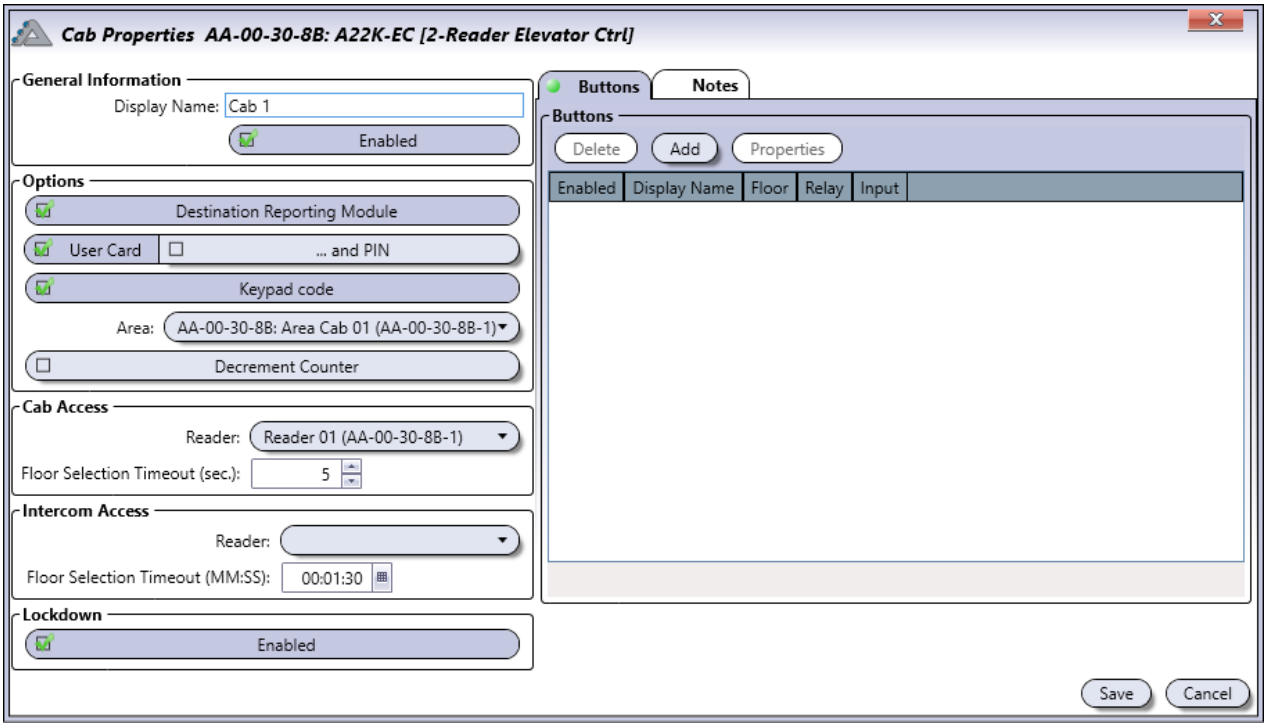




CABS

From the ***Dashboard*** tab, click on ***Cabs***, then select a cab and click on ***Properties*** to open the **Cab Properties** menu. Each A22K EC adds two elevator cabs.





General Information

- **Display Name:** Enter a display name for the floor cab.
- **Enable:** Enable (checked) or Disable (unchecked) the Cab.

Options

- **Destination Reporting Module:** Enable (checked) or Disable (unchecked) the optional CA-A482-P Destination Reporting Module (DRM).
- **Card, PIN and Keypad Code:** If **Card** or **Keypad Code** are checked off, the **User** can have access granted using either option. If **...and PIN** is selected, the **User** will need to present a card and put in a PIN (also known as a keypad code).
- **Area:** Set the Area associated to the cab.
- **Decrement Counter:** When selected, the door will count down the uses of a card or PIN.

Cab Access

- **Reader:** Select a card reader for cab floor selection.
- **Floor Selection Timeout (sec.):** Enter the time required for floor selection.

Intercom Access

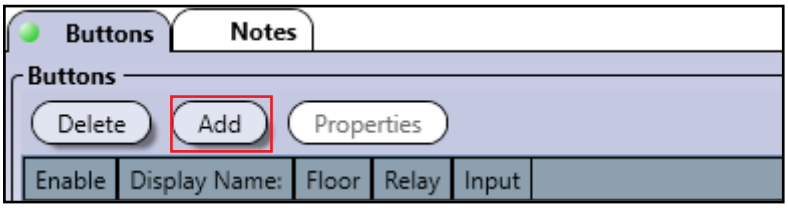
- **Reader:** Select a card reader for intercom floor selection.
- **Floor Selection Timeout (MM:SS):** Enter the time required for floor selection.

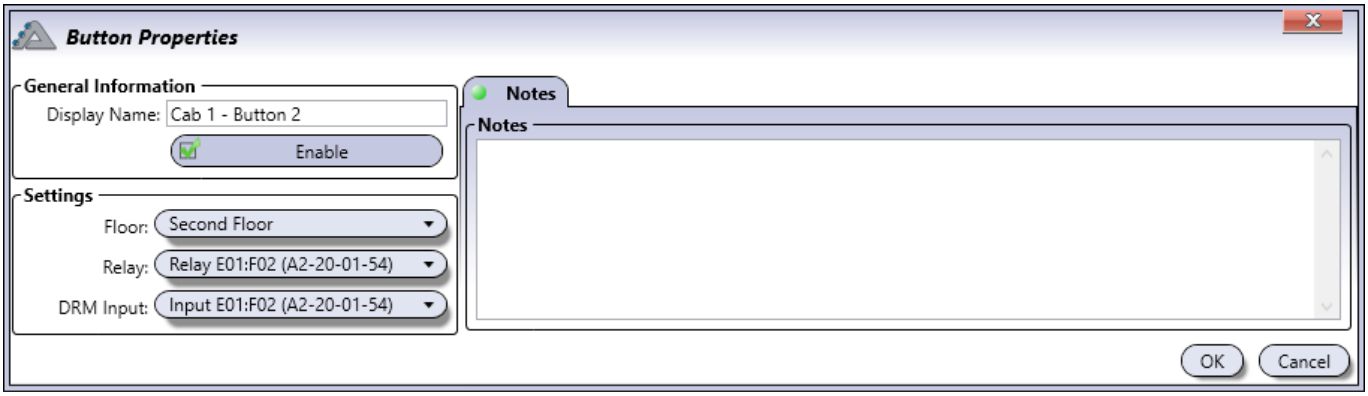
Lockdown

- E**nabled:** When selected, the lockdown feature will be enabled for the floor.

Buttons Tab

Click on the ***Buttons*** tab then Add to enter the **Button Properties** menu.





General Information

- **Display Name:** Enter a display name for the floor cab button.
- **Enable:** Enable (checked) or Disable (unchecked) the button.

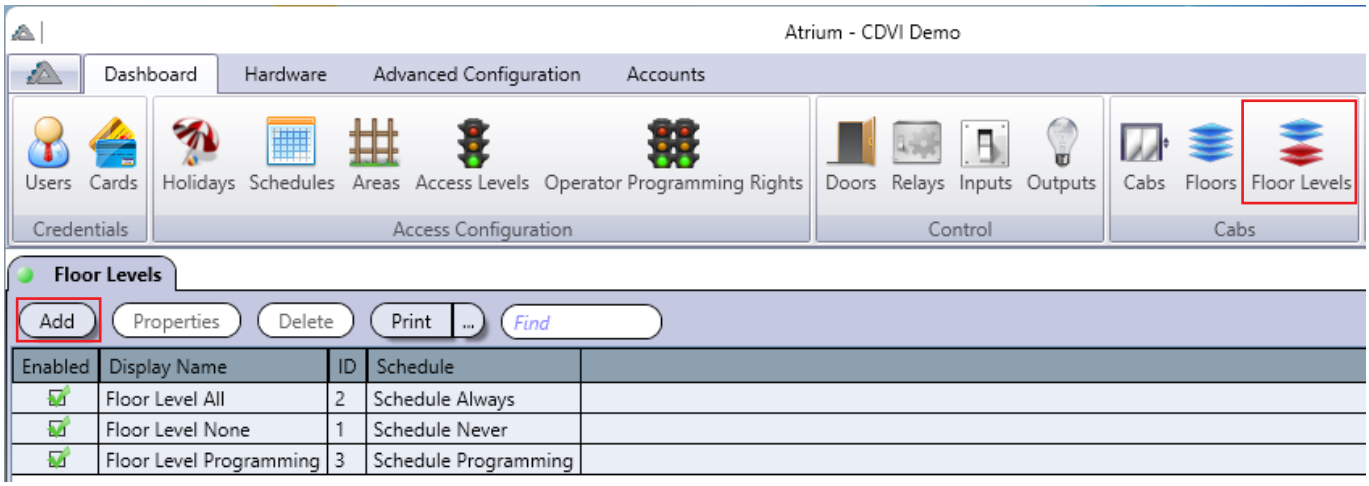
Settings

- **Floor:** Select the floor the button will call.
- **Relay:** Select on which CA-A480-A relay the cab button is connected.
- **DRM Input:** Select which DRM input the cab button is connected.

The Relay and DRM input names will match up if they are wired in order. (Ex. Relay E01:F01 will correspond with DRM Input E01:F01.)

FLOOR LEVELS

Floor Levels function like Access Levels (page 40) except that they apply to an entire floor instead of applying to an Area. From the ***Dashboard*** tab, click on ***Floor Levels*** to view them.

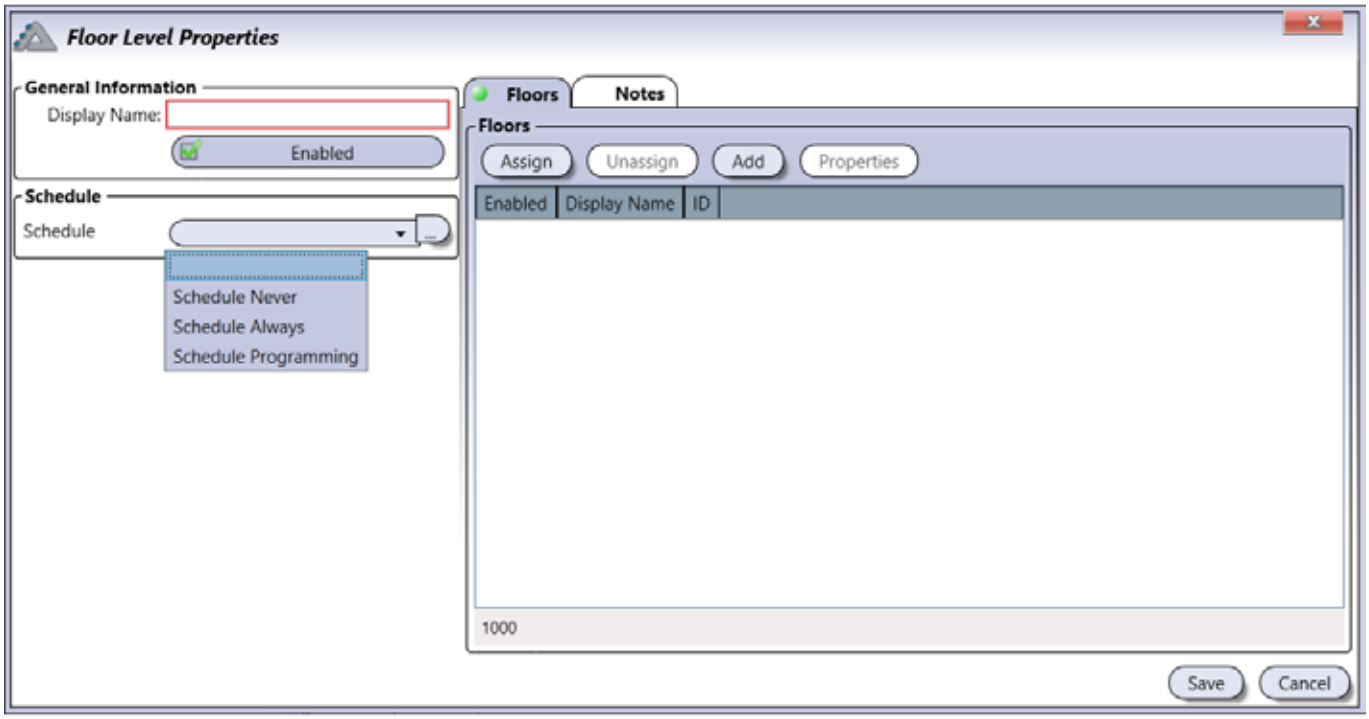


There are three default Floor Levels:

- **Floor Level None:** This floor level has Schedule Never, so there is no access to any floors assigned to it.
- **Floor Level All:** This floor level has Schedule Always, so there is access to every floor assigned to it 24 hours a day, 365 days per year including any programmed Holidays.
- **Floor Level Programming:** This floor level has the Learning Mode schedule, so there is access to every floor assigned to it 24 hours a day, 365 days per year including any programmed Holidays.

Click on ***Add*** to enter the **Floor Level Properties** menu.

Floor levels are similar to "Access Levels". When the selected schedule is valid, users assigned with the floor level will have access to the floors assigned to the floor level.



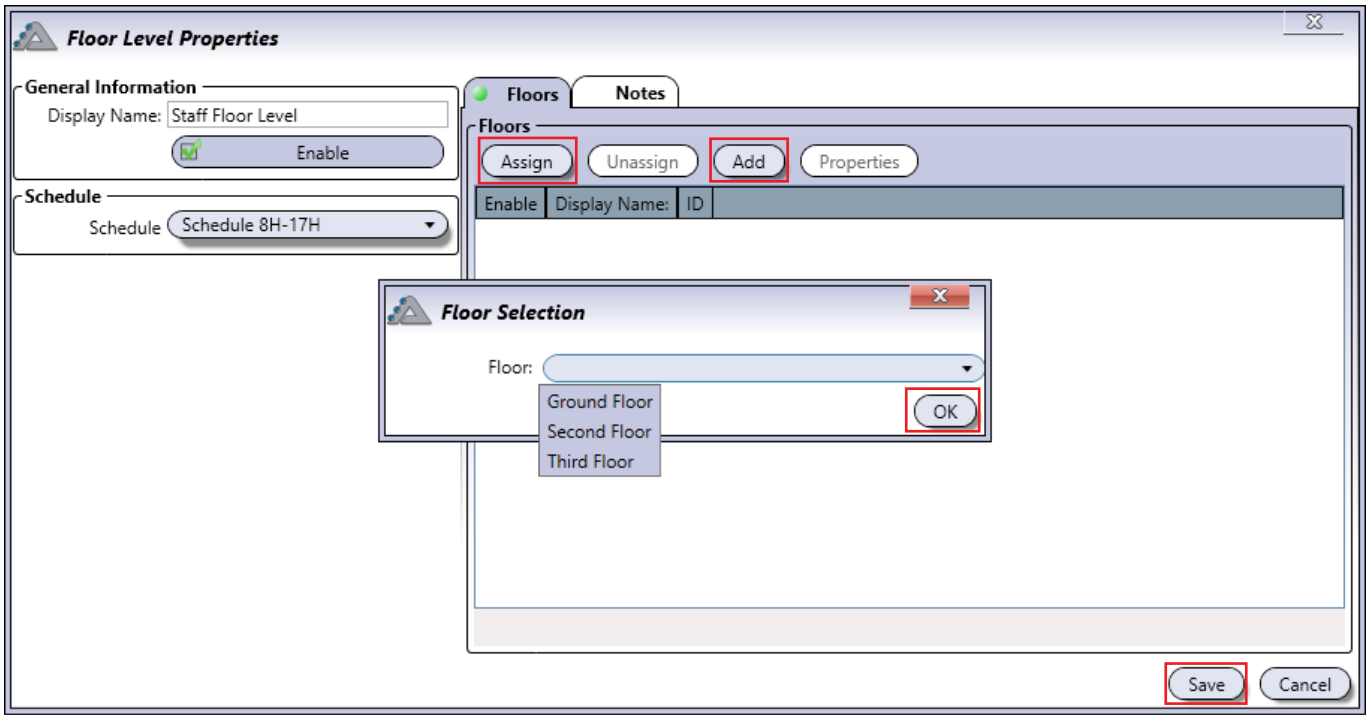
General Information

- **Display Name:** Enter a display name for the floor level.
- **Enable:** Enable (checked) or Disable (unchecked) the floor level.

Schedule

- **Schedule:** Select the schedule when users will have access to the assigned floors of the floor level.

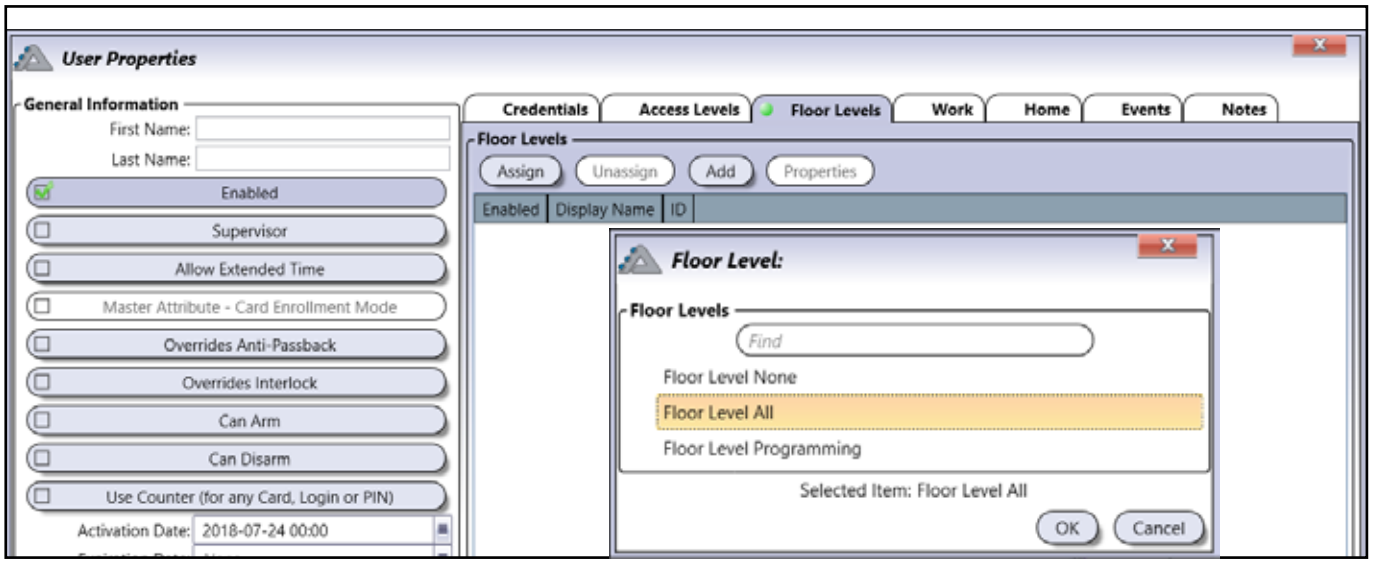
"Assign" existing floors or ***"Add"*** new floors to this floor level. The selected floors will give access to users according to the selected schedule in the floor level. Click OK after each selection.



Notes (tab)**:** Click anywhere inside the box to add notes.

Click ***Save*** to keep your changes.

You can "***Assign"*** or "***Add"*** Floor Levels to a User from the **User Properties** menu.



