

ADVANCED MANAGEMENT SYSTEM (AMS)

PROGRAMMING AND USER MANUAL



Instructions for first installation and *AMS* operation.

Additional technical details are given in the notes written in smaller characters and indented.

Introduction to the system

The AMS has been designed for managing access of various users to *compartments* of limited size (FIG. 1), but large enough to contain small objects, such as keys, smartphones, medicines, etc.

A single AMS cabinet can have from 12 to 28 compartments, but the system can further be expanded by adding another two cabinets that offer 16 compartments each, hence a total of maximum 60 all managed by the same database.

Each AMS compartment is in continuous communication with the central control unit (situated beneath the touch display). In particularly noisy environments from an electromagnetic point of view, if there are more than 60 compartments, the communication between the most peripheral compartments and the control unit may be problematic. The 60-compartment configuration was specifically designed to guarantee system stability.



FIG. 1: : Module and card/key holder

Access to the compartments is limited by a coded plastic *card* to which keys can be secured with seals. In this way, the cards become *key holders* and the words “card” and “key holder” will be used as synonyms and referred to as *card/key holder* in the explanations in this manual. In this manual, “compartment” means the space in which further “modules” (supplied on request) can be inserted whose access is controlled by the cards/key holders.

The cards/key holders, possibly with the associated keys, are locked in the compartment closing position by the system; they can be taken out (thus allowing access to the compartments) by having the system identify you as authorized *user*.

The AMS tracks all the movements (who has taken/returned and what) recording all the users and cards/key holders in its internal database.

The interface with which the AMS dialogues with the user is a user-friendly touch display (FIG. 2) and a marker (tag/badge) reader (FIG. 3) that uses RFID technology. In order to be read by the system, these tags simply need to be placed on a surface identified by dedicated graphics.



FIG. 2: display touch

FIG. 2: Touch display

The AMS identifies the users with 3 different systems that can be combined (User ID/username + password; tag/badge + password; tag/badge only) in all modes to ensure operating flexibility:



FIG. 3: RFID tag/badge reading panel

- ✗ *username*, number to be entered in the display panel
- ✗ *password*, number to be entered in the display panel
- ✗ *tag/badge* reading

Setting programming

“Programming” means loading to the system the *user/key holder* database and the *relations/authorizations* that tie the two groups together (users and key holders).

Before turning on the AMS, it has to be connected via the RJ45 network port to a computer on which a standard browser for access to a data network is installed. This can be done directly with a point-to-point connection between the computer and the AMS,

use a common network cable terminated with an RJ45 plug

or via a local area network (LAN) to which to connect both the AMS and the computer you want to use for programming.

Turning on the first time

As soon as the power is connected, the AMS will automatically access the network.

The AMS searches for the first available address in the network assigned by the local *DHCP server*. Once it has received the address, the system acquires and uses it until the system is turned off. It is hence a dynamic assignment. When the system is next turned on, the address may be different.

The system can be accessed from the computer in two ways:

1. Entering the address the network attributed to the system directly in the browser window. For example: <http://192.168.1.2> (without the prefix *www*).

The address can be identified by trial and error: in case of direct connection between the PC and the system or in case of a small network, it is the first one not occupied among those available that the LAN *DHCP server* assigns. If necessary, use a common application able to find the addresses in use in the network.

2. **Installing the free service *bonjour* (downloadable from the USB flash drive provided or free of charge at this address http://download.info.apple.com/Mac_OS_X/061-8098.20100603.gthyu/BonjourPSSetup.exe), and then entering the address <http://ams.local> in the browser window (again without the prefix *www*).**

First access

The first time you access, the AMS will, of course, not have any data stored in memory. In the *username* and *password* window, authenticate yourself as preset generic user (enter the code 0001 in both boxes) with both administrator and maintainer rights.

Viro AMS

Username:

Password:

The *main panel* will appear:

Viro AMS	
Main Panel	
Administrator Menu	
Users	+Add
Key holders	+Add
Table of user-key holder relation	
Access time slots (creation and modification)	+Add
Local public holidays (creation and modification)	+Add
Mantainer Menu	
Table of historical operations	
Boxes	+Add
Settings	
System	

From this panel, start entering all the database data.

Entering users

In the *administrator* menu on the *main panel*, click on *Add* next to *Users*.

Clicking on the item *Users*, you can change the data already entered and, in general, make all the desired additions/changes. The first time you access, this is not necessary as nothing has been entered yet.

The following page appears:

Viro AMS		Welcome, FirstUser. Change password / Log out
Home > Users > Add user		
Add user		Back to Users list
First, enter a user ID and password. After pressing the Save button, you'll be able to edit the other user options.		
User ID number:	<input type="text"/>	Required. 4 character length. Only numbers are accepted
Password:	<input type="text"/>	Must be a numeric password of length between 3 and 13.
Password confirmation:	<input type="text"/>	Enter the same password as above, for verification.
		<input type="button" value="Cancel"/> <input type="button" value="Save"/>

Enter the required data that identify the first user following the on-screen instructions.

