USER MANUAL

E-CONNECT

Management, centralization and supervision system service

Interface for intrusion detection control units

1 GENERALS

e-Connect is a cloud platform for the centralization, management and remote supervision of the intrusion detection, fire detection, CCTV systems and home and building automation applications based on EL.MO. products.
This manual describes in detail the management and supervision interface for intrusion detection control panels and how to access it via web browser.

1.1 Summary of the functions of the "intrusion" interface

- Monitoring of intrusion detection systems based on EL.MO. control panels from PC, tablet and smartphone.
- Protected Server structure with proprietary protocol encrypted data sending.
- The user can control the system remotely (perform arming/disarming, see the events log, exclude/include the inputs, enable/disable the outputs).
- Temperature management (for Villeggio, Pregio, Proxima series and Hercola control units).
- Management of the system components from graphic maps.
- Multiple clients management.

1.2 For the end-users

Through e-Connect, users can manage the fire alarm system of their home remotely, even from a smartphone or tablet, quickly dealing with any communication from the system.
e-Connect also allows to have most of the maintenance and configuration change interventions performed through remote assistance sessions, in order to reduce intervention times and remove the necessity of on-site interventions.

⚠ *Attention: see the limitations detailed in chapter 17 p. 12.*

1.3 Compatibility

Control unit	Connectivity
VILLEGGIO / VILLEGGIO NG-TRX series	LAN GPRS Wi-Fi (for control units with firmware v.8 or higher)

Control unit	Connectivity
Pregio series	LAN for Pregio control units with metal case Wi-Fi for PREGIO500 GPRS
QHUBO series	GPRS Wi-Fi (QHUBOWF only)
Proxima series	LAN GPRS
Hercola	GPRS Wi-Fi (for control units with board 99002388 or above)
ETRG2 series	LAN
Titania series (with firmware 5.2.0 or above)	LAN
NET832, NET9	LAN
ETR48 (with firmware 2.6 or above)	LAN
TACÓRA (with firmware 5.2 or higher)	GPRS LAN

If you use Internet Explorer to access the platform, ensure that the version is 10 or higher.

2 ACCOUNTS CREATION

Users managed by their installer will receive the domain name (e.g. installer_name) and the login credentials from the installer himself after accepting specific contractual terms and conditions.

3 USER LOGIN

Via your web browser, log into the e-Connect portal through the address provided by the installer.
If the installer has created a user account, all your systems are generally available for you to view by logging in via the address https://connect.elmospa.com/client. Otherwise, with a system account, you can log in through the address https://connect.elmospa.com/installer_name using the credentials provided by the installer.
Note: we suggest that you save the page address to the bookmarks for ease of use.
– enter user name and password defined in the registration procedure.
Note: in case you have forgotten the password, click on "Forgot Password?" and follow the steps.
– select **Remember Me** to speed up subsequent logins
– press **LOGIN**
At the first access, the user will be asked to read and accept all service conditions.
Check all the checkboxes to accept and press **OK**.

4 "SYSTEMS" PAGE

This page comes up, after login, if the user has been assigned more than one system.
As many lines as there are systems assigned to the user appear on the display, along with a "Export data" button to download a file in .xlsx format containing information on all the systems associated with the account, which is placed in the browser's Download folder.
For each of the systems' lines, you can view:

▼ **SYSTEM**
System name given by the installer.

▼ **DESCRIPTION**
The model of the fire or intrusion control unit in the system.

▼ **ARMING STATUS**
System on/off status.
= Sector on
= Sector off

= Unknown

▼ **ANOMALIES**

Shows any faults and/or anomalies.

= Fault/anomaly detected

= No fault/anomaly

= Unknown

▼ **REMOTE CONN.**

= Takes you to the page of the relevant system.

▼ **CONNECTION**

Indicates whether the system is connected to the internet.