LOCKDOWN

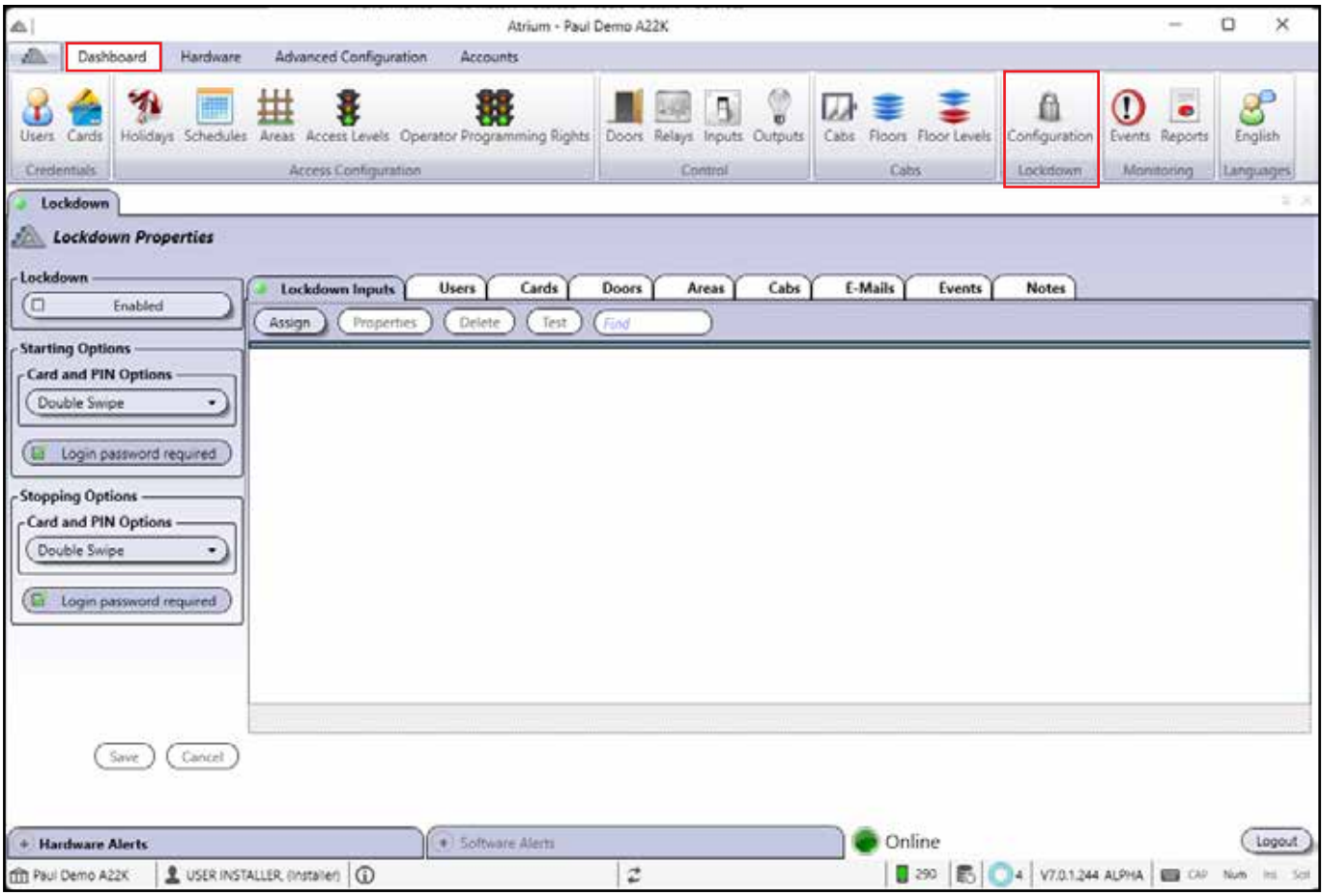
Lockdown parameters are put in place to secure a building against an active threat by instantly locking all doors. Any new access to these doors is prevented (or limited) until lockdown is ended. Configuring lockdown options allows you to use a card, input (such as one used by a pushbutton), or login to Atrium to start and end lockdown.

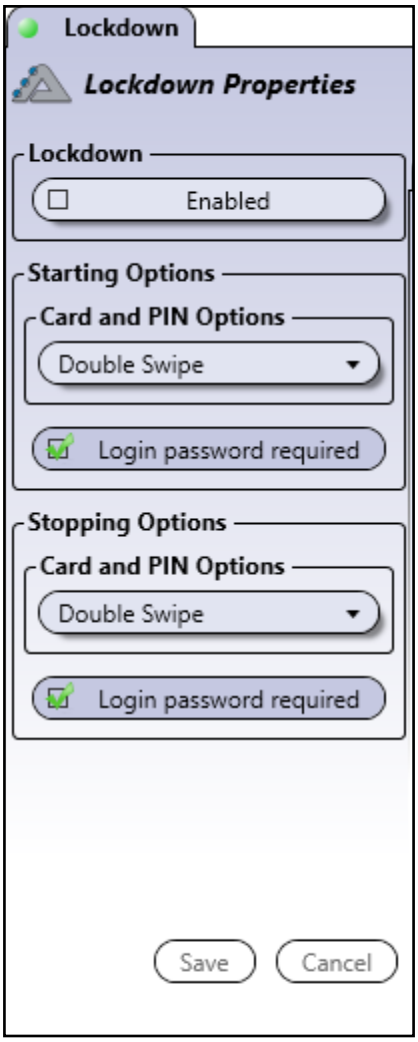
CDVI strongly recommends periodic and complete testing of the lockdown functionality. Tests should also be performed when:

- System hardware (controllers, expanders and/or add-on modules, field wiring, etc.) are added, modified (ex: firmware upgrade) or replaced.
- Modifications, systematic maintenance, upgrades or any other changes are made to the LAN/WAN used for communicating with an ATRIUM door controller.

LOCKDOWN PROPERTIES

The **Lockdown Properties** window contains all the fields used to configure lockdown. To display it, click on the ***Dashboard*** tab, then on ***Configuration*** in the **Lockdown** tab.

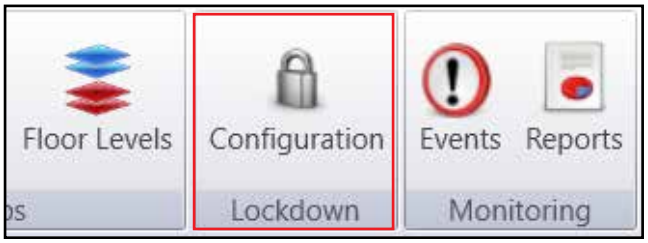




Lockdown: Lockdown is enabled by default. To disable it from being used, uncheck the box.

Starting Options: Select how Lockdown is started.

- **Card and PIN Options:** Select whether a single card swipe, double swipe or Two Man Rule (two different cards used one after the other) can start lockdown.
- **Login password required:** If this option is checked off, a user login password is required to start lockdown after clicking the ***Lockdown*** button. If unchecked, Lockdown can be started by clicking the Lockdown button and "OK" on the popup.



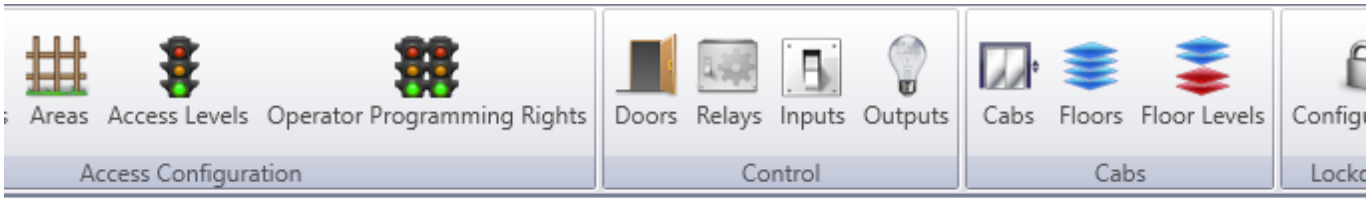
Stopping Options: Select how Lockdown is stopped.

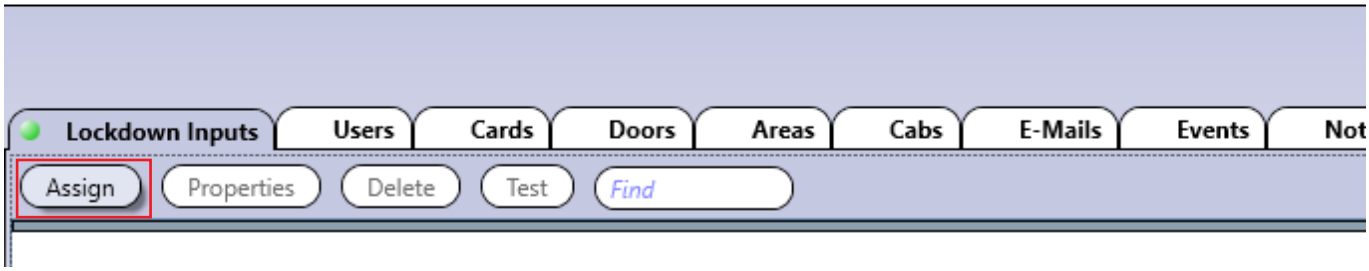
- **Card and PIN Options:** Select whether a single card swipe, double swipe or Two Man Rule (two different cards used one after the other) can stop lockdown.
- **Login password required:** If this option is checked off, a user login password is required to stop lockdown after clicking the ***Lockdown*** button. If unchecked, Lockdown can be stopped by clicking the Lockdown button and "OK" on the popup.

Click ***Save*** to keep your changes.

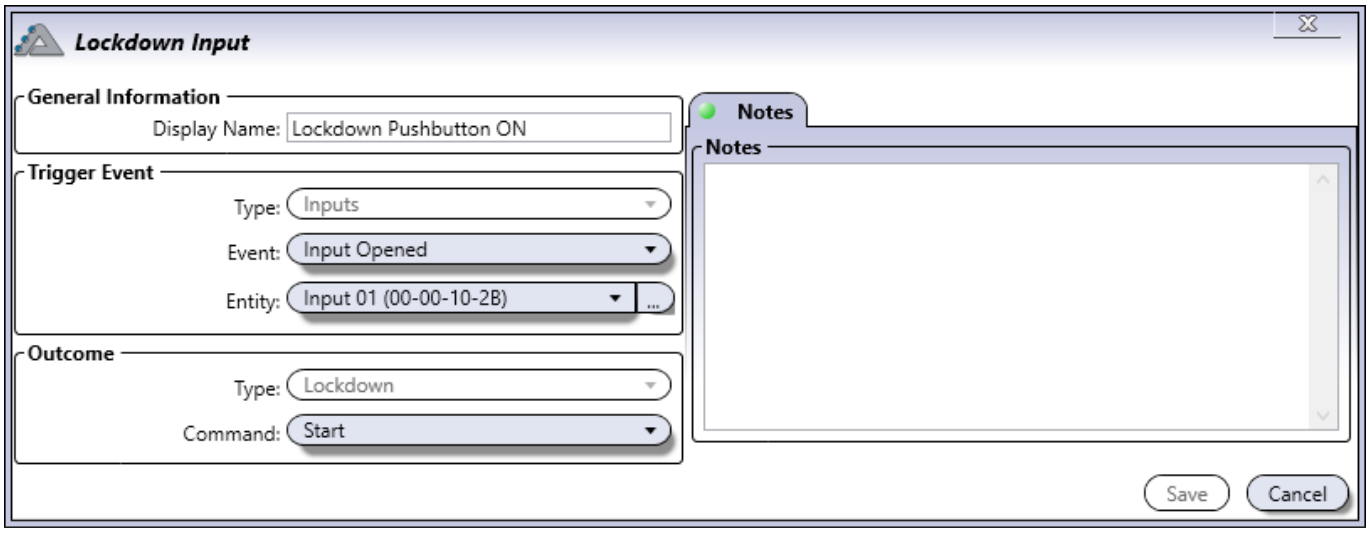
LOCKDOWN INPUTS

Lockdown Inputs are used to assign specific inputs on the Atrium panel to start and stop lockdown. Click on the ***Assign*** tab to open the **Lockdown Input** window or ***Properties*** to modify assigned inputs**.**





The **Lockdown Input** window shows available inputs for starting or stopping lockdown. The example below show an input being used to start lockdown**.**



General Information

- **Display Name:** The display name for this lockdown input can be modified here.

Trigger Event

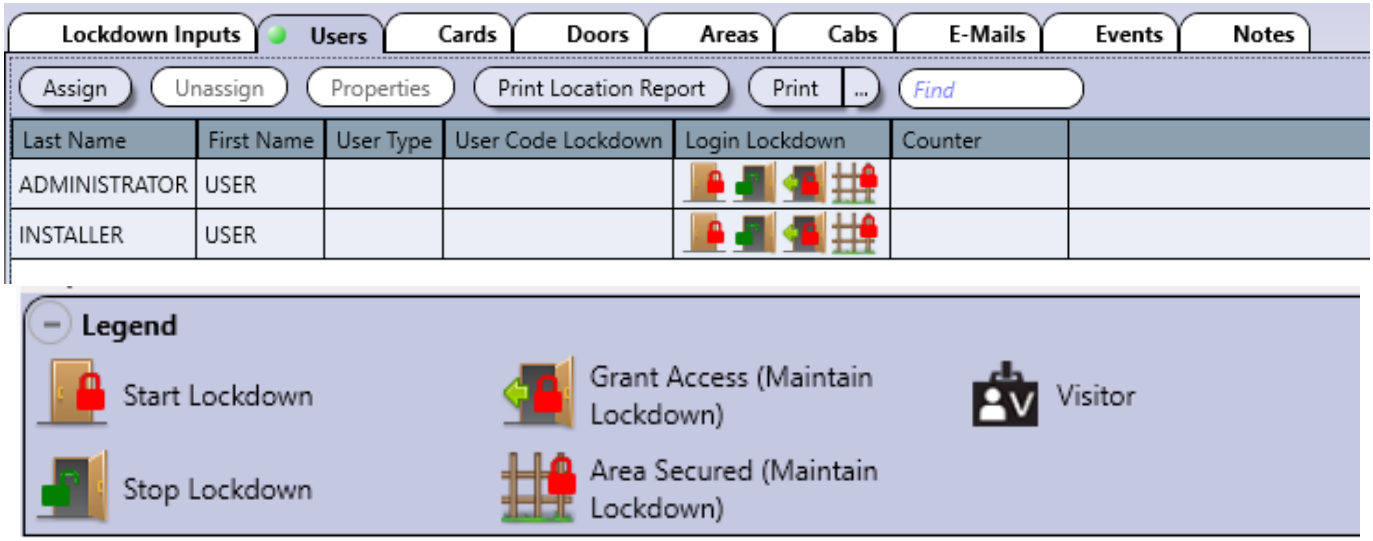
- **Type:** This option is locked to inputs only.
- **Event:** Select what condition triggers the command.
- **Entity:** Select the input being used.

Outcome

- **Type:** This option is locked to lockdown only.
- **Command:** Select what happens when the **Event** is triggered.

USERS

The **Users** tab is used to manage which users can start and stop lockdown, grant access during a lockdown, and confirm which areas have been secured, using a system login or PIN.



Assign: Select a User and give them Lockdown rights.

Unassign: Select a User and remove their Lockdown rights.

Properties: Edit an existing User's properties.

Find: Type in several letters or a full name to filter and find a specific User**.**

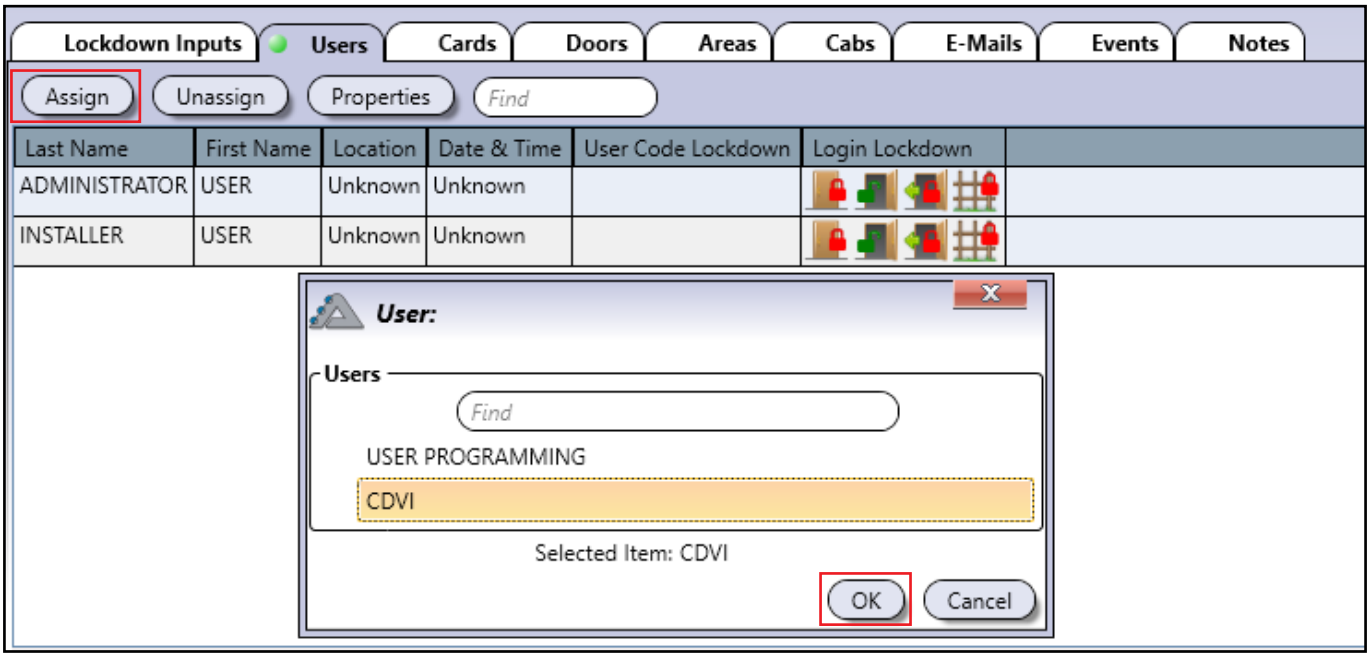
Print Location Report: Generate and print user's location report.

Print: it an eGenerate and print summary or detailed user report.