Warning: only numerical data is accepted.

Click on *Save* to go to the next page where you can enter the information associated with the user.

✔ The user "0002" was added successfully. You may edit it again below.

Change user

[Back to Users list](#)

User ID number:	<input type="text" value="0002"/>		
<small>Required. 4 character length. Only numbers are accepted</small>			
Password:	<input type="password"/>		
Personal info			
First name:	<input type="text"/>		
Last name:	<input type="text"/>		
Email address:	<input type="text"/>		
Phone numbers			
<small>Number</small>	<small>Type</small>	<small>Note</small>	<small>Delete?</small>
+ Add another Phone Number			

- **E-mail address and phone number:** these are important, as they will be used by the system to send the user system notifications and alarms if enabled to receive notifications.

User Type classification

Enable user access
Temporarily disable users that should not or can't access to key-holder cards

The user types of this user. Hold down "Control", or "Command" on a Mac, to select more than one.

User type:

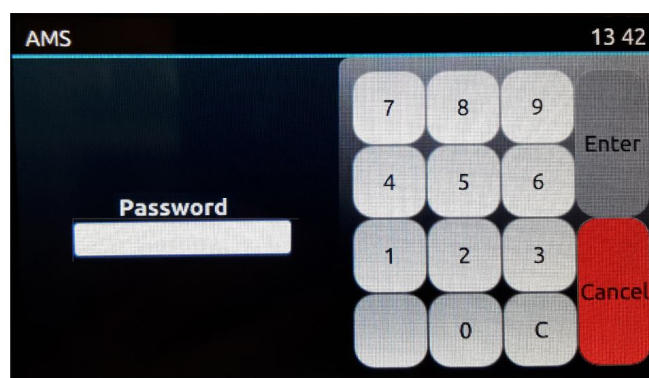
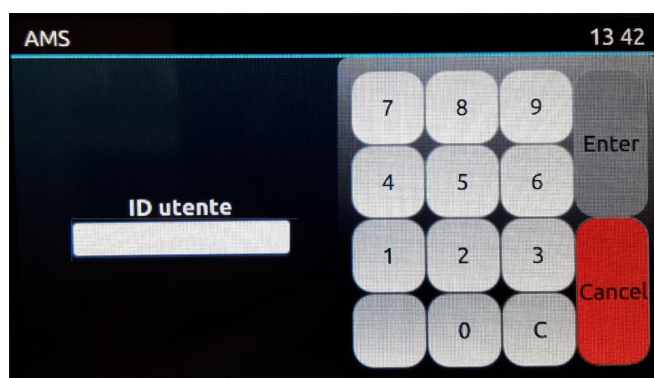
Available user type	Chosen user type
<input type="text" value="Filter"/> <ul style="list-style-type: none"> Administrator Maintainer 	
Choose all	Remove all

- **Enable user access:** unticking this option, you temporarily disable a user without having to delete him or her from the database. That way, it will be very fast to restore this user.
- **User type:** establishes what rights the created user has.
There are 3 types of user:
 - Administrator: may enter/change users, cards/key holders and access/take out rights.
 - Maintainer: may consult the history database table with the list of activities carried out, add/remove modules/compartments and view/change the general system settings.
 - Basic user: may only use the AMS but not access the main panel.

The administrator and maintainer activities are complementary, however, an administrator may also be a maintainer at the same time and vice versa and thus accumulate the functions. The first user 0001/0001 is in fact an administrator and maintainer at the same time.

Panel authentication	
<input checked="" type="checkbox"/>	Enable keypad authentication
<input type="checkbox"/>	Enable password request with badge
Security	
<input type="checkbox"/>	Send system notifications to user e-mail address
<input type="checkbox"/>	Send SMS notifications to user mobile phone
Privacy	
<input checked="" type="checkbox"/>	Public profile <small>If checked, personal details (name and contacts) are visible on touchscreen</small>
RFID badge	
RFID badge ID:	Edit

- **Enable keypad authentication:** in the absence of an RFID identification tag/badge, you can choose whether or not the user may identify himself or herself by entering his or her user ID/password in the panel:



- **Enable password request with tag/badge:** if enabled, the AMS will ask you to enter the access password once the user has been recognized via the tag/badge.
- **Send system notification to user e-mail address:** if enabled, the AMS will send system notifications and any alarms to the e-mail address stored.
- **Send SMS notifications to user mobile phone:** if you have an SMS sending service via the Web, you can enable sending of notifications and any alarms to the phone number stored.
- **Public profile:** if enabled, the AMS shows the data of the current holder of the card/key holder taken. Do not enable it, if you want to protect the privacy of the holder.
- **RFID badge ID:** this function is particularly important. It is used to associate an RFID tag/badge with the user. Click on *Edit* to go to the next page.