= System connected

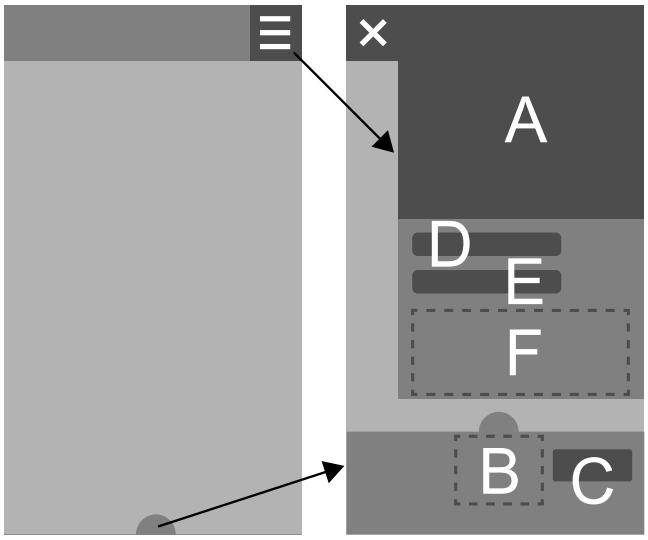
= System disconnected

Please note: this manual is applicable only for intrusion-detection systems; for fire detection systems, please refer to the relevant manual.

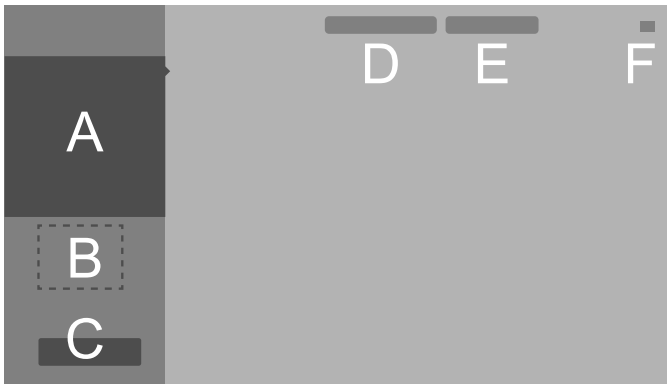
5 INTERFACE

This chapter describes the menus and other elements that you can access from each screen of an e-Connect system. Examples in the following chapters refer to the interface for wide screens.

On small screens (e.g. smartphone)



On wide screens (e.g. PC)



A - Navigation menu
B - Control panel information
C - "Login" button
D - Quick link to other accounts
E - Change language
F - Account options

5.1 Navigation menu

Each menu item corresponds to a different page.
Each single page is described in a dedicated chapter.

5.2 Control panel information

The following items are listed:
- Control panel connection status.
- Control panel model and firmware version.
- Control panel IP address.
- Last connection start date.

5.3 "Login" button

The button only appears if the control panel is connected and it has the following states:

▼ **Login**
No user is authenticated.
Click to log in.
The user ID is the progressive number that identifies the different users that may access control panel.
The user code is the personal secret code assigned to that ID.

▼ **Busy**
Another user has logged in or a remote assistance session through e-Connect is in progress.
It is not possible to authenticate.

▼ **Exit**
Click to exit and make the control panel available to other users.

If no operations are carried out, or if you close the browser page without logging out, the control panel will be disconnected after a short while.
There is no need to log into the control panel to control home automation.

5.4 "Supervision" button

It allows the user to quickly provide the installer with the authorisation to access his system for diagnostic purposes.
Click on the button to provide (ENABLED) or remove (DISABLED) the authorisation for supervision.

5.5 Quick link to other accounts

This menu allows to link other accounts already registered in the e-Connect server and to quickly switch from one to another without exiting the e-Connect platform.
When you select a new account, a window will appear to request login credentials.
The new identified account will then appear in the list of the available accounts.
The list shows the accounts of the control panels registered in the e-Connect server and linked to one's account.
To remove the account of a control panel that you do not want to display anymore, click on the red "×".

5.6 Change language

This drop-down menu allows to choose the display language.

5.7 Account options

Use this menu to set the most common options for management of e-Connect accounts.
Some functions, marked by a star, are not available to users managed by an installer since the installer himself manages them.

▼ **Systems**
Takes you to the Systems page (chap. 4 *p. 2*).

▼ **Connect to DVR**
This option is only available if the installer has configured the function for the user.
It allows to open the login page of the DVR/NVR installed at the user.

▼ **Redirect to panel IP**
This entry only appears if the control panel is connected.

It allows you to access other active services connected to the same network as the control panel, using the same IP address.