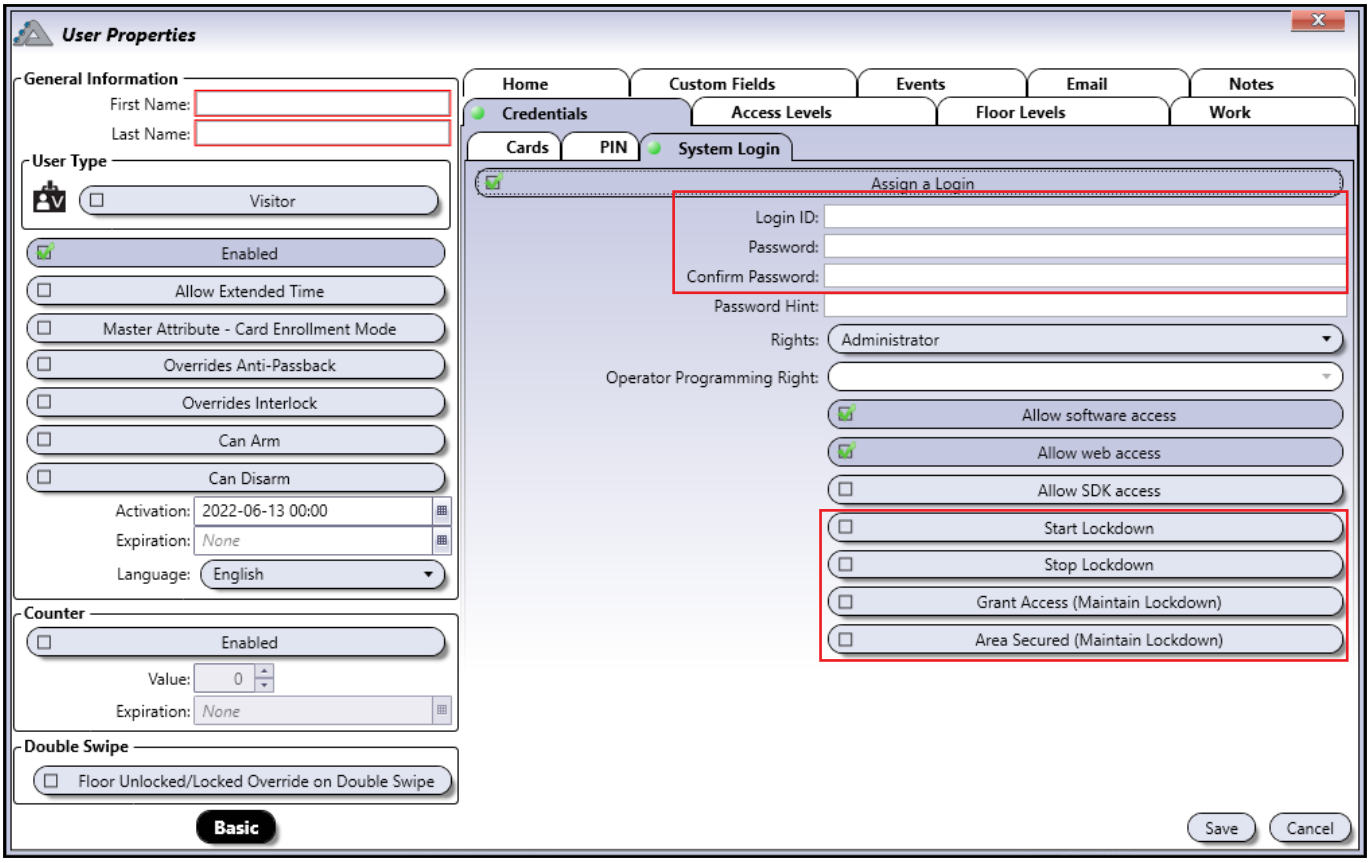
Legend: Displays the different Login Lockdown rights available when logged into Atrium. For more information on these rights, see the User Properties menu on the next page.

ASSIGNING A USER

Click on ***Assign*** to open the **User** menu. Select a User in the list or use the **Find** filter to specify one, then click ***OK***.



The **User Properties** window appears after selecting your User. The **System Login** tab displays important information used for logging into the system and for using Lockdown.



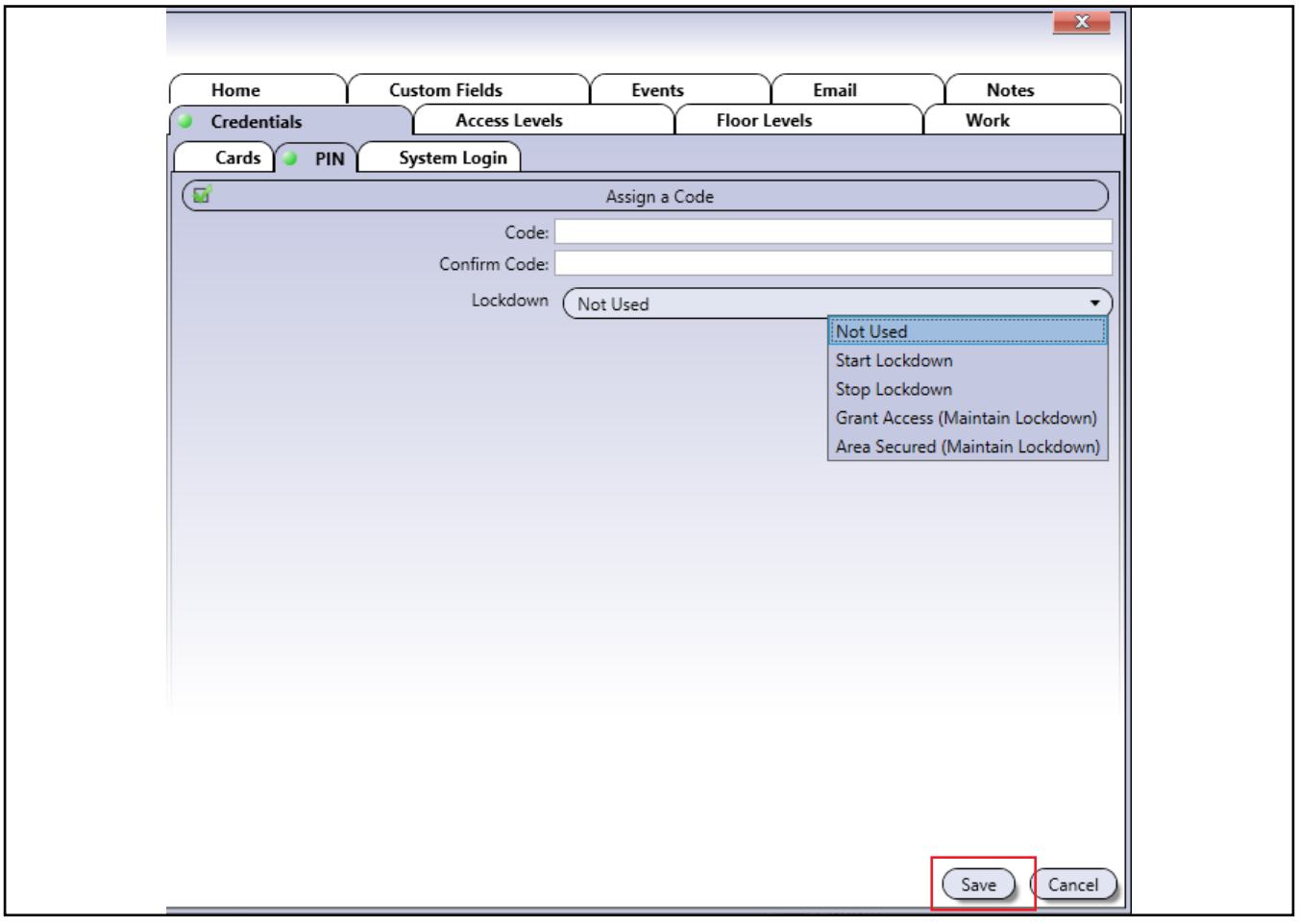
Type in a **User Name** for the login, a **Password**, and the password again to **Confirm Password**.

Select one or more Lockdown Rights for the User. Click ***Save*** if all changes are complete, or use the **PIN** tab to continue configuration.

- **Start Lockdown:** This User can start lockdown.
- **Stop Lockdown:** This User can stop lockdown.
- **Grant Access (Maintain Lockdown):** This User can Grant Access through a door during lockdown. After the door's unlock time ends, it locks and remains locked for the duration of the lockdown.
- **Area Secured (Maintain Lockdown):** This User can designate an Area as secured during a lockdown.

ASSIGNING A PIN FOR LOCKDOWN

Click on the ***PIN*** tab and check off the **Assign a Code** box. After typing in a 5-digit PIN, select what this PIN does from the **Lockdown** dropdown menu. The options available are the same as the above Lockdown Rights, but only one can be selected per user PIN.



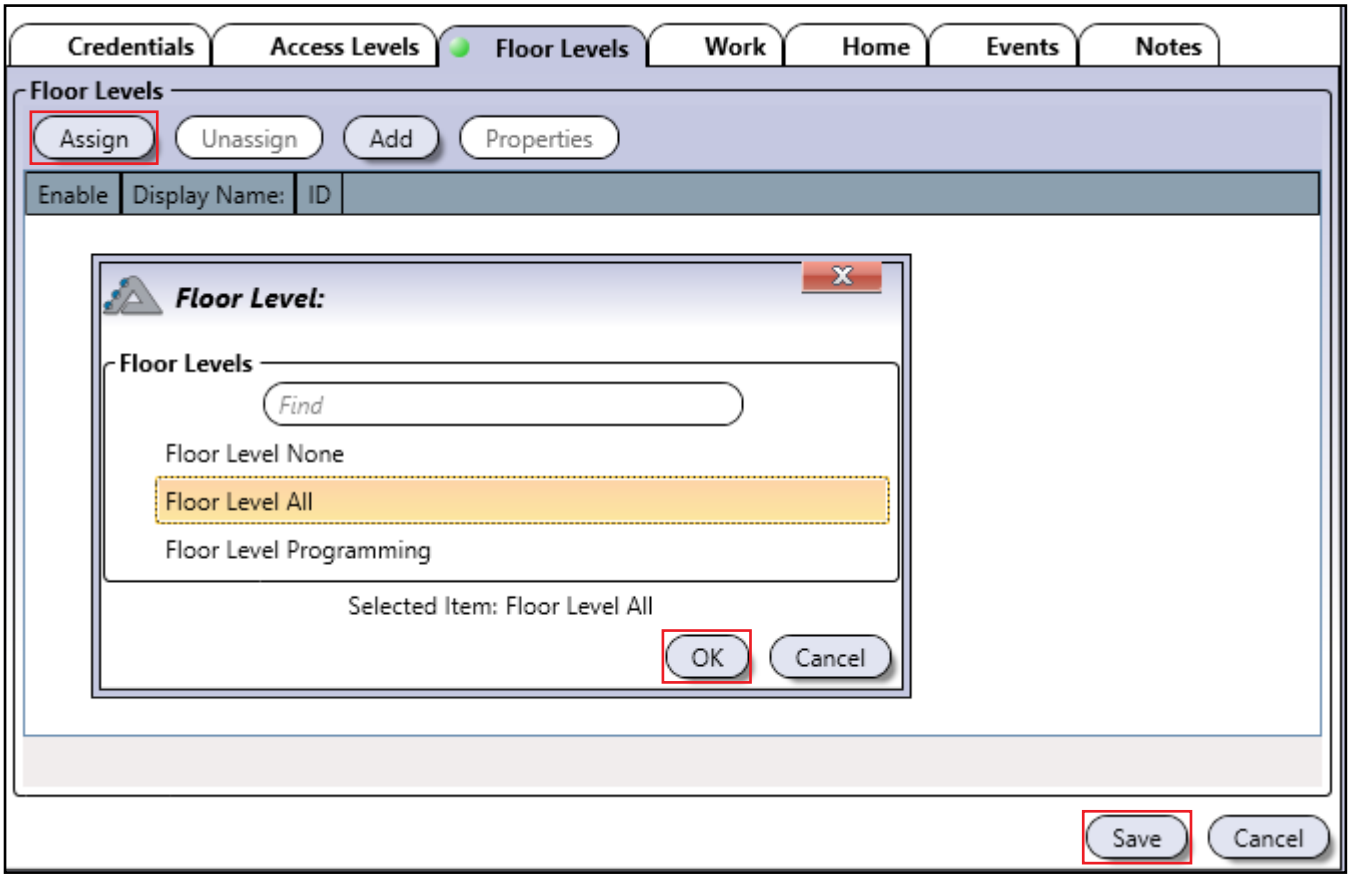
Click ***Save*** if all changes are complete, or use the **Floor level** tab to continue configuration.

ASSIGNING FLOOR LEVELS FOR LOCKDOWN

See below for assigning floor levels to a user. If you don't have elevator control integrated into Atrium, you can skip this section. The Floor Level specifies what floors the user has access to and can grant access to during a lockdown.

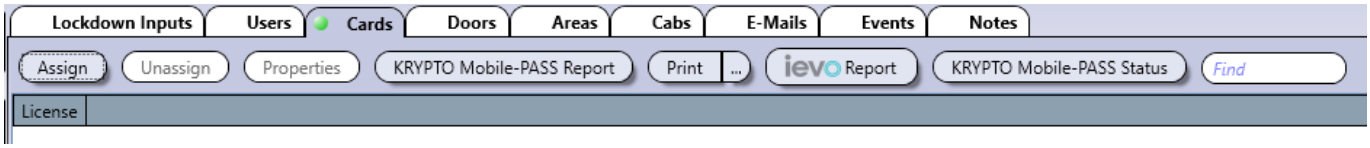
Assigning Floor Levels to a user allows the Grant Access function to be used on elevator cabs during lockdown. See the Cabs section in the Lockdown Activated Menus chapter for more information.

Click on the ***Floor Levels*** tab and click on ***Assign***. Select a Floor Level from the list and ***Save***.



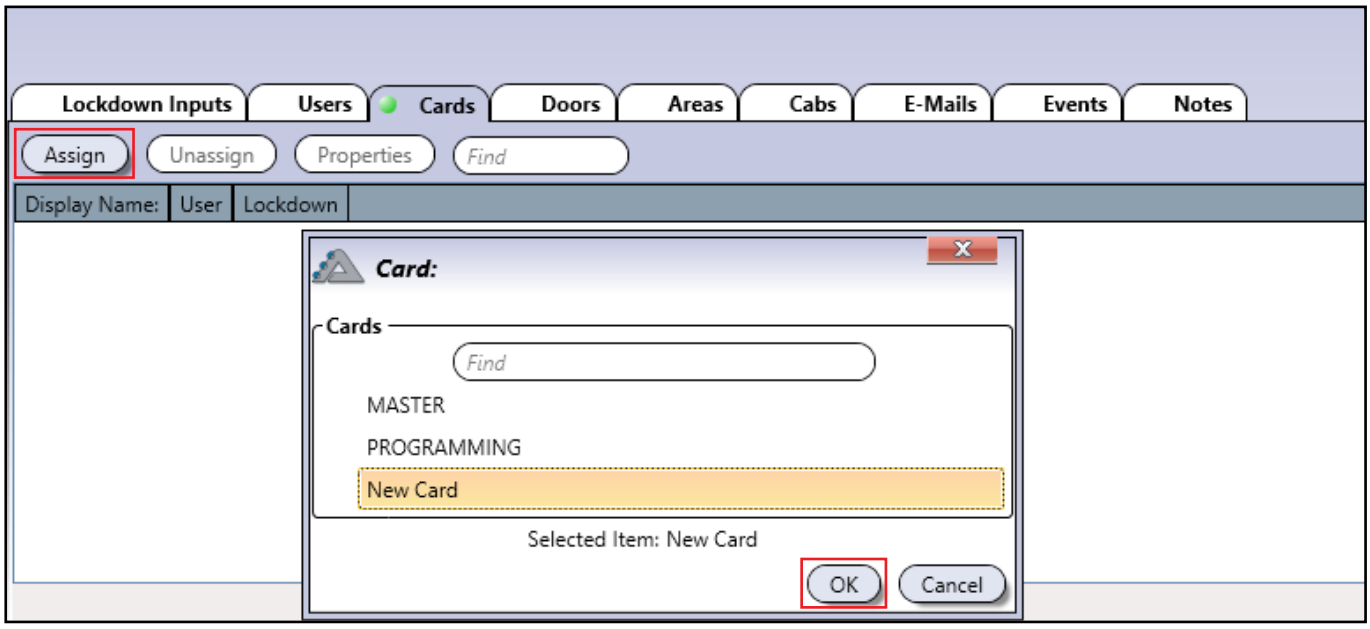
CARDS

The **Cards** tab is used to manage which cards can start and stop lockdown, grant access during a lockdown, and confirm which areas have been secured.

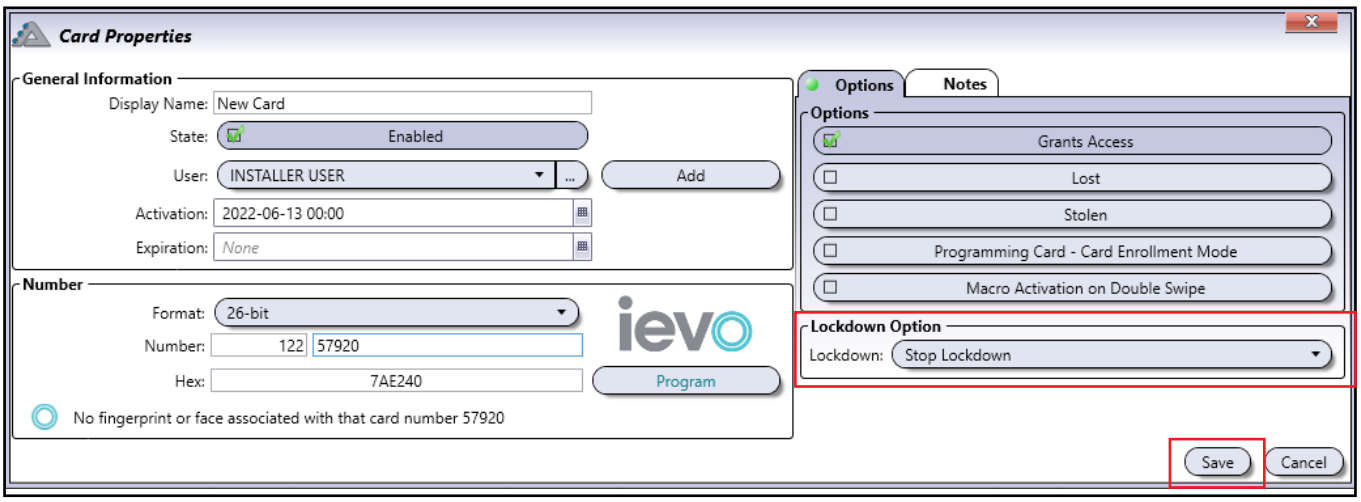


ASSIGNING A CARD

Click on ***Assign*** to open the **Card** menu. Select a Card in the list or use the **Find** filter to specify one, then click ***OK***.



The **Card Properties** window appears after selecting your Card. Select what this card does from the drop-down menu in **Lockdown Option** and click ***Save***.

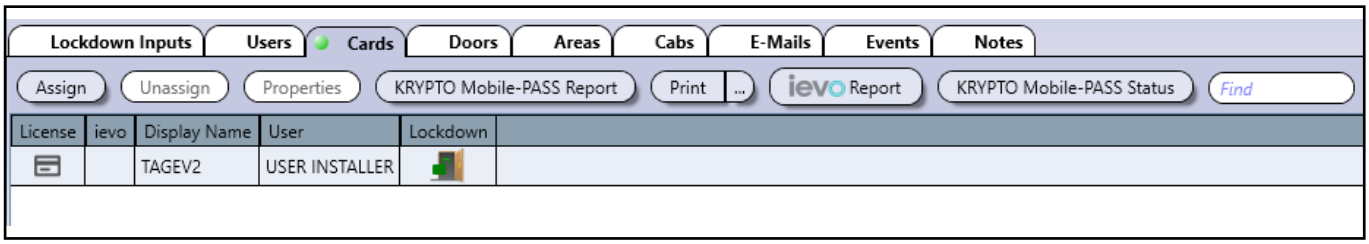


Lockdown Option

- **Start Lockdown:** This Card can start lockdown.
- **Stop Lockdown:** This Card can stop lockdown.
- **Grant Access (Maintain Lockdown):** This Card can Grant Access through a door during lockdown. After the door's unlock time ends, it locks and remains locked for the duration of the lockdown.
- **Area Secured (Maintain Lockdown):** This Card can designate an Area as secured during a lockdown.