Viro AMS Welcome, **FirstUser**. [Change password](#) / [Log out](#)

[Home](#) > [Users](#) > 0002 > [Change RFID badge ID](#)

✔ The user "0002" was changed successfully. You may edit ID tag.

Change RFID badge ID
Put the badge on the reader and then press **Load last badge ID**

Badge ID:

[Load last badge ID](#)
[Save](#)
[Cancel](#)

At this point, place the tag/badge on the reader and hold it there until you hear a confirmation sound (a long beep), then click on the *Load last badge ID* button. In the text box that was initially empty, the tag/badge ID just read will appear, click *Save* to finish the procedure and go back to the Change User page.

Portachiavi

Numero massimo di portachiavi: Numero massimo di diritti di accesso (portachiavi) che possono essere detenuti contemporaneamente da questo utente.

Permessi di prelievo portachiavi

Disabilitare le limitazioni delle fasce orarie
Impostare fasce orarie nel Menu Portachiavi

opzionale

ID impiegato:

Note:

[Annulla](#) [Salva](#)

Key holders

Max key holders: Maximum number of access rights (key holders) that can be held simultaneously by this user.

Key holders picking permissions

Disable limitations of time slots
You can set time slots in Key holders menu

Optional

Employer ID:

Note:

[Cancel](#) [Save](#)

- **Max key holders:** in this box you can enter the maximum number of cards/key holders that a user may take at the same time from all the cards/key holders assigned to him or her.
- **Disable limitations of time slots:** a user might be enabled to take out cards/key holders only in certain time slots (see page 13); tick this option to quickly disable these limitations.

Once you have entered all the data, click on *Save* to finish creation of the first user. The system automatically goes to the *Users* page where you can enter other users by clicking on the *Add user* button and repeating all the operations described above.

Viro AMS Welcome, FirstUser. [Change password](#) / [Log out](#)

[Home](#) > [Users](#)

Select user to change [Add user](#) + [Back to Main Panel](#)

Q

Action: 0 of 4 selected

<input type="checkbox"/>	Username	First name	Last name	Active	Administrator	Maintainer
<input type="checkbox"/>	0001	FirstUser		✔	✔	✔
<input type="checkbox"/>	0002	SecondUser		✔	✘	✘
<input type="checkbox"/>	0003	ThirdUser		✔	✘	✘
<input type="checkbox"/>	0004	FourthUser		✔	✘	✘

4 users

Filter

By active

All

Yes

No


By groups

All

Administrator

Maintainer

For security reasons, after creating your user, you need to delete the default user 0001. The AMS does not allow deleting the user connected at that moment, therefore in order to do so, you need to log out by clicking on the link *Log out* at the top right. Re-access the panel with the data of your user, i.e. one of those created with at least administrator or maintainer access level and delete the user 0001 following the procedure described on page 8.

 **Warning!** If you delete the user *0001/0001* and you then cannot remember the user ID and/or password of the administrator or maintainer created, you will no longer be able to access the system!!! You will have to contact *Viro* technical support, as only they may delete the entire database and reset the initial factory conditions.

Viro AMS Welcome, FirstUser. Change password / Log out

Home > Users

Select user to change Add user + Back to Main Panel

Search

Action: **Delete selected users** Go 1 of 5 selected

Username	First name	Last name	Active	Administrator	Maintainer
<input type="checkbox"/> 0001	FirstUser		✓	✓	✓
<input type="checkbox"/> 0002	SecondUser		✓	✗	✗
<input type="checkbox"/> 0003	ThirdUser		✓	✗	✗
<input type="checkbox"/> 0004	FourthUser		✓	✗	✗
<input checked="" type="checkbox"/> 0005	FifthUser		✓	✗	✗

5 users

Filter

By active
All
Yes
No

By groups
All
Administrator
Maintainer

Deleting users

On the *Users* page, select the user to be deleted by ticking the relative box; from the drop-down menu at the top, select the option *Delete selected users* and click the *Go* button. A second page will open where you will be asked to confirm that you want to delete the user from the database.

Viro AMS Welcome, FirstUser. Change password / Log out

Home > Kmsusers > Users > Delete multiple objects

Are you sure?

Are you sure you want to delete the selected user? All of the following objects and their related items will be deleted:

- User: 0005

Yes, I'm sure

Copying the key holder authorizations from one user to one or more other users

Viro AMS Welcome, FirstUser. Change password / Log out

Home > Users

Select user to change Add user + Back to Main Panel

Search

Action: **Copy key holder permissions to selected users** Go 1 of 4 selected

Username	First name	Last name	Active	Administrator	Maintainer
<input type="checkbox"/> 0001	FirstUser		✓	✓	✓
<input type="checkbox"/> 0002	SecondUser		✓	✗	✗
<input type="checkbox"/> 0003	ThirdUser		✓	✗	✗
<input checked="" type="checkbox"/> 0004	FourthUser		✓	✗	✗

4 users

Filter

By active
All
Yes
No

By groups
All
Administrator
Maintainer

On the *Users* page, select the user/s to whom you want to attribute the authorizations to take/return the cards/key holders already associated with an existing user by ticking the relative box; from the drop-down menu at the top, select the option *Copy key holder permissions to selected users* and click the *Go* button.