For example, it is possible to connect to the login page of a DVR or of a domotics service.

▼ **Change Password**

Use this function to change the password for logging in to e-Connect.

The new password will be valid from the next login.

▼ **Change Email**

Use this function to change the e-mail address that e-Connect writes to.

▼ **Change user code**

This option is only available if the installer has configured the function for the user.

Allows you to change the user code, which is required to operate the control unit.

▼ **Change user name**

This option is only available if the installer has configured the function for the user.

Allows you to change the user name in the control unit.

▼ **Enable system block**

The option is only available with QHUBO series control units.

When enabled, the control unit will be set to system lock mode.

▼ ***Read Panel Data**

Use this function to acquire to e-Connect any changes made by the installer in the names of inputs, outputs, areas, users and so on.

We suggest that you read control panel data after each control panel configuration maintenance session.

The operation requires approx. 1 min and is affected by connection speed.

▼ ***Delete History**

Use this function to clear the events from the "History" page.

The password is the same as the one used to access e-Connect.

The history log saved inside the control panel will not be deleted.

▼ ***Delete Account**

You cannot delete an existing account while you are connected to the control panel.

⚠ *We advise against using this function. Cancellation of an existing account is an irreversible event: you will not be able to use the e-Connect service anymore. Installer intervention will be required to restore the service.*

▼ ***Generate Key**

Generate a new registration key: this procedure is necessary in case you need to replace the control panel.

⚠ *We advise against using this function. If you generate a new key, the previous one will be deleted from the server and the control panel that uses the previous key will no longer be able to connect to the e-Connect account, but it will keep consuming data traffic upon each connection attempt. At the same time, the new control panel will not be able to connect until the new code is inserted. Key insertion and removal require installer intervention.*

▼ **Settings → Supervision**

Disabled locally (QHUBO control units only): the installer cannot modify system configuration, neither remotely nor in local connection.

Disabled: the installer cannot modify system configuration remotely (default option).

Enabled: the installer is allowed to access system configuration and perform remote assistance for control panels connected via e-Connect.

Enabled until 24:00: supervision is enabled; it will be disabled at midnight.

▼ **Settings → Default Page**

Choose which page will be first displayed when opening software interface.

▼ **Settings → Extended area info on status page**

Flagging this option will provide a more detailed visualization of the area states in the "Status" page.

▼ **Settings → Time zone**

Set proper time zone.

⚠ *This function is not available for users that belong to installer domains.*

In case there are VISIO2K sensors, other options will appear in **Settings** page. See paragraph 14.1 *p. 12*.

▼ **Exit**

Log out.

6 "STATUS" PAGE

6.1 Control panel status

From left to right:

1 Zone status
2 Anomalies
3 Alarm
4 Tamper

The following icons provide information on control panel status.
They replicate the control unit indicating LEDs.

▼ **Zone status**

ON: no zones with alarm/tamper alarm events. The unit can be armed.

OFF: at least one zone not assigned to the exit path is alarmed.

Blinking: the unit is disarmed and at least one zone assigned to the exit path signals an anomaly event.

– click to open "Inputs" page

For older control units, the indication might be different:

Green: battery OK.
Yellow blinking: battery anomaly.

▼ **Anomalies**

ON: no anomaly.

Blinking: presence of anomalies.

⚠ *If control unit LED has been programmed to be off when there are no anomalies, the icon will comply with this rule.*

– click to open "Faults" page

For older control units, the indication might be different:

Green: the mains voltage is present.
Yellow blinking: mains anomaly.

▼ **Alarm**

OFF: no alarm events.

ON: alarm presence.

Blinking: alarm memory presence.

The number at top right indicates the total number of alarmed zones.

– click to open "History" page

▼ **Tamper**

OFF: no tampering.

ON: tamper alarm presence.

Blinking: tamper memory presence.

The number at top right indicates the total number of tampering zones.

– click to open "History" page

6.2 Additional information

The three central panes provide additional information.

▼ **Recent events**
Last 5 events stored in the memory of the control panel.

– select "View All" to open "History" page

▼ **Alarmed Inputs**
Details on currently alarmed zones.

▼ **Active Outputs**
Details on currently active outputs.