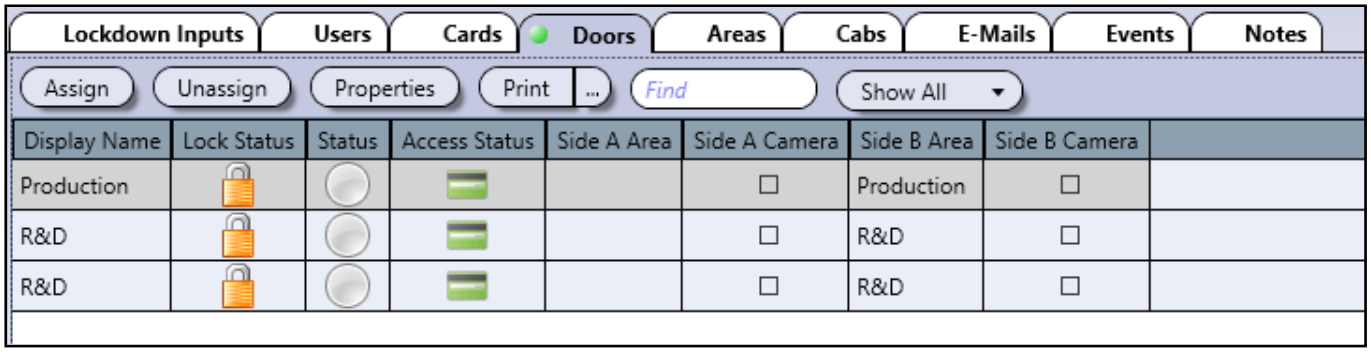
A Card must be assigned to a User for its selected **Lockdown Option** to function.

The Card and its Lockdown Option are now assigned.



DOORS

The **Doors** tab shows the list of doors available for lockdown. Only doors assigned to this list can be locked down.



Assign: Select a Door and assign it to the Lockdown list.

Unassign: Select a Door and remove it from the Lockdown list.

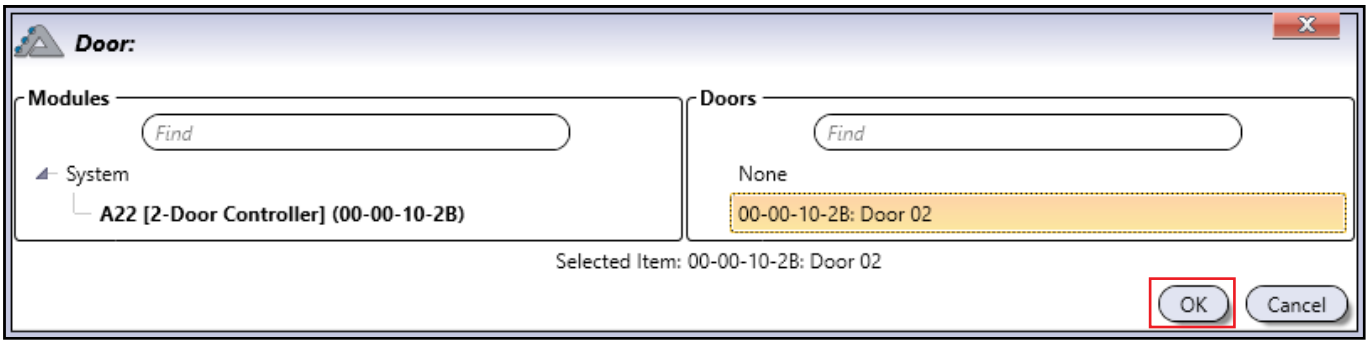
Properties: Edit a Door's properties.

Print: Generate and print door report for all or selected doors.

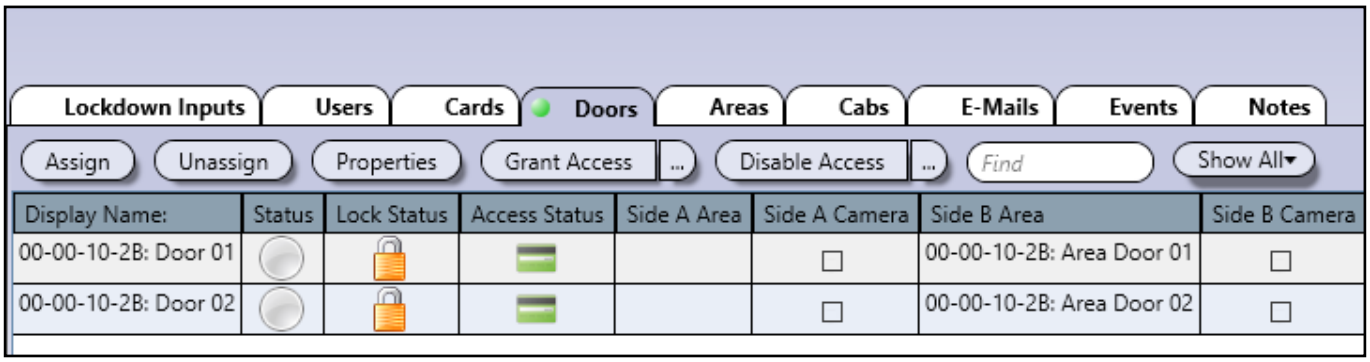
Find: Type in several letters or a full name to filter and find a specific Door**.**

ASSIGNING A DOOR

Click on ***Assign*** to open the **Door** menu. Select a Door in the list or use the **Find** filter to specify one, then click ***OK***.

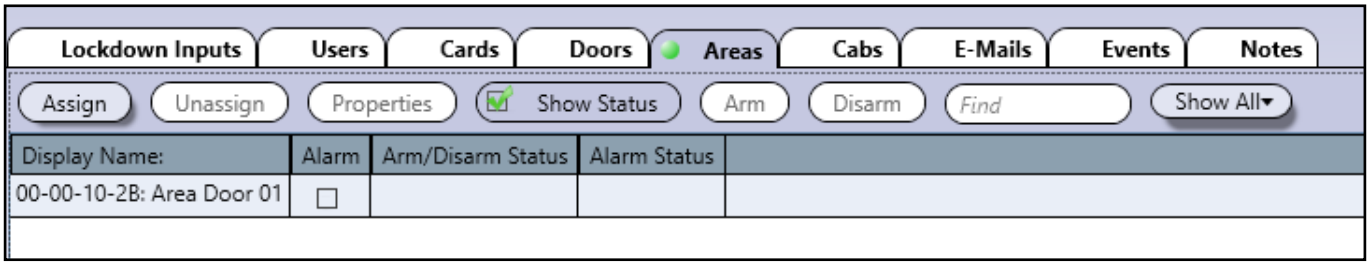


The Door is now assigned to the Lockdown list.



AREAS

The **Areas** tab shows the list of areas available for lockdown. To lockdown a door, its area must also be assigned to this list.



Assign: Select an Area and assign it to the Lockdown list.

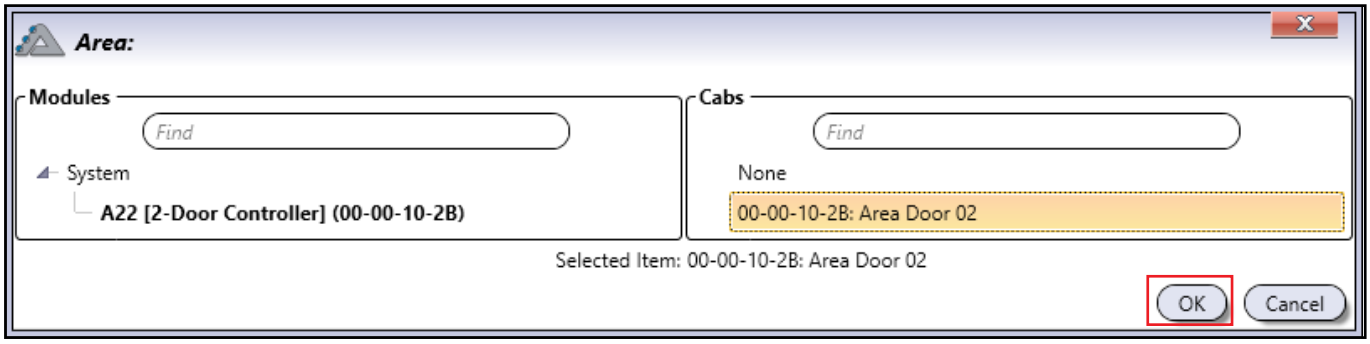
Unassign: Select an Area and remove it from the Lockdown list.

Properties: Edit an Area's properties.

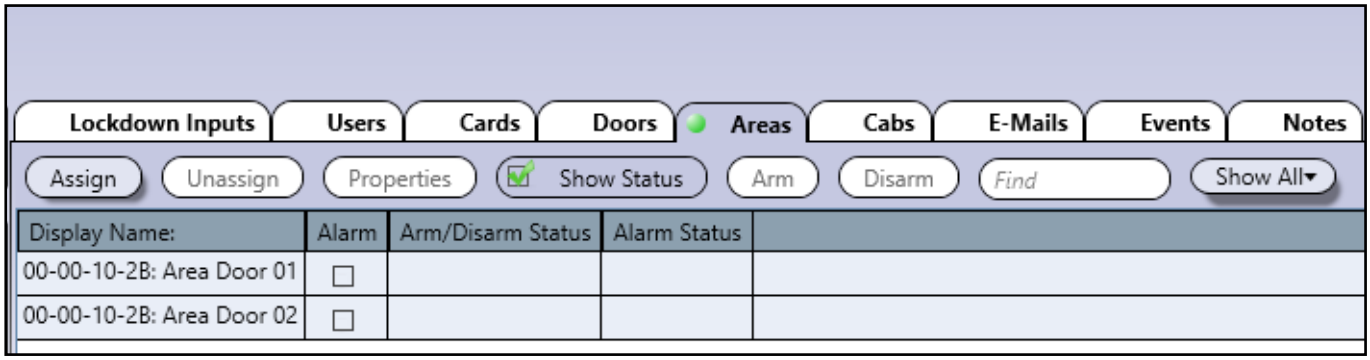
Find: Type in several letters or a full name to filter and find a specific Area**.**

ASSIGNING AN AREA

Click on ***Assign*** to open the **Area** menu. Select an Area in the list or use the **Find** filter to specify one, then click ***OK***.

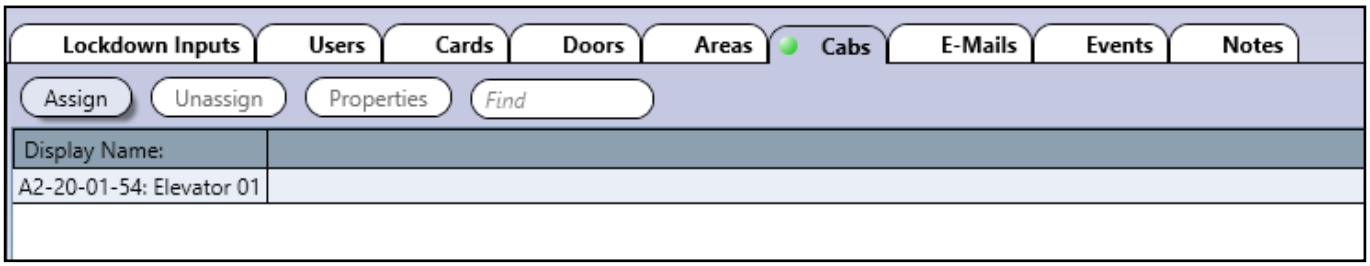


The Area is now assigned to the Lockdown list.



CABS

The **Cabs** tab shows the list of elevator cabs available for lockdown. Only cabs assigned to this list can be locked down.



Assign: Select a Cab and assign it to the Lockdown list.

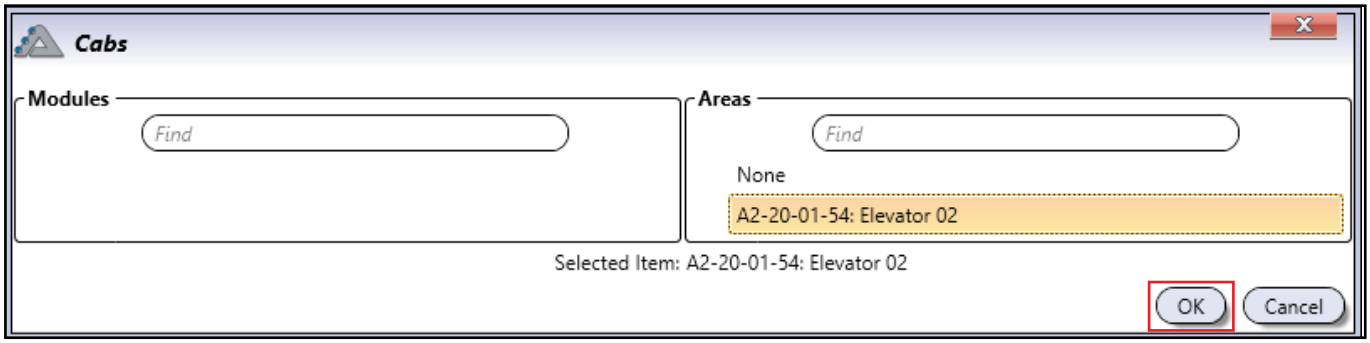
Unassign: Select a Cab and remove it from the Lockdown list.

Properties: Edit a Cab's properties.

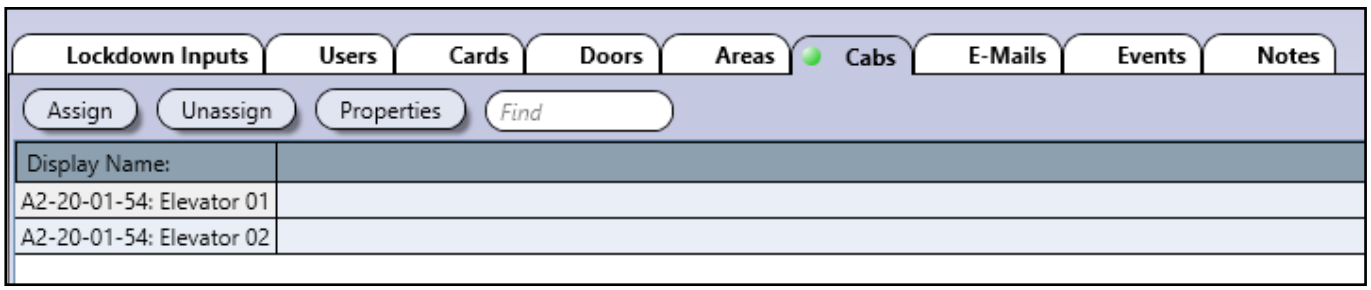
Find: Type in several letters or a full name to filter and find a specific Cab**.**

ASSIGNING A CAB

Click on ***Assign*** to open the **Cab** menu. Select a Cab in the list or use the **Find** filter to specify one, then click ***OK***.

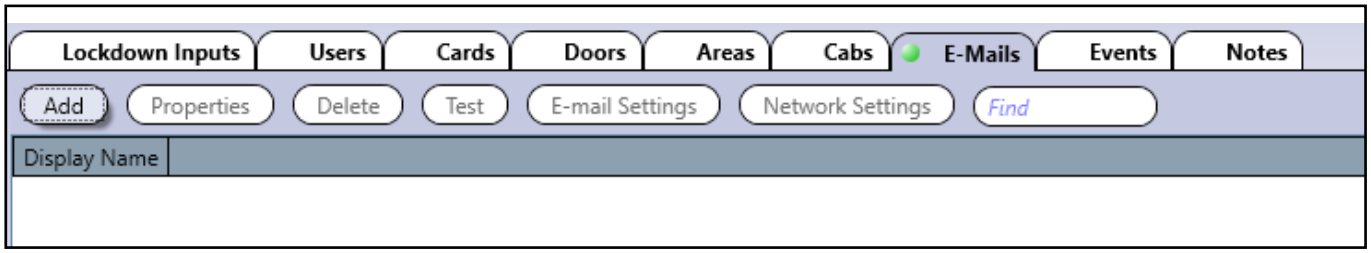


The Cab is now assigned to the Lockdown list.



EMAILS

The **Emails** tab shows the list of email notifications for starting and stopping Lockdown. For more information on emails, check the **Email Notifications** chapter.



Assign: Add an email notification to the Lockdown list.

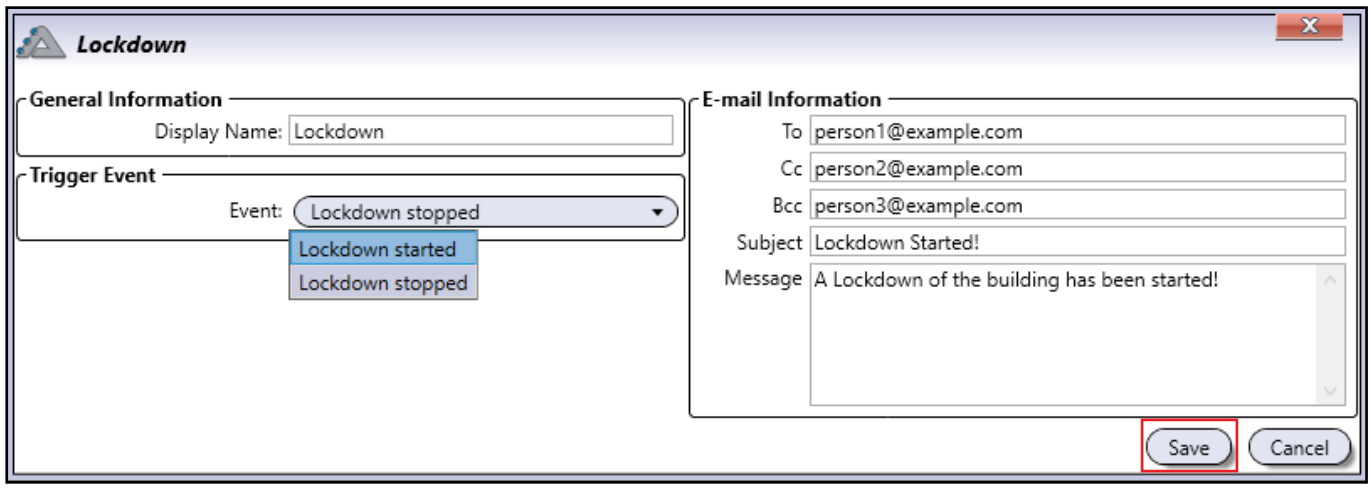
Properties: Edit an existing lockdown email notification.

Delete: Delete an email notification from the Lockdown list.

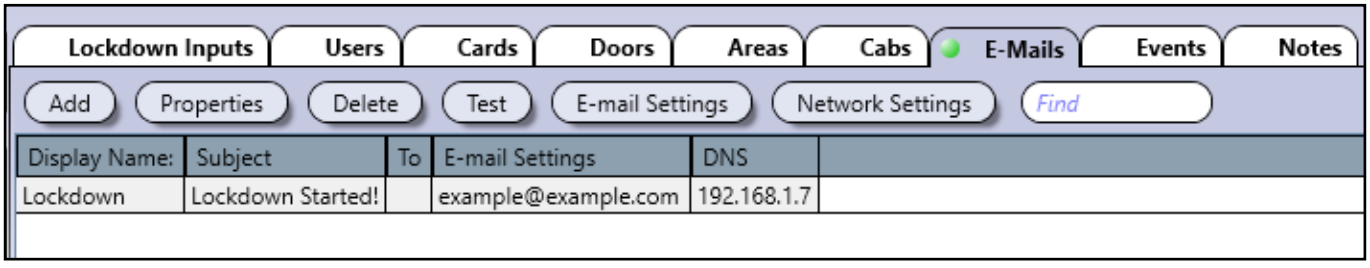
Test: Test an email notification in the Lockdown list. Always test to confirm functionality.