Viro AMS Welcome, FirstUser. Change password / Log out

Home

Select the user to copy the key-holder permissions from:

From user: 0001

The permissions will be copied to user(s):

- 0004

Copy

A second page will open where you need to select from the drop-down menu the user from whom you want to copy the authorizations, then confirm by clicking the *Copy* button.

Changing the password

To change the password, access the *main panel* (only the *administrator* and the *maintainer* may change a password). Click on the link *Change password* on the top right bar.

Welcome, **FirstUser**. [Change password](#) / [Log out](#)

The following page will appear where you will be asked to enter the *Old password*.

Viro AMS Welcome, **FirstUser**. [Change password](#) / [Log out](#)

[Home](#) > [Password change](#)

Password change

Please enter your old password, for security's sake, and then enter your new password twice so we can verify you typed it in correctly.

Old password:	<input type="text"/>
New password:	<input type="text"/>
Password (again):	<input type="text"/>

[Change my password](#)

If you cannot remember the old password or the administrator (the only one authorized to change the password) wants to change the password of a generic user (who may not change his or her own password because he or she may not access the *main panel*), a new user has to be created to replace the old one.

In this case, you can create the new user (with the new password), then copy the key holder authorizations of the old user to the new user as described above and, finally, delete the old user (and the old password).

Entering cards/key holders

In the *administrator* menu on the *main panel*, click on *Add* next to *Key holders*.

Clicking on the item *Key holders*, you can change the data already entered and, in general, make all the desired additions/changes. The first time you access, this is not necessary as there is nothing to change yet.

Viro AMS Welcome, **FirstUser**. Change password / Log out

Home > Key holders > Add key holder

Add key holder [Back to Key holders list](#)

Key holder name:

Seal number:
The serial number on the seal

Location:
The box where the key holder card is. If location is blank, the key holder card is not currently available.

Current owner:
The user who holds now the key holder card. If the key holder card is not present in the system, one owner must be defined.

Magnetic code:
Copy the code on the back of the key holder card

Note:

[Change or add access time slots](#)

Access rights management

Users to enable for this key holder	Enable message notification to user	Exclusion of access rights on public holidays	Select access time slots	Delete?
-------------------------------------	-------------------------------------	---	--------------------------	---------

[Add another Access Right](#)

- **Key holder name:** this is the name that will be shown on the display at the time of taking/returning the card/key holder and is the name to be written on the label positioned on the inside of the card/key holder.
You can enter from 1 to 30 alphanumeric characters in this box.
- **Seal number:** you can also associate a serial number to the seal that ties one or more keys to the card/key holder.
- **Location:** this is the number of the compartment where the card/key holder is. If the position is empty, the card/key holder is not present at the moment.
- **Current owner:** this is the user ID/username that identifies the user currently holding the card/key holder.
A position or a holder must always be associated with a card/key holder; for this reason, when you delete a card/key holder from the system, you need to manually associate the user called “viro” as holder.
- **Magnetic code:** this is the code that identifies the card/key holder, which the AMS recognizes by reading a magnetic sequence at the time of insertion into the compartment seat.
The code is unique and is assigned by the manufacturer at the time of physical creation of the card/key holder and is printed on the back of the card/key holder. Nothing stops you from adopting a different external recognition system in order to have greater security. It is however essential that the card/key holder be recorded in the AMS database with the original magnetic code.
- **Note:** space to enter any notes associated with the card/key holder.
- **Change or add access time slots:** this is a link that takes you to the *Access time slots* page. Each user can be disabled to take out cards/key holders outside certain time slots. See page 13 for all the details..

- **Access rights managements:** in this section, you can decide who may take out the card/key holder and limit its use over time. The list is initially empty, therefore, at the time of initialization or changing a card/key holder, click on *Add another access right*.
 - **Users to enable for this key holder:** from this box, select the user you want to enable for taking out the card/key holder from the drop-down menu.
 - **Enable message notification to user:** if this box is selected, notification messages relating to important events (e.g. expiry of the useful time to return the card/key holder) will be sent to the user; the notifications will be sent according to what was defined on the specific page of the user.
 - **Exclusion of access rights on public holidays:** if this box is selected, no one is allowed to take out the card/key holder during holidays. See page 14 for a detailed explanation on how to customize the list of holidays.
 - This procedure is useful to quickly prevent card/key holder movement on the usual business closing days without having to set a certain time slot for each user.
 - **Select access time slots:** selecting the corresponding boxes, you establish in which of the available time slots the card/key holder can be moved. The symbol **+** allows immediately setting a new time slot. See page 13 for the instructions on setting and managing time slots.

Once you have entered all the data, click on *Save* to finish creation of the first card/key holder. The system automatically goes to the *Key holder* page where you can enter other cards/key holders by clicking on the *Add key holder* button and repeating all the operations described above.