6.3 Area status

The panel on bottom shows the state of the sectors of each area in use.
- Sector armed. Click to disarm.
- Sector disarmed. Click to arm.

If "Extended area info on status page" option is enabled, the armability state of the sector will be displayed too.

Total arming and disarming

A bar shows the state of the system:

Partial arming.
At least one sector is armed, but not all.

Total disarming.
All sectors are disarmed.
To arm all sectors at the same time, click on the right side of the bar or on the **Arm all** writing.

Total arming.
All sectors are armed.
To disarm all sectors at the same time, click on the left side of the bar or on the **Disarm all** writing.

⚠ *The user code is required if the user has not logged into the control unit yet.*

7 "ANOMALIES" PAGE

This page shows the ongoing anomalies or their memories.
At the side of each anomaly, an icon shows:
- Anomaly presence.
- Anomaly memory.

8 "HISTORY" PAGE

This page shows the events stored in the control panel.

▼ **Export history**
Click to export the server's history log to an unformatted .txt file.

▼ **Server Time**
Hour at which the event occurred, measured by the e-Connect server.

▼ **Panel time**
Hour at which the event occurred, communicated by the control panel.

▼ **Description**
Event description, communicated by the control panel.

▼ **Details**
Additional event details, communicated by the control panel.

▼ **Sectors**
Sectors involved.

▼ **ID**

Progressive event number in the log.

The icon indicates that a VISIO2K detector has generated an image upon the occurrence of this event.
Click on the icon to open the image.
For details, please see 14 *p. 11*.

Icon available for the installer who enters the user's control unit interface.
Click on the icon to schedule a maintenance session for the corresponding event, creating a memo.
See the installer manual for further information.

To clear event log, see chapter 5.7 *p. 4*.
When viewing the page from a Smartphone:
- + sign indicates that there are additional details to be displayed: click it to get the expanded view;
- - indicates that it is possible to collapse the details.

9 "AREAS" PAGE

This screen shows the status of the control unit areas.
Note: if "Extended area info on status page" option is enabled, the information included in this page will appear on status page.

▼ **Area N**

Name of the sector of the area N.
The zones associated to the sector (which are also reported on "Inputs" page) are displayed.

▼ **Status**

- - Sector armed. Click to disarm.
- - Sector disarmed. Click to arm.
- - Sector armed in Max Security mode (this command is not available via e-Connect).

▼ **Armable**

- - This sector can be armed. No anomaly.
- - This sector cannot be armed.

Global commands

▼ **Arm all**

Click to arm all the sectors of the areas pertaining to the user.

▼ **Disarm all**

Click to disarm all the sectors of the areas pertaining to the user.

⚠ *The user code is required if the user has not logged into the control unit yet.*

When viewing the page from a Smartphone:
- + sign indicates that there are additional details to be displayed: click it to get the expanded view;
- - indicates that it is possible to collapse the details.

10 "INPUTS" PAGE

This page shows control unit zone status.

▼ **Number**

Number of the zone corresponding to the BrowserOne numbering.

▼ **Input**

Zone name.

▼ **Status**

- **Idle** - Zone in idle condition.
- **Alarm** - Zone in alarm or tampering condition.
- **Bypassed** - Excluded zone.
- **Idle** - idle zone with at least one alarm memory.

Alarm - Alarm of a zone belonging to a disarmed sector.

It is possible to include/exclude a single zone by clicking on its status button.
This operation requires the user code.

▼ **Memory**

– - No alarm or tamper memories for this zone.

! - Presence of at least one alarm or tamper memory for this zone.

When viewing the page from a Smartphone:

- + sign indicates that there are additional details to be displayed: click it to get the expanded view;
- - indicates that it is possible to collapse the details.

11 "DOMOTICS" PAGE

This page shows the status of the outputs managed by the control unit.

▼ **Number**

Number of the output corresponding to the BrowserOne numbering.

▼ **Output**

Output name.

▼ **Status**

Disabled - Output disabled.

Enabled - Output enabled.

Controlling outputs remotely

The outputs command depends on the control unit model; the command may be given for each output separately and only with outputs programmed by software with "Manual control" property.
Click on a button on the "Status" column to change the status of the relative output (enabled/disabled).
User code is normally required to perform this operation. Nevertheless, control unit programming allows to specify, for each single output, whether to require or not user authentication. If the output can be enabled without authentication, no user code will be required.