ADDING A LOCKDOWN EMAIL

Click on ***Assign*** to open the **Lockdown** menu for emails. The window below shows an example of an email notification for Lockdown. Click ***Save*** when finished.

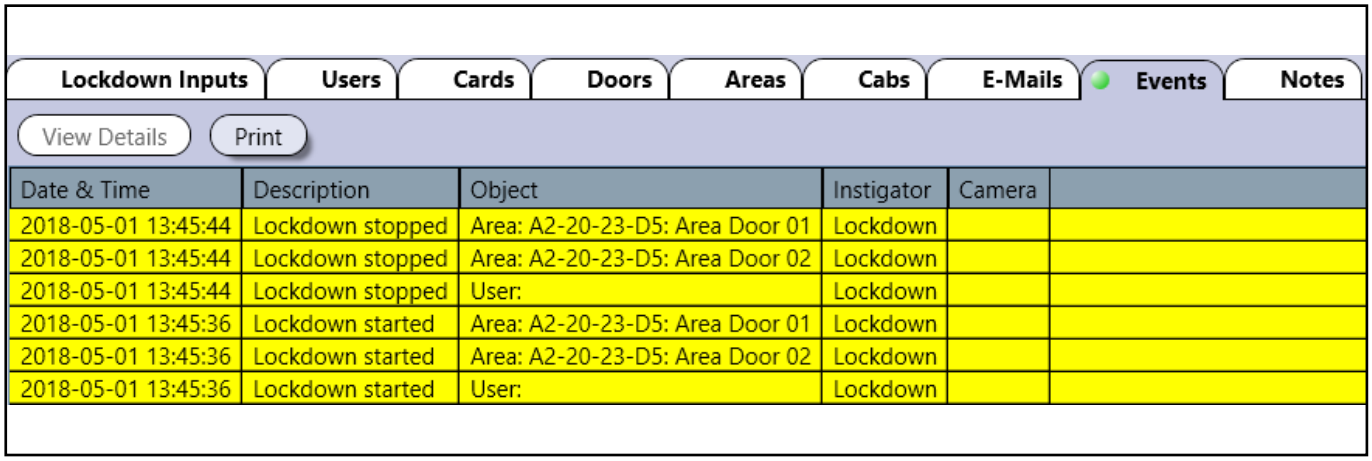


The Email is now assigned to the Lockdown list.



EVENTS

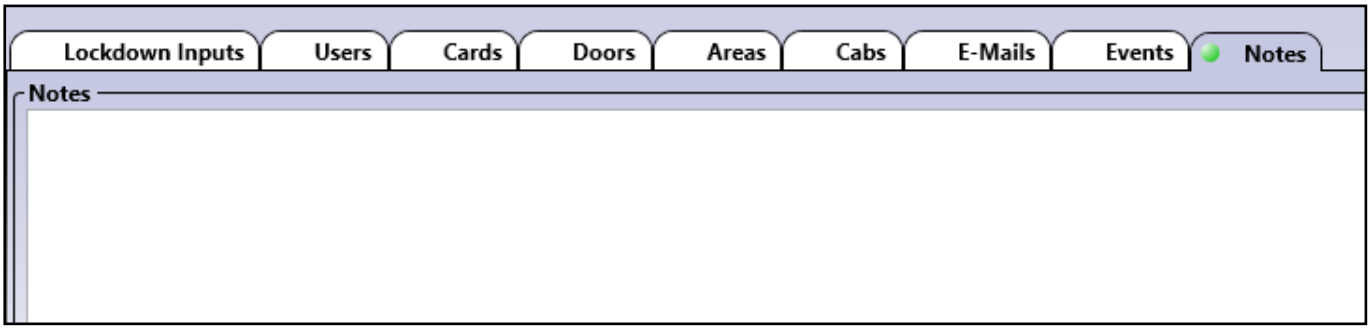
The **Events** tab shows the list of all events related to Lockdown.



Date & Time	Description	Object	Instigator	Camera	
2018-05-01 13:45:44	Lockdown stopped	Area: A2-20-23-D5: Area Door 01	Lockdown		
2018-05-01 13:45:44	Lockdown stopped	Area: A2-20-23-D5: Area Door 02	Lockdown		
2018-05-01 13:45:44	Lockdown stopped	User:	Lockdown		
2018-05-01 13:45:36	Lockdown started	Area: A2-20-23-D5: Area Door 01	Lockdown		
2018-05-01 13:45:36	Lockdown started	Area: A2-20-23-D5: Area Door 02	Lockdown		
2018-05-01 13:45:36	Lockdown started	User:	Lockdown		

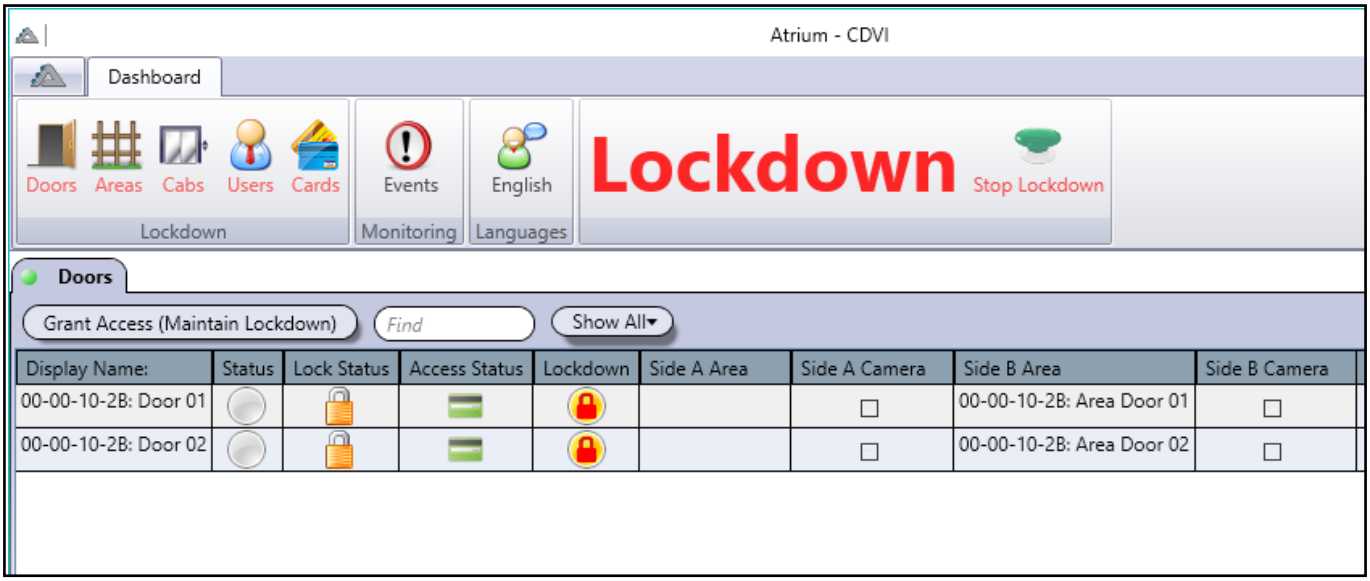
NOTES

The **Notes** tab provides a space to type in notes.



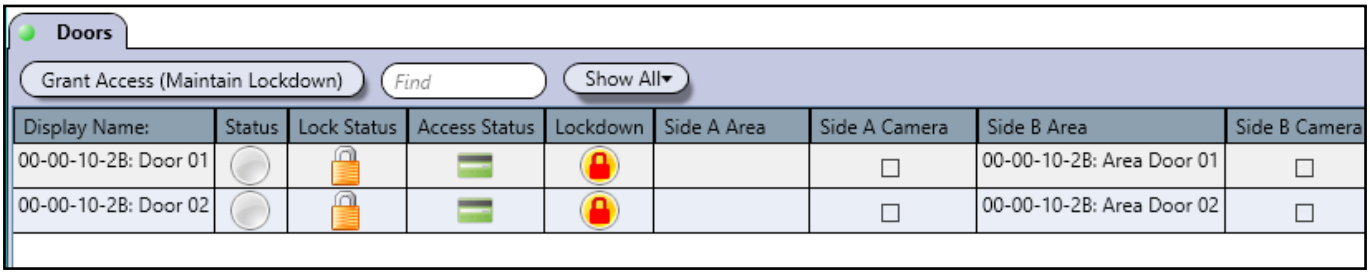
LOCKDOWN ACTIVATED MENUS

When **Lockdown** is activated, the Atrium menus are restricted and all system configuration is disabled. Click ***Stop Lockdown*** to restore all menus.



DOORS

The **Doors** tab shows the list of doors currently under lockdown. Only doors previously assigned in the Lockdown Door menu are shown.



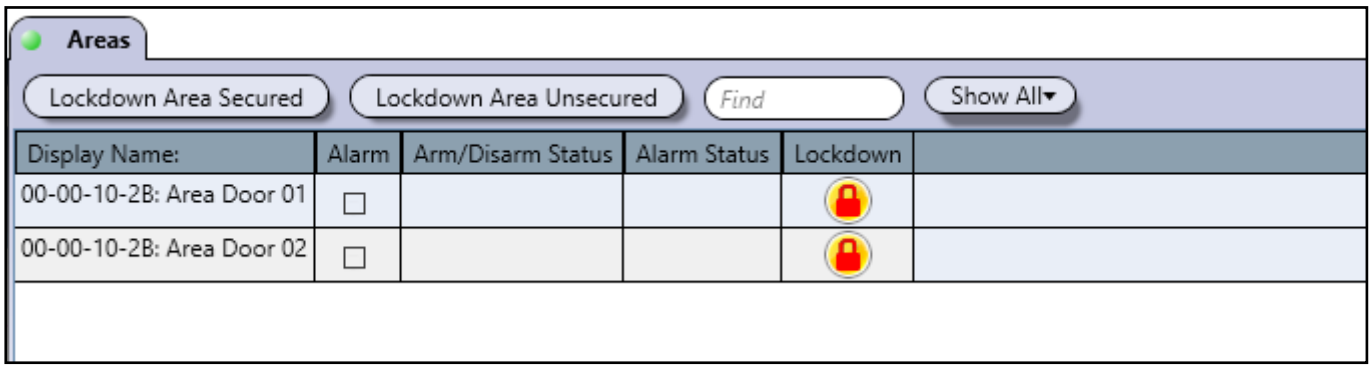
Grant Access (Maintain Lockdown): Grant Access through the door during lockdown. When the door relocks, Lockdown remains in effect. Note that this option is selectable only if it is assigned in the User's Lockdown rights.

Find: Type in several letters or a full name to filter and find a specific Door.

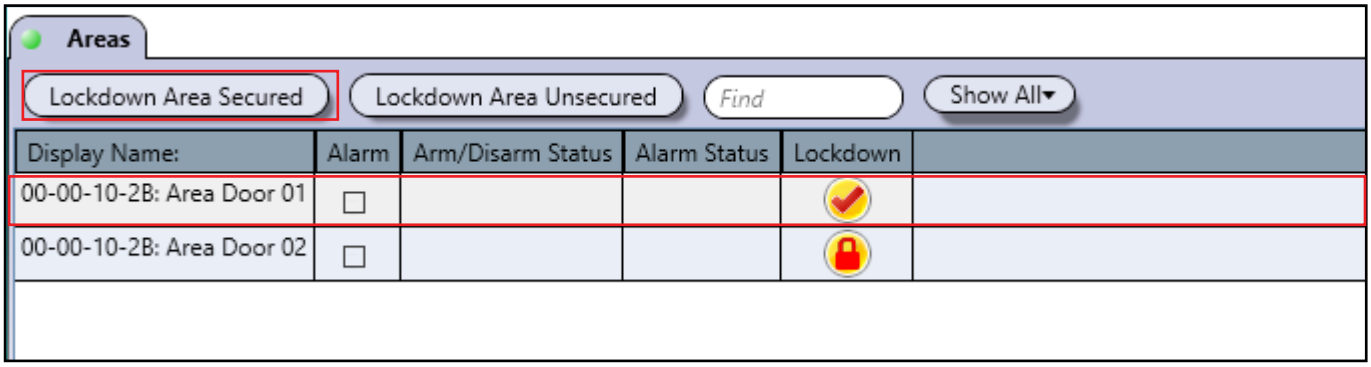
Show All: Click to toggle between all doors or only doors on a specific module.

AREAS

The **Areas** tab shows the list of areas currently under lockdown. Only areas previously assigned in the Lockdown Area menu are shown.



Lockdown Area Secured: Select an area and click on this button to indicate that the area is clear of any threat. The area should be checked physically



Always confirm that someone has physically checked the area(s) before setting the area(s) as secure in Atrium.

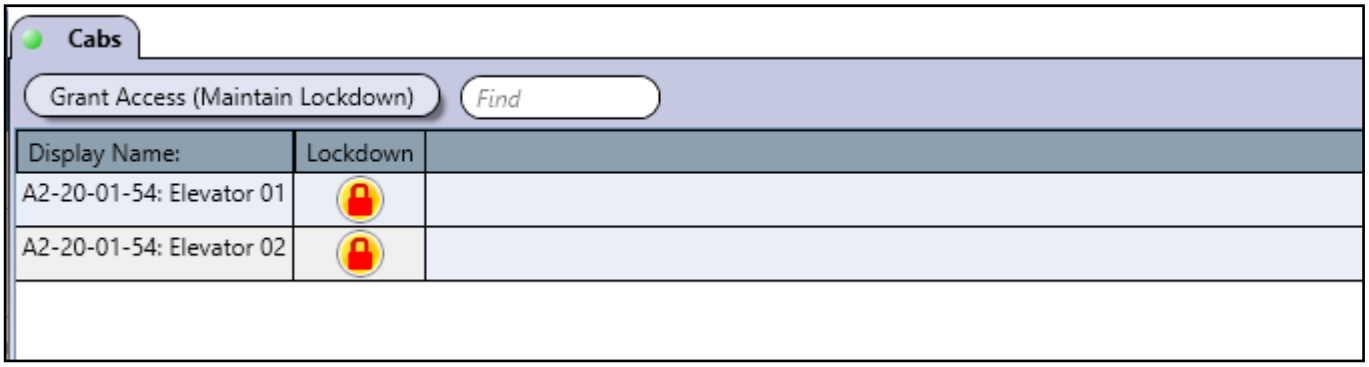
Securing areas one at a time helps confirm that they are safe, but this does not stop lockdown.

Lockdown Area Unsecured: Areas are unsecured by default and are potentially unsafe until they have been physically checked to confirm safety**.**

Show All: Click to toggle between all doors or only doors on a specific module.

CABS

The **Cabs** tab shows the list of elevator cabs currently under lockdown. Only cabs previously assigned in the Lockdown Cab menu are shown.

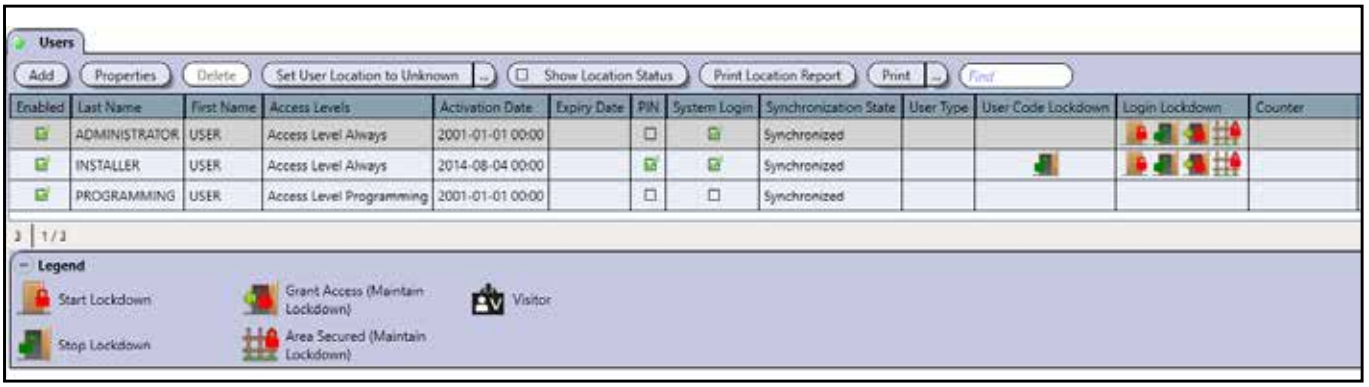


Grant Access (Maintain Lockdown): Grant Access to allow a user to temporarily select elevator cab floors during lockdown. After the Grant Access ends, Lockdown remains in effect. Note that this option is selectable only if it is assigned in the Cab's Lockdown rights.

Find: Type in several letters or a full name to filter and find a specific Cab.

USERS

The **Users** tab shows the list of all users in Atrium. **User Code Lockdown** and **Login Lockdown** rights are also displayed (if they have been assigned).



EVENTS

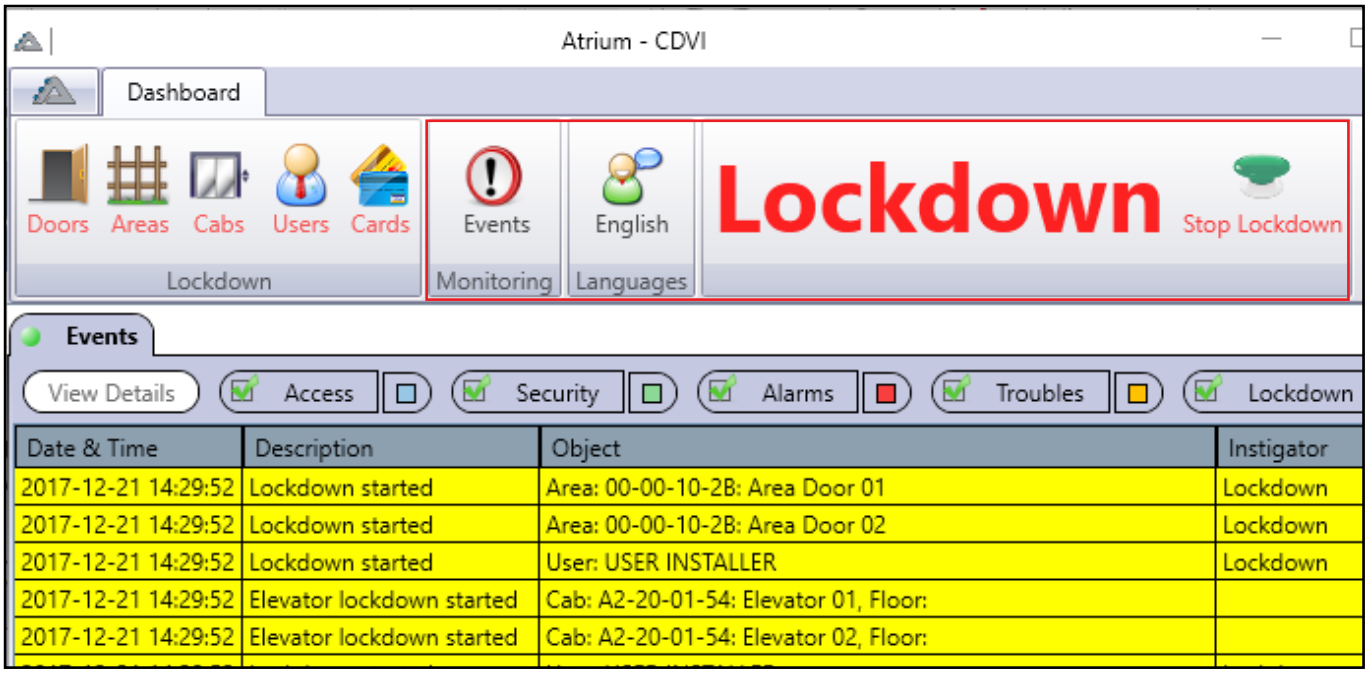
The **Events** tab shows the list of all events related to Lockdown.