Viro AMS
Welcome, **FirstUser**. [Change password](#) / [Log out](#)

Home > Key holders

Select key holder to change

Add key holder **+**
Back to Main Panel

Action: ----- Go	0 of 8 selected		
Key holder name	Location	Current owner	Taken
<input type="checkbox"/> OM	4		
<input type="checkbox"/> ON		0001	July 21, 2016, 5:55 p.m.
<input type="checkbox"/> OO	1		
<input type="checkbox"/> OP	5		
<input type="checkbox"/> OQ		0001	Jan. 1, 2001, 7:21 a.m.
<input type="checkbox"/> OR	7		
<input type="checkbox"/> OS	2		
<input type="checkbox"/> OT	3		

8 key holders

Deleting cards/key holders

Viro AMS
Welcome, **FirstUser**. [Change password](#) / [Log out](#)

Home > Key holders

Select key holder to change

Add key holder +
Back to Main Panel

Action: Delete selected key holders ▾ Go 1 of 8 selected

	Key holder name	Location	Current owner	Taken
<input type="checkbox"/>	OM	4		
<input type="checkbox"/>	ON		0001	July 21, 2016, 5:55 p.m.
<input type="checkbox"/>	OO	1		
<input type="checkbox"/>	OP	5		
<input type="checkbox"/>	OQ		0001	Jan. 1, 2001, 7:21 a.m.
<input type="checkbox"/>	OR	7		
<input type="checkbox"/>	OS	2		
<input checked="" type="checkbox"/>	OT	3		

8 key holders

On the *Key holders* page, select the card/key holder to be deleted by ticking the relative box; from the drop-down menu at the top, select the option *Delete selected key holders* and click the *Go* button. A second page will open where you will be asked to confirm that you want to delete the card/key holder from the database.

Table of user/key holder relations

Viro AMS
Welcome, **FirstUser**. [Change password](#) / [Log out](#)

Home > Table of user-key holder relation

Select table user key to change

Search

Username	First name	Last name	Keys	
0001	FirstUser		OM , ON , OO , OP , OQ , OR , OS , OT	<div style="border-bottom: 1px solid #ccc; padding: 5px;"> Filter </div> <div style="padding: 5px;"> By groups All Administrator Maintainer </div> <div style="padding: 5px;"> By key holder All OM ON OO OP </div>
0002	SecondUser			
0003	ThirdUser			
0004	FourthUser		OM , ON , OO , OP , OQ , OR , OS , OT	

4 table of user-key holder relation

This page gives the administrator an overall picture of the relations between users and key holders associated with them. From this table, through convenient internal connections, you can directly access the page of a user or the page of a card/key holder and check and make changes to the individual items described in the two previous paragraphs. Activating the default filters on the bar on the right, you can view only a selection of elements.

This function is very useful in case of complex databases with many users belonging to different control groups (administrators and maintainers).

Creating and changing access time slots

Viro AMS Welcome, **FirstUser**. [Change password](#) / [Log out](#)

[Home](#) > [Access time slots \(creation and modification\)](#)

Select access time slot to change

[Add access time slot](#) + [Back to Main Panel](#)

Action: [-----] 0 of 3 selected

<input type="checkbox"/>	Time slot day of week	Time slot start time	1 ▲	Time slot end time	2 ▲	Actions
<input type="checkbox"/>	Mon-Fri	7 a.m.		noon		Change Delete
<input type="checkbox"/>	Mon-Fri	noon		6:30 p.m.		Change Delete
<input type="checkbox"/>	Monday	noon		1 p.m.		Change Delete

3 access time slots (creation and modification)

On this page, the administrator can manage the time slots within which each card/key holder can be moved.

It is specified that a card/key holder can always be returned outside the time slot but it cannot be taken out. A late return is however recorded in the history database.

Use *Change* and *Delete* under actions to change/delete the existing time slots.

Clicking on the *Add access time slot* button, a new page will open where you need to select the *Weekday* from the drop-down menu and the *Time slot start time* and *Time slot end time*. Click on *Save* to save and go back to the previous page.

Viro AMS Welcome, **FirstUser**. [Change password](#) / [Log out](#)

[Home](#) > [Access time slots \(creation and modification\)](#) > [Add access time slot](#)

Add access time slot

[Back to Access time slots \(creation and modification\) list](#)

Weekday: [-----] ▼

Time slot start time: [12 ▼] [00 ▼]

Time slot end time: [12 ▼] [00 ▼]

Creating and changing local holidays

Home > Local public holidays (creation and modification)

Select holiday to change

[Add holiday](#) + [Back to Main Panel](#)

Action:	-----	Go	0 of 3 selected
<input type="checkbox"/>	Holiday	Actions	
<input type="checkbox"/>	san evaristo (5 February)	Change	Delete
<input type="checkbox"/>	Tutte le domeniche	Change	Delete
<input type="checkbox"/>	Natale di Gesù (25 December)	Change	Delete
3 local public holidays (creation and modification)			

On this page, the administrator can control the current holidays with the aim of customizing the function *Exclusion of access rights on public holidays* as described above.