LANGUAGES

The **Languages** tab shows the list of available languages.

STOP LOCKDOWN

Click here to Stop Lockdown. A password may be required if the option has been set in the Lockdown Configuration options.



IEVO BIOMETRIC INTEGRATION

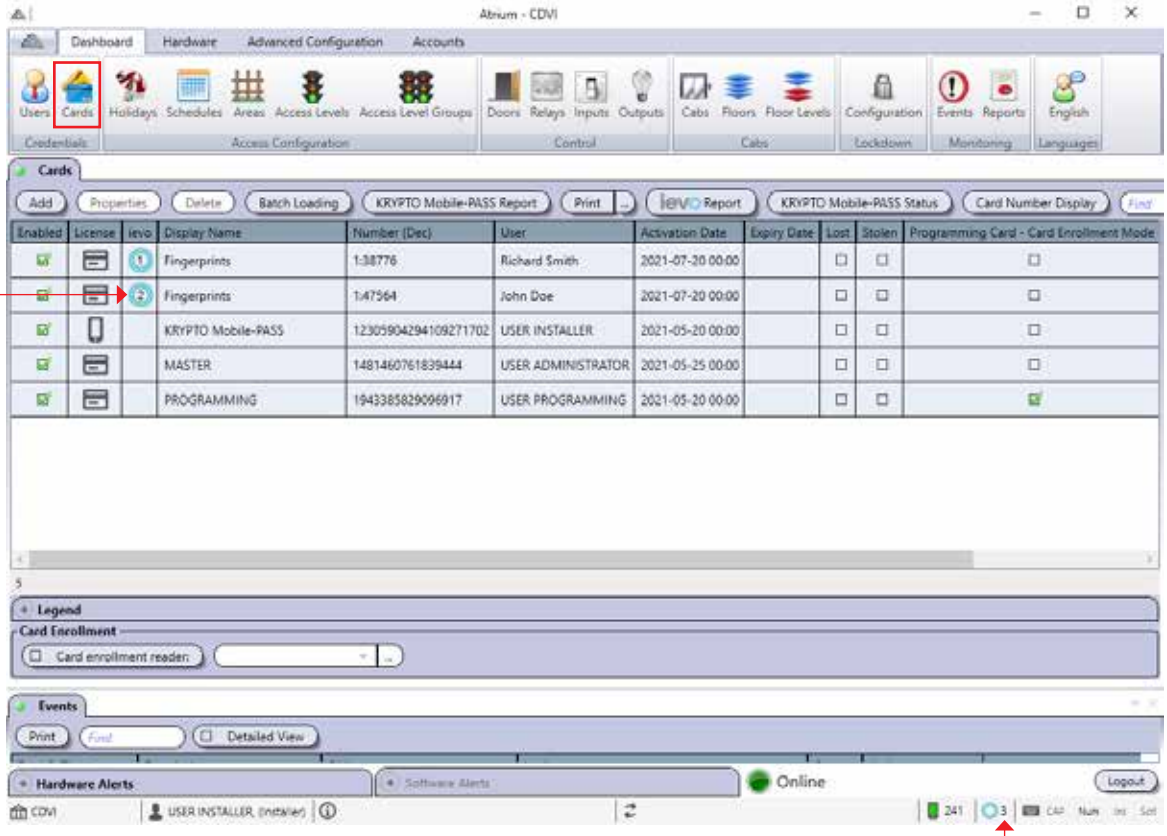
The integration of IEVO products with the ATRIUM system allows for a simple and efficient management of fingerprint templates. The integration works in tandem with IEVO's isync server pre-installed and running in the background. All fingerprint templates, up to 50,000, will be encrypted and stored in the IEVO controller. ATRIUM creates a random card number, 26-bit format, to which it will be possible to associate and register up to 10 fingerprint templates.

The IEVO digital fingerprint reader(s) and isync server must be installed beforehand. The ATRIUM software and the IEVO isync server must be installed on the same PC. Refer to the IEVO manual for installation instructions.

CARD MENU OVERVIEW

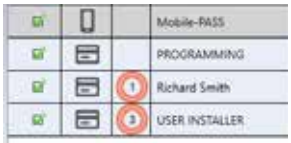
The card menu below illustrates the display available with IEVO integration.

The icon (circle) indicates that this card number is associated to a fingerprint and the number inside the icon indicates the number of registered fingerprints under that card.



The number beside the icon indicates the total number of registered fingerprints in the IEVO controller.

Double click on the icon to display the complete list of enrolled fingerprint templates.

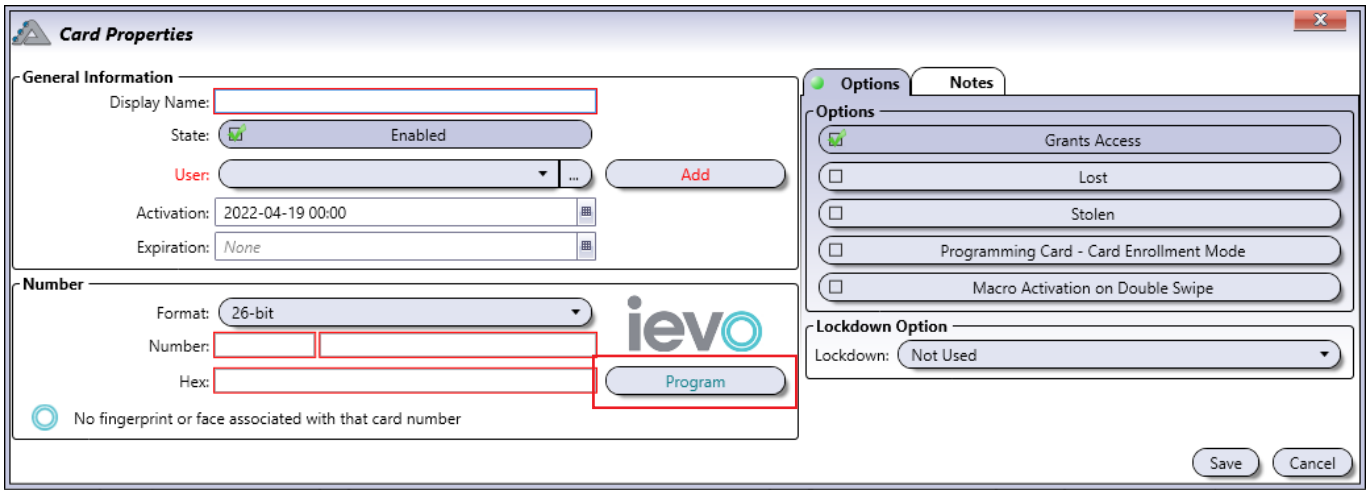


If the communication between the ATRIUM software and the IEVO controller is interrupted or lost, the IEVO icons will turn orange.

ENROLL AND ASSIGN A FINGERPRINT TO A USER

From the ***Dashboard*** tab, click on ***Cards***, and click on the ***Add*** button.

Make sure the user to whom you want to register a fingerprint, has previously been created in the ATRIUM system.



General Information

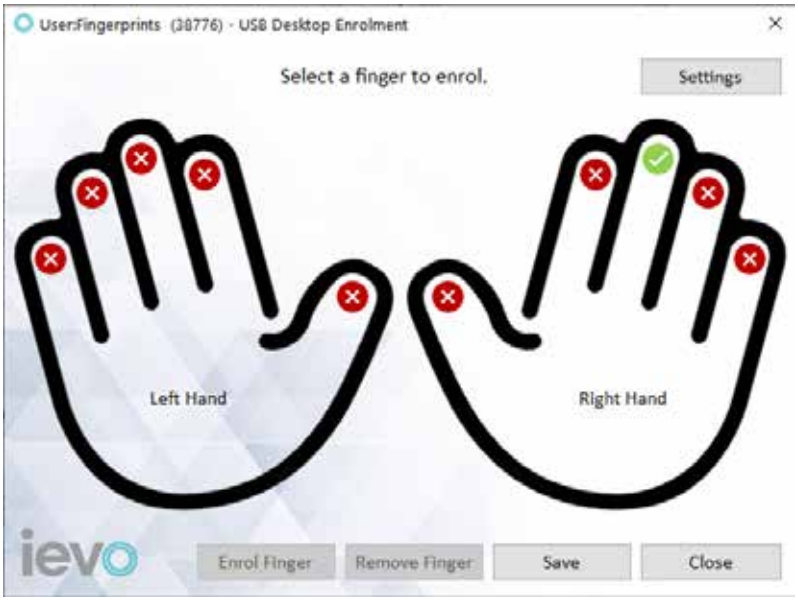
- **Display Name:** You **MUST** identify the card throughout the ATRIUM software. We recommend using a name that is representative of the card.
- **Enabled:** When selected, indicates that the card is active.
- **User:** You **MUST** assign this card to a User before starting the fingerprint enrollment process. Select an existing User or "Add" a new User. See page 16 to learn how to add and manage Users.
- **Activation Date:** Allows to select the date the card becomes valid. Enter the year, month, day and time of the day the card becomes valid or click on the calendar icon and select the date. The card will become active on the selected activation date and time.
- **Expiration Date:** Allows to select the date the card expires. This is useful for personnel on contract who would require an access for a specific period of time. Enter either the year, month, day and time of the day the card expires or click on the calendar icon and select the date and time. The card will expires on the selected date and time. For permanent cards, do not select an expiration date.

Number

- **Format:** The format used to record digital fingerprints is 26-bit format. The ATRIUM system allows digital fingerprints to be saved in 26-bit format (the default IEVO controller format). The "IEVO Program" button will appear once the 26-bit format has been selected (format programmed in the IEVO controller by default). If a different format has been configured in the IEVO controller, the "IEVO Program" button will not appear.
- **Number and Hex:** You will be able to find the card number displayed in the events once read by a card reader. Depending on the format selected, the card number may contain a family code.

Once the card parameters have been established, click on the IEVO ***"Program"*** button

We assume that all the necessary equipment for digital fingerprint registration has been installed. This includes the digital fingerprint reader and the USB desktop enrollment reader as needed.



Unenrolled fingers Enrolled fingers

Here are the steps to enrol a fingerprint template:

1. Select a finger you want to enrol and then click ***"Enrol Finger"***.

2. The USB Desktop Enrolment reader will now light up. Place the selected finger onto the sensor.

3. After the first scan is complete, follow the on-screen instructions and remove your finger from the sensor. To ensure a successful enrollment, the finger must be removed from the sensor after each successful scan.

2.

3.

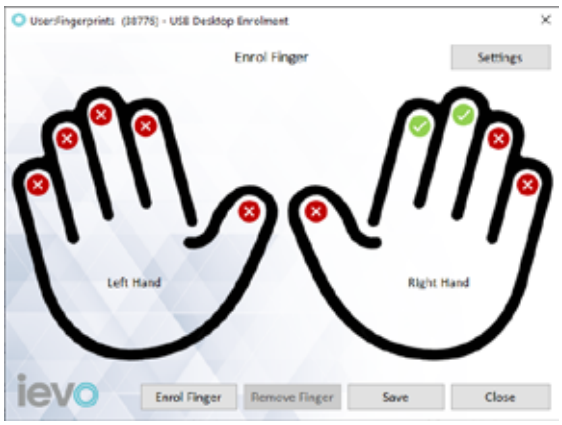
4. Place the finger back on the USB Enrollment reader when prompted. Wait and follow the on-screen instructions before removing the finger from the sensor.

5. When a successful scan is completed, a green check mark will appear beside the fingerprint. Click ***"OK"*** to complete the enrollment. Click ***"Cancel"*** to discard the current fingerprint scan if the image is not clear.

4.

5.

6. Repeat steps 1 to 5 to enrol another finger or click ***"Save"*** to complete the enrollment.

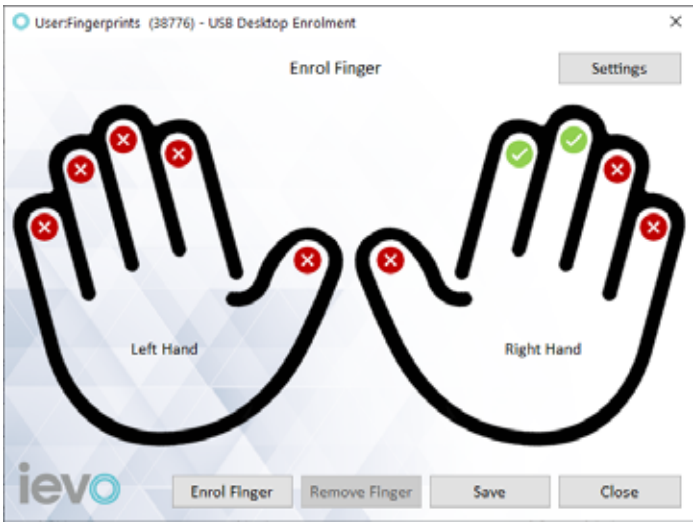


The isync server will now distribute the fingerprint templates across the system.

REMOVING A FINGERPRINT TEMPLATE

Here are the steps to remove a fingerprint template:

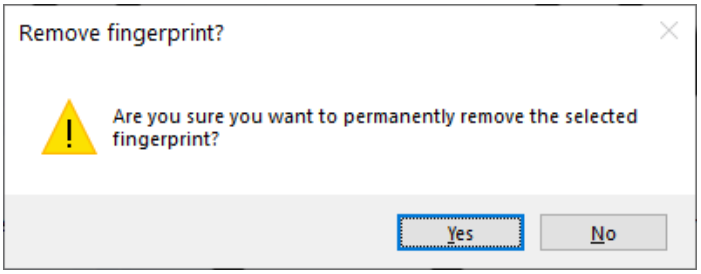
1. From the ATRIUM card properties window, click ***"IEVO Program"*** button.



Unenrolled fingers Enrolled fingers

2. Select an enrolled finger you want to remove and then click ***"Remove Finger"***.

3. Click ***"Yes"***. This will permanently delete the selected fingerprint.

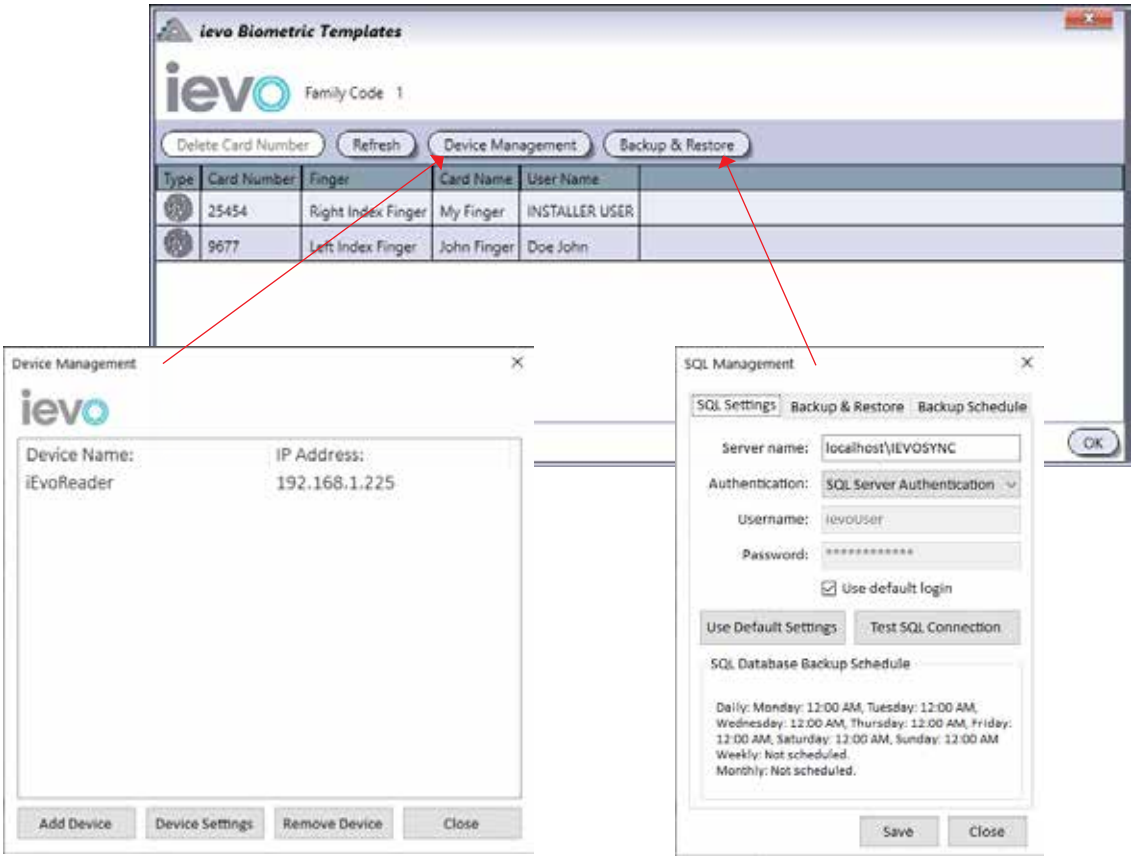


4. Repeat steps 2 and 3 to remove another finger or click ***"Save"*** to complete.

LIST OF FINGERPRINT TEMPLATES & SETTINGS

The complete list of enrolled fingerprints can be displayed by double clicking on the IEVO icon at the bottom right of the status bar of the ATRIUM software. You will be able to visualize at a glance the users who have a enrolled fingerprints. You will be able to delete a card and all the enrolled fingerprints attached to it easily. You will also be able to manage and configure devices as well as back up and restore enrolled fingerprints from the ATRIUM software.

Double click on the icon to display the complete list of enrolled fingerprint templates.



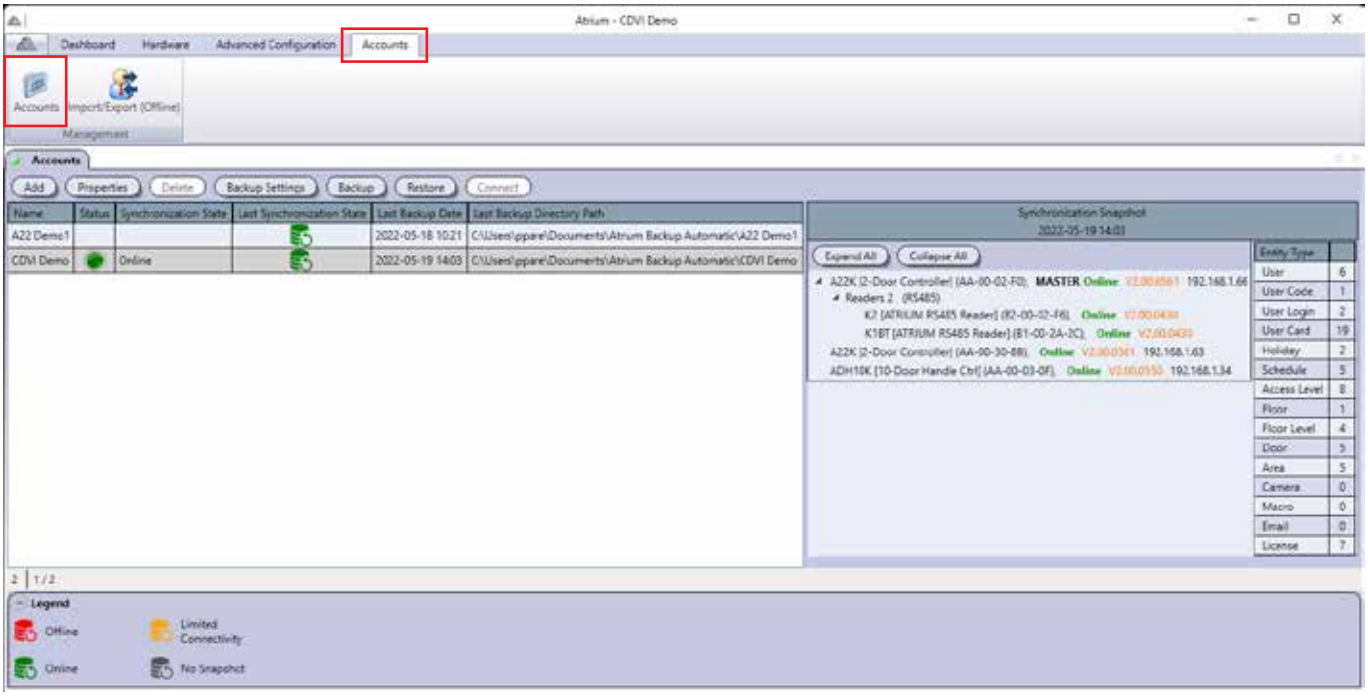
Please see the IEVO manual for details on device management and configuration as well as backing up and restoring enrolled digital fingerprints.

ACCOUNTS

Accounts are used when a computer connects to different ATRIUM installations. Typically, an installer creates a separate account for each client (site) he may have.

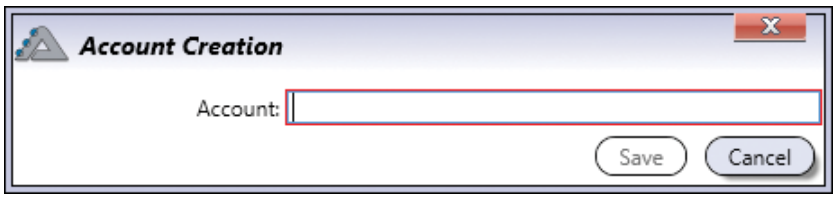
Each account has two dedicated database files; one for the static entities (users, cards, schedules, input, outputs, areas, tamper switches, etc.) and one for the events.

For each account, you will have the date as well as the directory path to which the last backup was made. When you select an account, you will get an overview of all modules that were online during the last backup, their IP addresses, serial numbers and the firmware installed at that time. In addition, you will get an overview of the amount of users, cards, doors, etc. that were in the selected ATRIUM account at the time of the last backup.



ADDING AN ACCOUNT

From the ***Accounts*** tab, click on the ***Accounts*** icon, and click on the ***Add*** button.



- **Account:** Identifies the account throughout the ATRIUM software. We recommend using a name that is representative of the account. Click on ***"Properties"*** to change the name of an account.

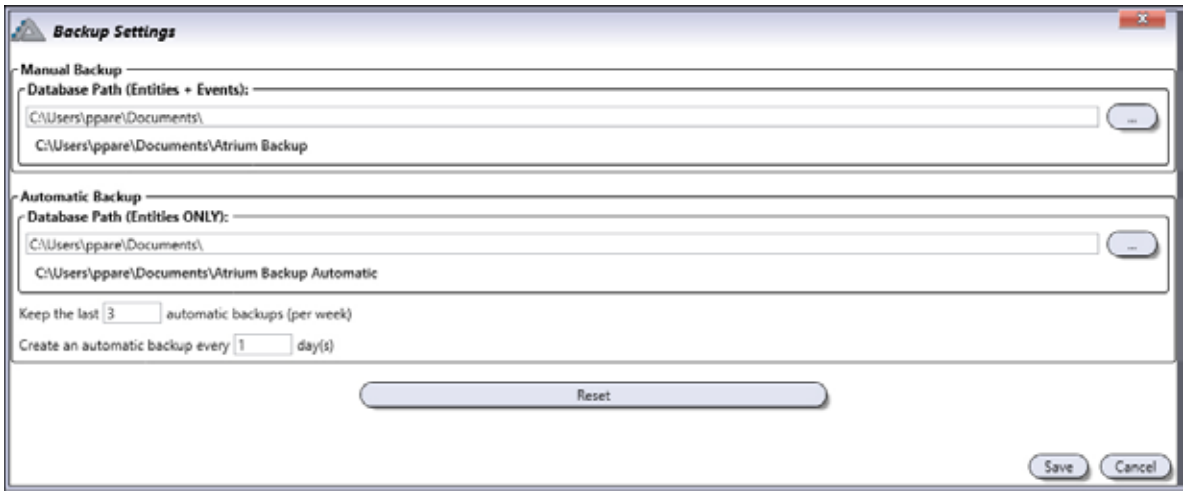
DELETING AN ACCOUNT

To delete an existing account, select the account from the list and click on the ***Delete*** button. A dialogue box will appear requesting confirmation. Deleting an account will erase the two database files related to this account. The Default account cannot be deleted.

BACKUP SETTINGS

Allows you to save the ATRIUM databases (entities and/or events) to the account you are logged in to.

From the ***Accounts*** tab, click on the ***Accounts*** icon, select an account from the list, and click on the ***Backup Settings*** button.



Manual Backup

- **Database Path (Entities + Events):** The "Atrium Backup" folder was created automatically when installing the ATRIUM software at the following location: C:\Users\user\Documents\. All backups made manually will be saved to this location by default. You can save your manual backups to the location of your choice (hard disk, network or USB key) by clicking on the button at the end of the directory path. A manual backup will generate two files (Entities + Events), a .bak file that includes all system configuration (Entities) and another .bak file for system events only (Events). Backups filenames are automatically generated as follows; account name-Date and time (CDVI Demo 2022.05.05-16.28.25.bak and CDVI DemoEvents 2022.05.05-16.28.25.bak)

Automatic Backup

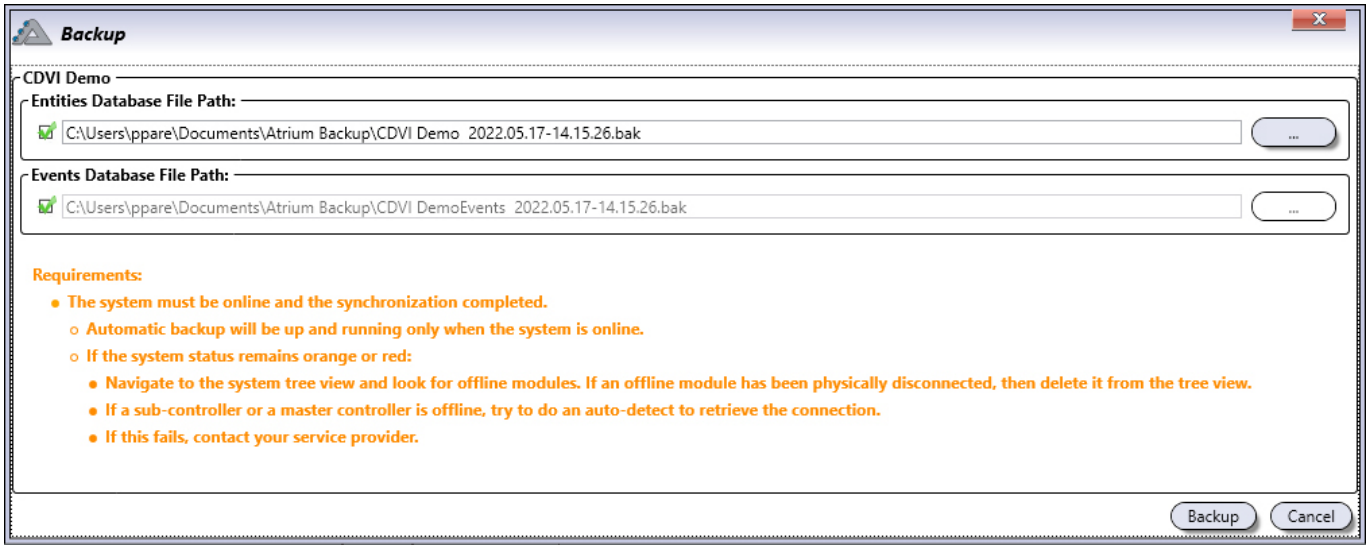
- **Database Path (Entities ONLY):** The "Atrium Backup Automatic" folder was created automatically when installing the ATRIUM software at the following location: C:\Users\user\Documents\. All backups made automatically will be saved to this location by default. You can save your automatic backups to the location of your choice (hard disk, network or USB key) by clicking on the button at the end of the directory path. An automatic backup will generate a .bak file that includes all system configuration without events. (entities ONLY). The backup filename will be generated automatically as follows; account name-Date and time (CDVI Demo 2022.05.05-16.28.25.bak)
- **Keep the last (??) automatic backups (per week):** This function determines the number of automatic backups that will be kept per week. By default, it will keep the last three (3) backups in the pre-defined directory.
- **Create an automatice backup every (??) day(s):** This function determines at what daily frequency the ATRIUM software, if it is kept running, will make an automatic backup. By default, the software will make an automatic backup every day, if you enter 7, it will make an automatic backup every 7 days and will be saved in the pre-defined directory.
- **Reset:** It will put back the default directory path.

The automatic backups are generated only if all modules are online (green icon status). This is to make sure that all backup are complete and generated without corrupted data. It is important to check that all modules are online before making a manual backup.

BACKUP (MANUALLY)

Manual backups will be saved to the location determined in the "Backup settings" section. You can also save your manual backups to a location of your choice (hard drive, network or USB drive) by clicking the button at the end of the directory path. Manual backups include full system configuration (entities + events).

From the ***Accounts*** tab, click on the ***Accounts*** icon, select an account from the list then click on the ***Backup*** button.



- **Entities Database File Path:** The entities database backup includes all system data except events.
- **Events Database File Path:** The events database is linked with the entity database and cannot be done by itself. It must therefore imperatively be done at the same time as that of the entities.

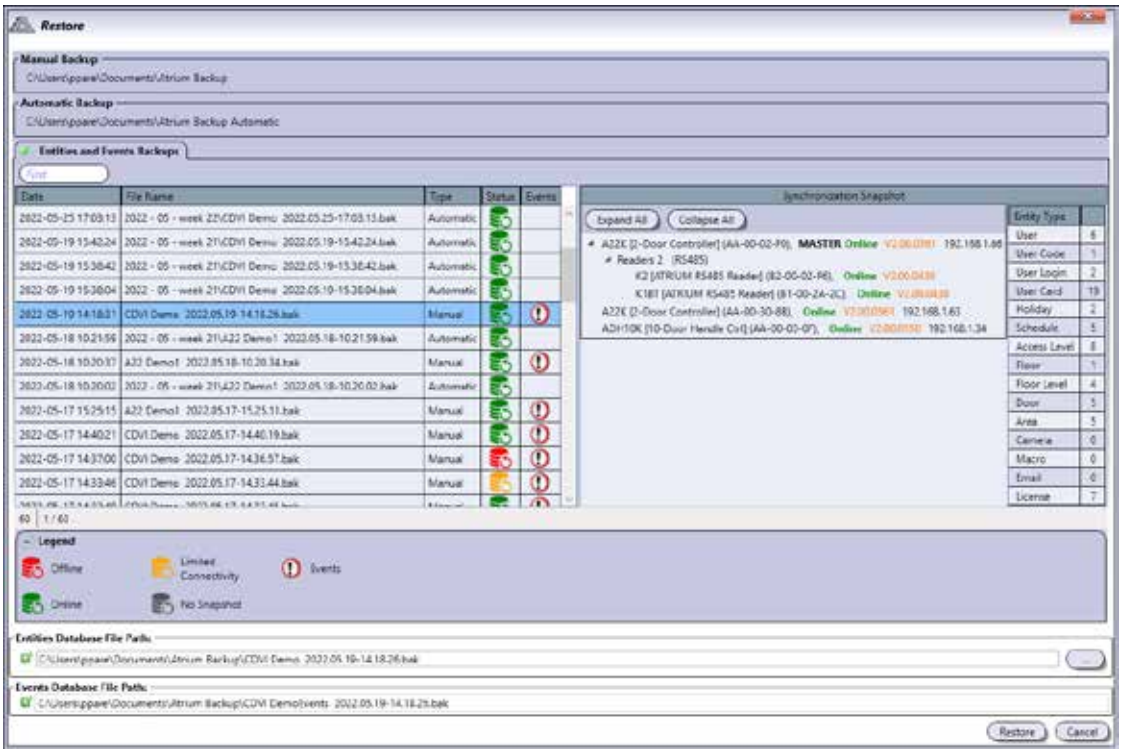
Both database backup will be save in the pre-determined directory path in the "Backup Settings". The file name is automatically generated with the account name and the date and time (See the text with the blue background in the image above). The date and time is generated when you previously click on the "Backup" button. You can rename the file to your need and also change the directory path by clicking the button at the end of the directory path.

It is important to make sure that all modules are online before making a manual backup. It will assure you to have a complete backup without corrupted data.

RESTORE

The restore option allows you to have a list of all backups made of the selected account at a glance. Choose a backup from the list, in order to have a preview (snapshot) of this backup before performing a restore. You will be able to see all the modules that were online during this backup, their IP addresses, serial numbers and the firmware installed at that time. In addition, you will get an overview of the number of users, cards, doors, etc. that were in the ATRIUM account at the time of the backup.

From the ***Accounts*** tab, click on the ***Accounts*** icon, select an account from the list, and click on the ***Restore*** button.



The list includes backups made automatically or manually, identified in the «Type» column.

The status of each backup is identified as follows;

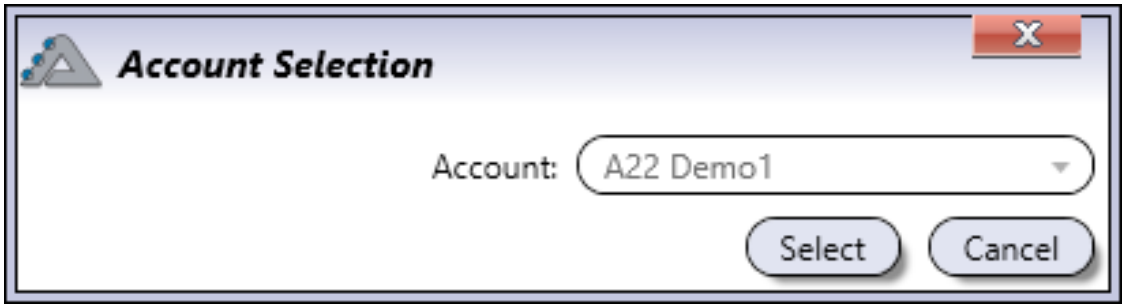
- **Green icon:** all modules were online during the backup
- **Red icon:** the master controller was offline during the backup
- **Yellow icon:** one or more sub-controllers was offline during the backup
- **Gray icon:** Unable to get an overview (No Snapshot) of the system during the backup
- **Event icon:** Backup includes events as well

The automatic backups are generated only if all modules are online (green icon status). This is to make sure that all backup are complete and generated without corrupted data. It is important to check that all modules are online before making a manual backup.

CONNECT

Select an account from the list and click on "Connect", then click on "Select" to confirm your selection and start synchronization with the account.

From the ***Accounts*** tab, click on the ***Accounts*** icon, select an account from the list, and click on the ***Connect*** button.

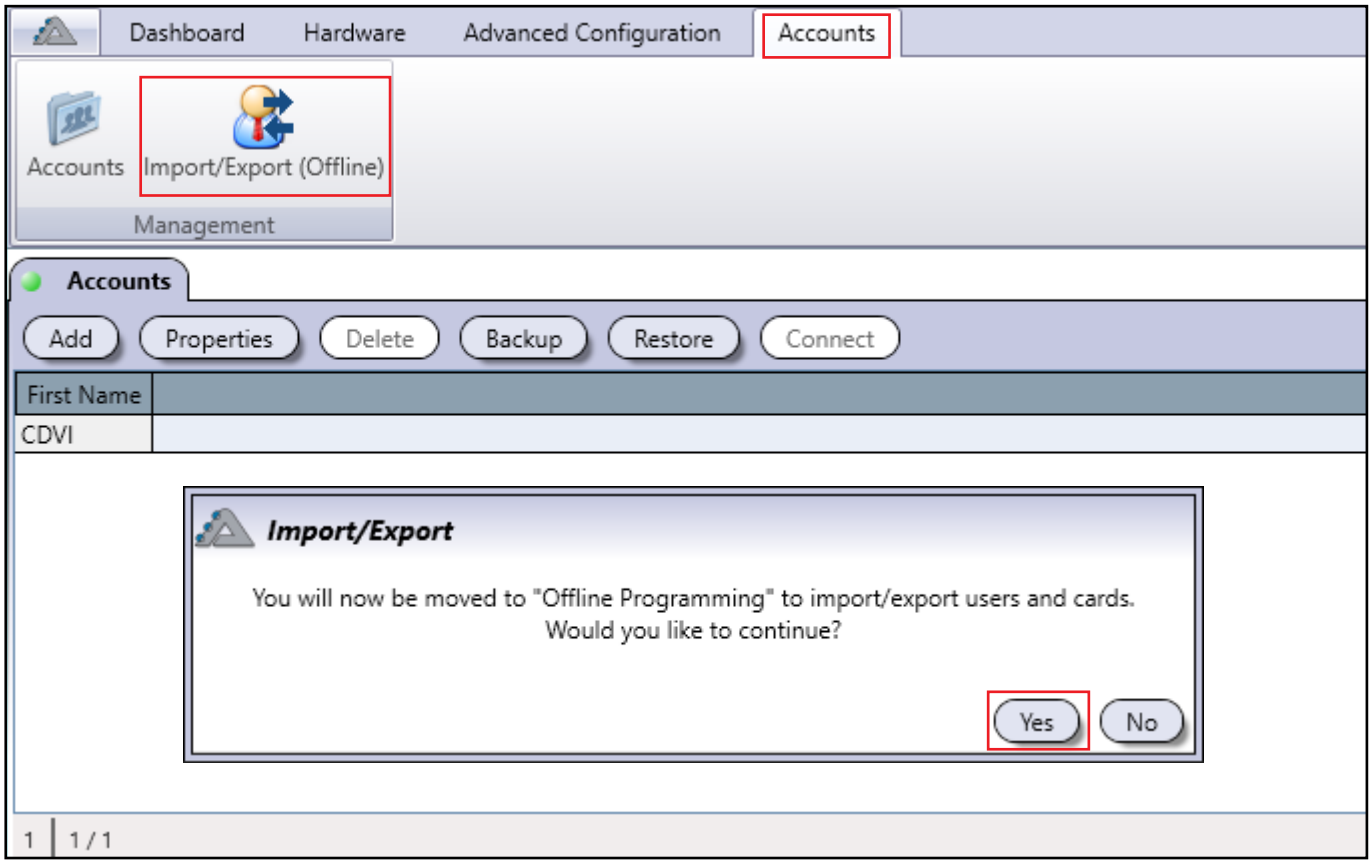


OFFLINE CONFIGURATION

Offline Programming allows you to import and export a database of users, cards and access levels. It also allows you to add or modify Users, Cards, Holidays, Schedules, Access Levels and Operator programming rights without being synchronized with a module.