Use *Change* and *Delete* under actions to change/delete the existing holidays.

In order to provide maximum flexibility, you can also change the characteristics of default holidays, e.g. Christmas. Clicking on the *Add holiday* button, a new page will open where you can enter the characteristics of the new customized holiday: *Name*, *Day* and *Month*.

Home > Kmskeys > Local public holidays (creation and modification) > Add holiday

Add holiday

Predefined:	userdefined
Name:	<input type="text"/>
Day:	-----
Month:	-----
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Main Panel

Mantainer Menu	
Table of historical operations	
Boxes	 Add
Settings	
System	

The following paragraphs describe the operations that may only be carried out by the maintainer.

Table of historical operations

Viro AMS
Welcome, **FirstUser**. [Change password](#) / [Log out](#)

Home > Table of historical operations

Select table of historical operations to change [Back to Main Panel](#)

Action:

<input type="checkbox"/> Action time	User	Action	Object of action	Event type description
<input type="checkbox"/> Sept. 22, 2016, 10:45 a.m.	0001	Deletion	0005	
<input type="checkbox"/> Sept. 22, 2016, 10:41 a.m.	0001	Change	0005	Changed first_name and is_staff.
<input type="checkbox"/> Sept. 22, 2016, 10:41 a.m.	0001	Addition	0005	
<input type="checkbox"/> Sept. 22, 2016, 10:39 a.m.	0001	Change	0004	Changed first_name and is_staff.
<input type="checkbox"/> Sept. 22, 2016, 10:39 a.m.	0001	Addition	0004	
<input type="checkbox"/> Sept. 22, 2016, 10:38 a.m.	0001	Change	0003	Changed first_name and is_staff.
<input type="checkbox"/> Sept. 22, 2016, 10:38 a.m.	0001	Addition	0003	
<input type="checkbox"/> Sept. 22, 2016, 10:38 a.m.	0001	Change	0002	Changed first_name and is_staff.
<input type="checkbox"/> Sept. 22, 2016, 10:38 a.m.	0001	Change	0001	Changed first_name. Changed tag for kms user "0001".
<input type="checkbox"/> Sept. 22, 2016, 10:37 a.m.	0001	Change	0002	Changed is_staff.
<input type="checkbox"/> Sept. 22, 2016, 10:33 a.m.	0001	Change	0002	Changed is_staff.
<input type="checkbox"/> Sept. 22, 2016, 10:23 a.m.	0001	Addition	0002	
<input type="checkbox"/> Sept. 22, 2016, 10 a.m.	0001	Login	0001	
<input type="checkbox"/> Sept. 22, 2016, 9:58 a.m.	0001	Logout	0001	
<input type="checkbox"/> Sept. 22, 2016, 9:55 a.m.	0001	Login	0001	
<input type="checkbox"/> Sept. 22, 2016, 9:54 a.m.	0001	Logout	0001	

Filter

By action time

- Any date
- Today
- Past 7 days
- This month
- This year

By Action

- All
- Addition
- Change
- Deletion
- Login
- Logout
- Login failed
- Panel Login
- Panel Login failed
- Take
- Take failed
- Give back
- Give back failed
- Alarm
- Expired notify

By group

- All
- Administrator
- Maintainer

This table shows all the events recorded in the internal database, such as alarms and accesses to the AMS. Activating the default filters on the bar on the right, you can view only a selection of elements. You can download the entire database in CSV format by selecting the relative options from the drop-down menu and clicking on the *Go* button.

Viro AMS			Welcome, FirstUser. Change password / Log out	
Home > Boxes				
Select box to change				Add box +
ID	Enable	Actions		
1	✓	Disable	Check	
2	✓	Disable	Check	
3	✓	Disable	Check	
4	✓	Disable	Check	
5	✓	Disable	Check	
6	✗	Enable	Program	

The AMS internally identifies each compartment with a number, which in the table is indicated in the *ID* column.

You can see whether or not a compartment is enabled in the *Enable* column.

The *Actions* column shows what action you can take for the compartment.

- **Disable button:** allows disabling the compartment so that it is no longer seen by the AMS as present and will not be shown on the display as destination if the user wants to return a card/key holder.
This command is useful in case of a compartment fault if you do not want to remove all the compartments downstream.
- **Check button:** allows easily identifying the position of the compartment on the noticeboard by turning on the compartment LED.
This command is useful as the compartment ID number is unknown to the maintainer (it is only indicated in the ID column).
- **Remove button:** this command is available only for the last compartment entered, because it is the first that has to be deleted and physically removed in case of a reduction in the number of compartments, as the compartment modules are connected to each other in succession from the first to the last.
- **Program button:** this command allows marking the compartment with the *ID* number of the row selected. This should be done when readjusting the compartments or when you are inserting a new module. The operation is very easy, even if requiring a direct intervention on the electronic card of the module, which must be programmed.