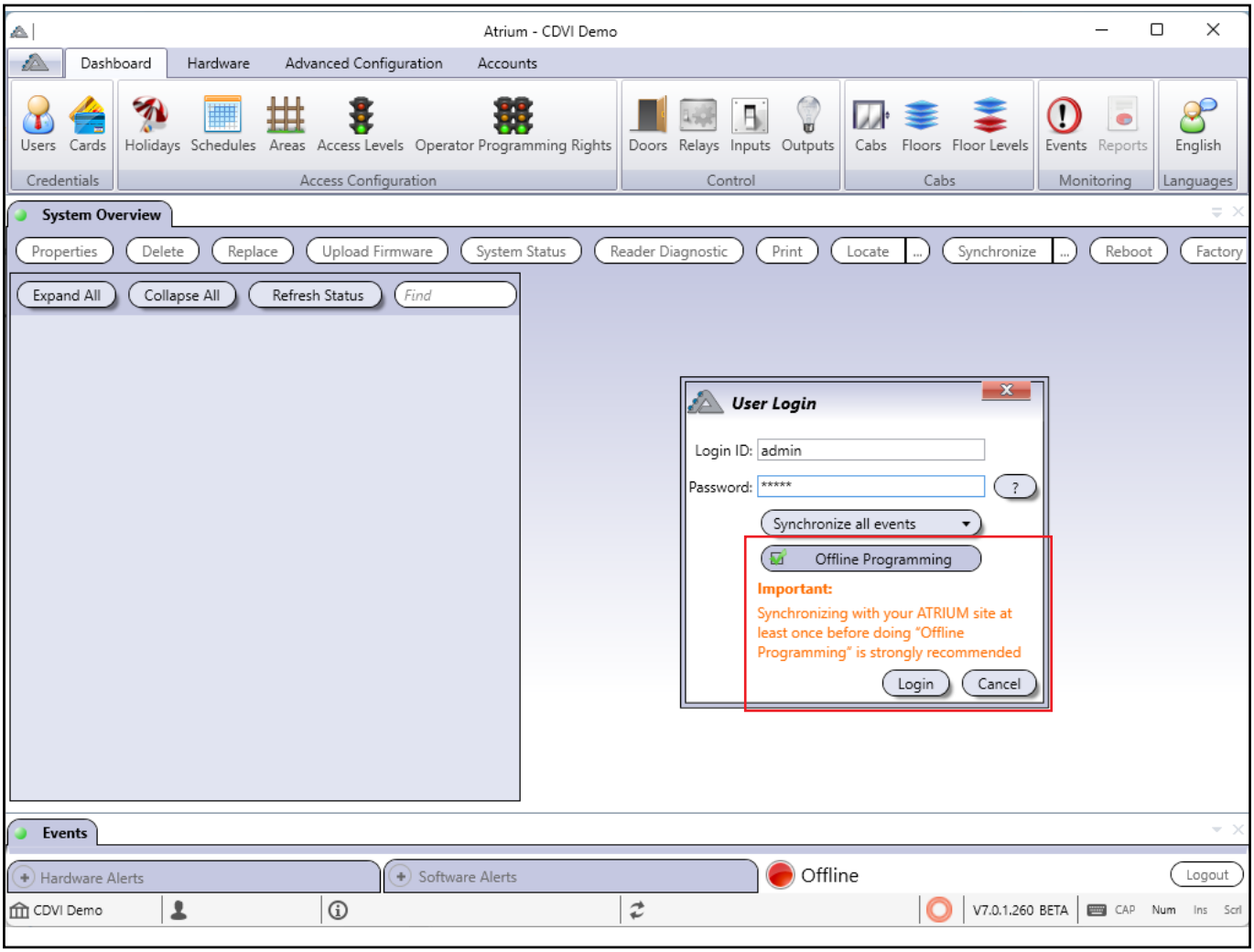
STARTING OFFLINE MODE (LOGGED IN)

From the ***Accounts*** tab, click on the ***Accounts*** icon, and click on the ***Import/Export (Offline)*** button. Click ***Yes*** in the popup window to move to offline programming.



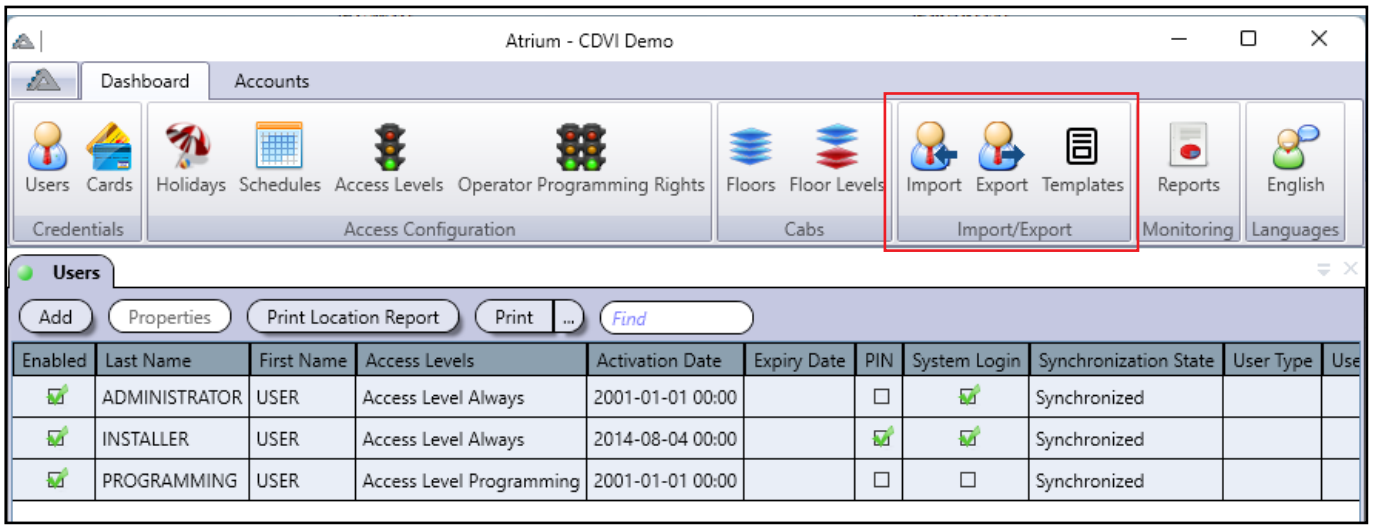
STARTING OFFLINE MODE (LOGGED OUT)

Run the Atrium Software and select an account to login to. From the ***User Login*** window, check off the ***Offline Programming*** option and click ***Login***.



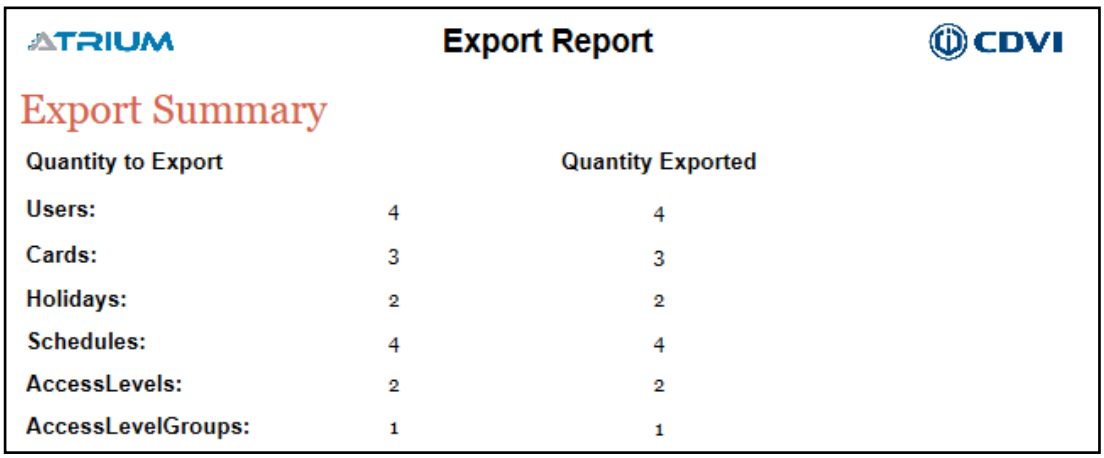
IMPORT/EXPORT MENUS

Import/export options are useful for building a database and exporting an existing database. Only users, cards, and access levels can be imported/exported.



Import: Click here to import a database. This database includes users, cards and access levels, as well as holidays and schedules (if specified). The file format must be **.csv**, **.xml**, **.txt** or **.xls** and follow a specific template (found by clicking on ***Templates***).

Export: Click here to export a database. This database includes all information except for hardware, areas, and doors. The file format is in **.xml**. Atrium will generate an **Export Report** showing what entities were successfully exported.



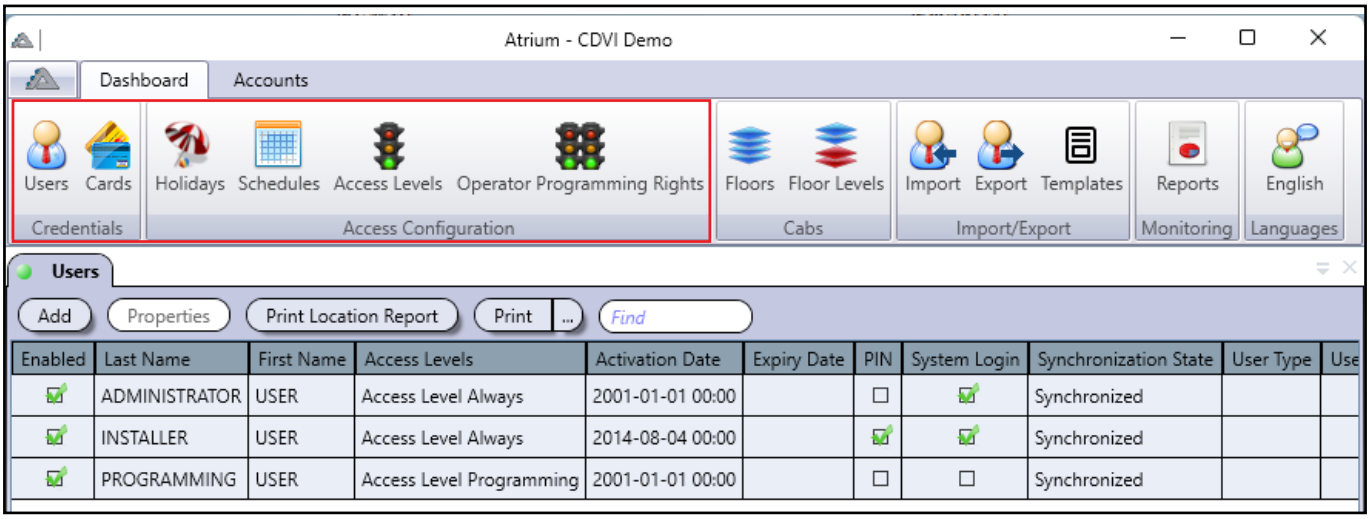
Templates: View import templates in **.csv**, **.txt** and **.xls** format. The sample template below shows the way to enter information for best results.

	A	B	C	D	E	F	G	H
1	First_Name	Last_Name	User_Code	Card_Name	Card_Format	Card_Number	Card_Hex_Number	Access_Level_Id
2	John	Doe	11111	John Doe Card	26-bit	236:20469	EC4FF5	2
3	Marc	Doe	22222	Marc Doe Card	30-bit	1348:33490	54482D2	2
4	Steve	Doe	33333	Steve Doe Card	44-bit	1041257005055	F26FC0FFFF	2
5	Brian	Doe	44444	Brian Doe Card	AWID 50-bit	2029426423	78F696F7	2
6	Allan	Doe	55555	Allan Doe Card	HID 37-bit	1592:370350	6385A6AE	2
7	Curtis	Doe	66666	Curtis Doe Card	HID 40-bit	207:21573	CF5445	2
8	Ken	Doe	77777	Ken Doe Card	IOProx XSF 39-bit	4987:58125	4987E30D	2
9	George	Doe	8888	George Doe Card	KeyScan 36-bit	198:33262	C681EE	2
10	Adam	Doe	99999	Adam Doe Card	Track 2	4564654654656566	1037877B369030	2
11	Marvin	Doe	10101	Marvin Doe Card	Universal	516616586408084	1D5DC2C1E3094	2

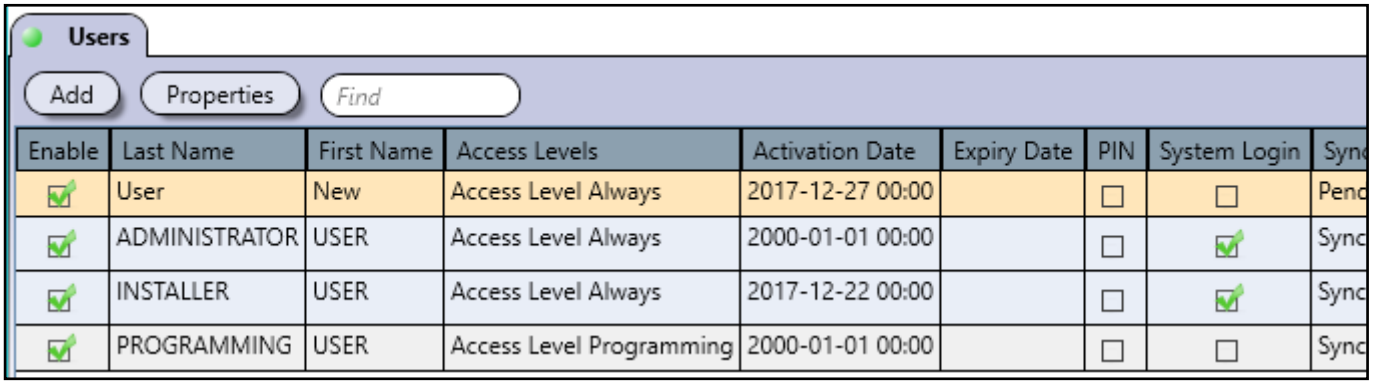
Entering the **Card Number** or **Card Hex Number** is necessary to add cards. .

DATABASE CONFIGURATION

Credentials and **Access Configuration** can be added and modified with an existing module offline or without any module.



Any new entity added or modified in offline mode is highlighted.



Enable	Last Name	First Name	Access Levels	Activation Date	Expiry Date	PIN	System Login	Sync
☑	User	New	Access Level Always	2017-12-27 00:00		☐	☐	Pend
☑	ADMINISTRATOR	USER	Access Level Always	2000-01-01 00:00		☐	☑	Sync
☑	INSTALLER	USER	Access Level Always	2017-12-22 00:00		☐	☑	Sync
☑	PROGRAMMING	USER	Access Level Programming	2000-01-01 00:00		☐	☐	Sync

Logging out and back into the account for normal configuration with the module displays this window:

Click **Yes** to accept these changes and merge them with the account database.

Click **No** and the specific entities will be highlighted and their Synchronization Status will show as "Pending".

If **No** is selected, the entities will remain pending in the database until they are deleted or **Yes** is chosen on the popup window to synchronize them. .

6] Warranty - Terms & Conditions

The "5 Year Warranty" is offered by CDVI exclusively for CDVI products featuring the logo "5 Year Warranty", and supplied by authorized CDVI dealers participating in the offer. You can obtain the address of the local authorized dealer participating in the offer by contacting CDVI or a local CDVI subsidiary. The "5 Year Warranty" is only applicable to hidden defects detected during the lifetime of the product, as defined by the CDVI Group (5 years or 200 000 operations - whichever of the two expires first).

The "5 Year Warranty" conditions shall not modify the sales conditions between CDVI and its customers.

DURATION OF THE OFFER:

- This offer is valid from July 1st 2010; CDVI reserves the right to terminate this offer without prior notice.
- However, any product already registered up to the date of withdrawal of the offer will remain eligible for the "5 Year Warranty".
- The warranty applies only to the available products mentioned in the above statement.

CONDITIONS :

- Hidden defects are guaranteed for an unlimited shelf life (period of time before use).
- The "5 Year Warranty" only applies to products installed by a skilled and experienced personal with the necessary trade qualifications to install according to the highest standards, respecting the standards, instructions and guidelines defined by CDVI and according to the maximum recommended specifications.
- To enable CDVI to determine whether a product is eligible to claim for the "5 Year Warranty", after prior issue of a return of materials authorization number (RMA) by CDVI, the customer must return the product and all of its accessories in the original packaging with a copy of its invoice. The transport fees shall be paid by the customer and the package must be returned to CDVI or to a CDVI authorized repair centre.
- Eligibility for the "5 Year Warranty" cover must be confirmed by CDVI.
- The "5 Year Warranty" only covers the replacement or repair of the parts acknowledged as faulty by CDVI.
- CDVI reserves the right to respect its obligation by replacing the product or the parts acknowledged as faulty by a standard part replacement or by a product or new parts, or by an updated or improved version of the product with identical or similar functionalities.
- In respect of the applicable law, CDVI cannot be held responsible for material or immaterial damages caused to goods or to third parties and as a direct or indirect result of the installation, utilization, product faults or poor functioning of a device.
- The "5 Year Warranty" is non-assignable and non-transferrable.
- The "5 Year Warranty" is limited to the eligible product and is strictly limited to the conditions in effect on the date of purchase by the customer.

NOT COVERED BY THE "5 YEAR WARRANTY":

- Any product which has undergone even the slightest modification or change;
- Any product which has been installed and/or used with any auxiliary device not supplied by CDVI;
- Any product which has been used for demonstrations or display;
- Any product or its elements considered as "consumables" such as fuses, lights and batteries for example;
- Failure or malfunctioning as a result of an accident, poor storage conditions, unsuitable assembly, bad utilization or handling, poor maintenance, unsuitable repair or intervention.
- Any call-out and installation fees (for assembly and dismantling) as well as transport costs (to and from the repair centre) and maintenance fees.

NOTES:

Copyright (C) 2011-2018 CDVI. All rights reserved. ATRIUM Access Control is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this product, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

All other brand and product names are trademarks or registered trademarks of their respective companies.

The information contained in this publication is subject to change without notice.

NOTES:

NOTES:

NOTES:

CDVI
Security to Access

CDVI FRANCE
(Headquarter)
www.cdvi.com

CDVI AMERICAS
[CANADA - USA - LATIN AMERICA]
www.cdvi.ca

CDVI BENELUX
[BELGIUM - NETHERLAND - LUXEMBOURG]
www.cdvibenelux.com

CDVI CHINA

CDVI IBÉRICA
[SPAIN - PORTUGAL]
www.cdviberica.com

CDVI ITALIA
www.cdvi.it

CDVI MAROC
www.cdvi.ma

CDVI POLSKA
www.cdvi.com.pl

CDVI SUISSE
www.cdvi.ch

CDVI NORDIC
[SWEDEN - DENMARK - NORWAY - FINLAND]
www.cdvi.se

CDVI UK
[UNITED KINGDOM - IRELAND]
www.cdvi.co.uk

www.cdvigroup.com

Extranet : CDVI_ASW_IM_13_EN_A4_CMYK

All the information contained within this document (pictures, drawing, features, specifications and dimensions) could be perceptibly different and can be changed without prior notice. Printed in Canada - May 2022