Programming the electronic card of the module

You need to short-circuit the two programming contacts (simply by touching them with the tip of a metal screwdriver) located on the rear of the card (FIG. 4). The compartment LED will come on yellow/orange to indicate that you have entered programming.

If the LED comes on red, it means that the module has already been programmed, in which case just enable the compartment.

At this point, click on the *Program* button in the same row as the desired ID to mark the compartment with the chosen ID. The compartment LED will go off. The AMS will ask you to confirm; click on *Yes* to finish programming

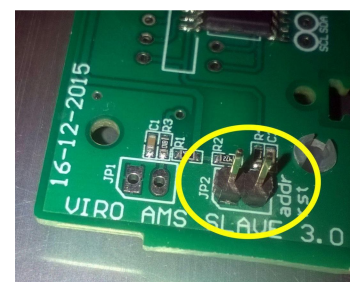


FIG. 4: Programming contacts

Viro AMS Welcome, **FirstUser**. [Change password](#) / [Log out](#)

Home > Settings

Change settings Back to Main Panel

Language

Language:

Security

Login errors count limit:

Login errors time limit in sec.:

Number of consecutive vibrations to raise an alarm:

Period in sec. to calculate consecutive vibrations:

Lock time in sec. for login faults and alarms:

Activate relay 1 on alarms

Activate relay 2 on alarms

Expired key-holder alarm delay in minutes:

On this page, the maintainer can change the standard operating parameters:

- **Language:** the software/display language is available in Italian and English.
- **Login errors count limit:** this is the maximum number of errors allowed during login before the system goes into locked state.
- **Login errors time limit in sec.:** you can set a time limit (in seconds) for any code entry attempts, that way limiting the possibility of unauthorized access attempts.
- **Number of consecutive vibrations to rise an alarm / Period in sec. to calculate consecutive vibrations:** the preset values were intentionally chosen to prevent false alarms. They can be customized according to noticeboard fastening.
- **Lock time in sec. for login faults and alarms:** the AMS may go into locked state both after a certain number of incorrect login attempts and when it goes into alarm. The duration of the locked state can be changed at will by the maintainer.
- **Activate relay1/relay2:** the AMS has already been set up to be connected to an external alarm system; there are two relays on the electronic card, which if enabled by ticking these boxes, activate at certain times: relay1 activates in case of tampering and break-in attempts; relay2 activates when e-mail/SMS notifications are sent.
- **Expired key-holder alarm delay in minutes:** if a key holder is returned with a delay greater than that set in this box, a delay notification is sent (to users enabled to receive notifications) at the time the key holder is returned.
- The parameters of your e-mail server have to be set in the *Server mail* section. In order to receive notifications also via SMS, you need to have a messaging service via Web active.

System management

[Back to Main Panel](#)

System commands

Shutdown for maintenance or transportation:


Restore the original configuration:

Set system clock

Time:

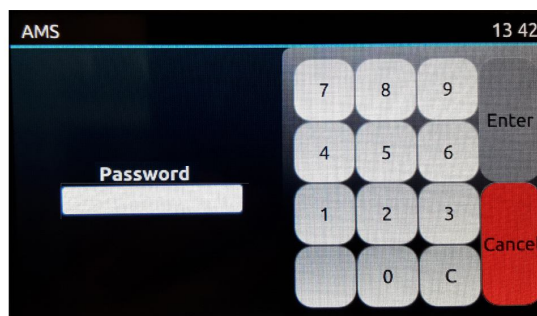
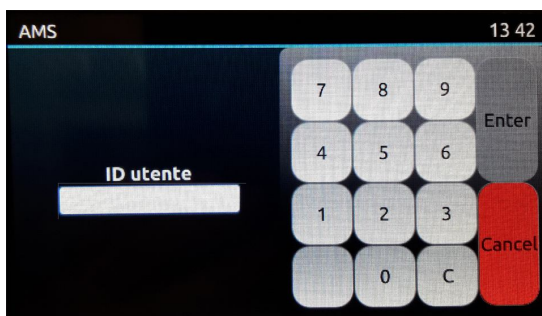
Date:

On this page, the maintainer can carry out some general operations on the system:

- **Shut down button:** clicking on this button, the AMS will turn off. To turn it back on, disconnect and reconnect the power.
- **Reset button:**  **Warning!** Clicking this button, all the settings will be reset; use it only in extreme cases.
- **Clock setting:** allows manually entering the date and time. It is essential to keep the date and time updated so that the database is consistent. If the AMS is connected to the Internet by means of the RJ45 network port on the front panel, the update will occur automatically.

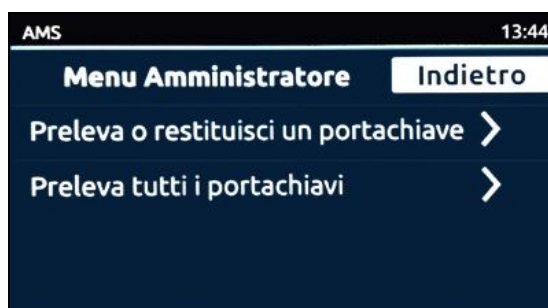
All the data update and card/key holder movement operations are recorded in the database. Only by initially entering the correct date and time can the event correctly be positioned in the time scale.

Taking/returning cards/key holders



In order to access the compartments, you first have to authenticate yourself by tapping the touch display and entering the *user ID and password* or by placing the tag/badge on the RFID tag reader. You can also enable the *password* request after the tag/badge has been recognized.

After authenticating, following screen will appear on the touch display to the **administrator** only:



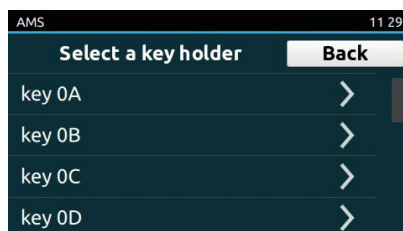
Toccando il simbolo > corrispondente alla seconda voce *Preleva tutti i portachiavi* è possibile aprire in sequenza tutti i vani velocemente e prelevare tutti i portachiavi di cui si possiedono i diritti di prelievo.

Toccando il simbolo > corrispondente alla prima voce *Preleva o restituisci un portachiave* si accede all'elenco dei portachiavi.

Tapping the arrow > corresponding to the description *Take all keyholders* it is possible to open all the compartments quickly and take all the key-holders that have the right to be withdrawn.

After authenticating yourself, your personal page will appear on the touch display with the list of cards/key holders the administrator has chosen to make available to you.

It may also be that you may not take all the key holders at the same time, but only a certain number set by the administrator.



Tapping and holding the central area of the screen, scroll up or down until the name of the card/key holder you want to take/return appears.

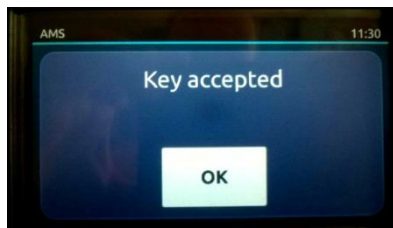
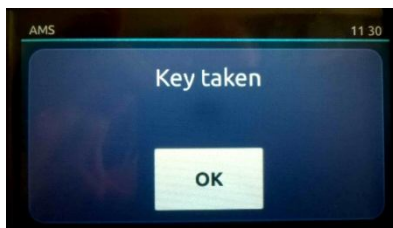
You cannot sweep across the touch display. Only minimal pressure of your finger is required for the contact to be recognized.

Now lift your finger and tap the arrow > corresponding to the card/key holder chosen. The next page will appear informing you whether or not you can use the card/key holder.

If the card/key holder has already been taken by another user, the message *Key holder not available* will be shown; if no compartment is available for return, it will be signalled with a message.

The motorized mechanism that holds the card/key holder locked opens waiting for the card/key holder to be taken or returned. You have 10 seconds to take/return the card/key holder during which the compartment LED flashes waiting for you to complete the operation.

When you take or return the card/key holder, the AMS signals this action with one of the two following messages:



The event is recorded in the internal database, which now knows when the card/key holder was taken/returned and who took/returned it.

In case of unauthorized return (a different card/key holder, incomplete insertion, etc.), the AMS signals it with dedicated messages

Movement alarm

If a prowler attempts to remove (or noticeably moves) the AMS, the system responds with an alarm message and sends dedicated messages to the users enabled to receive notifications.

Tampering alarm



All the AMS connections are protected by a metal door with key lock. Every time the door is opened, it is recorded in the database and the system also sends alarm messages to the users enabled to receive notifications.

Connections



Power supply: connect the transformer supplied.

Pipe wrench: turn clockwise to open, counterclockwise to close. Se in posizione aperta è possibile collegarsi alla bacheca attraverso il cavo di rete, via LAN o direttamente con un PC.

If in the open position it is possible to connect to system via network cable, LAN or directly with a PC.

Button ON/OFF

Ethernet network RJ-45 connector: connect the network cable (not supplied).

Backup battery in the event of a power failure

In the event of a power failure, an internal battery will keep the AMS powered. The AMS automatically shuts down if the power failure lasts more than 1 hour in order to safeguard database integrity. When the power is restored, the AMS will automatically turn on again.

NB: If after turning on again, the AMS is reconnected to the network, the date and time will not have to be updated.

If, on the other hand, the system is not connected to the network, the date and time will have to be updated each time it is turned off.

This condition is indicated on the display by a light at the top right with the symbol of a flashing power plug. In case of an emergency, the system can be powered by connecting directly to the 12V power jack. It is advisable to replace the internal buffer battery every 2 years (supplied by Viro as spare part).