12 "MAPS" PAGE

This page shows system zone and output positions and their status.
Click on a sector or an output to change its status.

13 "TEMPERATURE" PAGE

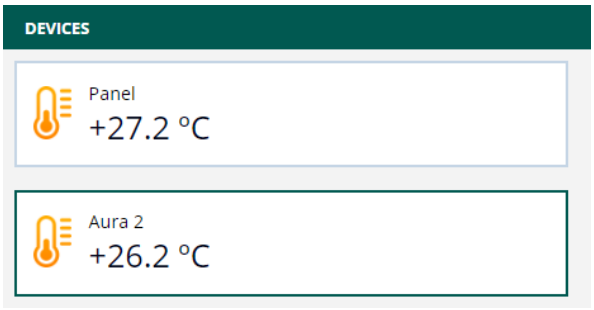
Page to manage temperature:

- visualisation of the temperature detected (by the onboard or the external sensor);
- management of control-unit-integrated chronothermostat (only for VILLEGGIO and HERCOLA series control units);
- management of chronothermostats controlled by AURA keypads.

⚠ *The installer has to enable the user to manage the thermostats. See installer manual.*

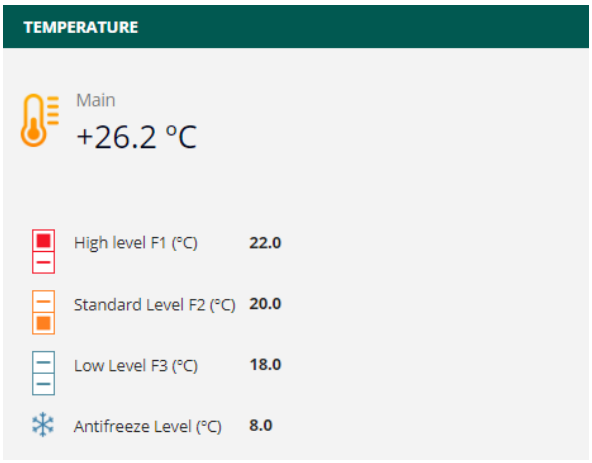
Devices

Select the device pertaining to the chronothermostat to control.



Temperature

It shows the temperature detected by the device, the set high, medium, low and antifreeze thresholds.



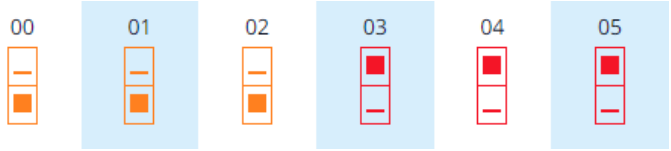
Mode

Chronothermostat management panel.

- **Enabled daily**
  Select to enable daily mode: an unique program will be applied to all days.
  Press + - to manually change the programmed temperature (in steps of 0.1°C).
  The set temperature will be applied until the following scheduled threshold change, then it will be reset to the programmed value.
- **Enabled weekly**
  Select to enable weekly mode: a specific program will be applied to each day.
  Press + - to manually change the programmed temperature (in steps of 0.1°C).
  The set temperature will be applied until the following scheduled threshold change, then it will be reset to the programmed value.
- **Manual temperature setting**
  Select to enable temperature manual setting.
  Press + - to set the temperature.
  The change will be applied to current time interval and to all following intervals until it is changed again.
- **OFF**
  Select to keep the chronothermostat off.
- **Antifreeze**
  Select to set the chronothermostat to antifreeze mode.

Once done, click on "Save" to save device settings.
As an alternative, it is possible to propagate the changes to all the devices at the same time: this can be useful, for example, to program the switch to antifreeze function for all the chronothermostats included in the system.
Click to "Set all" to propagate the changes to all devices.

Daily program



Chronothermostat configuration panel.
Click on **Set** to open **Chronothermostat** page.
Use + - buttons to set the temperature levels.
Click multiple times on a time slot to change the applied level.

- **Read**
  Click to read the current configuration of the chronothermostat related to the selected device.

▼ **Write**

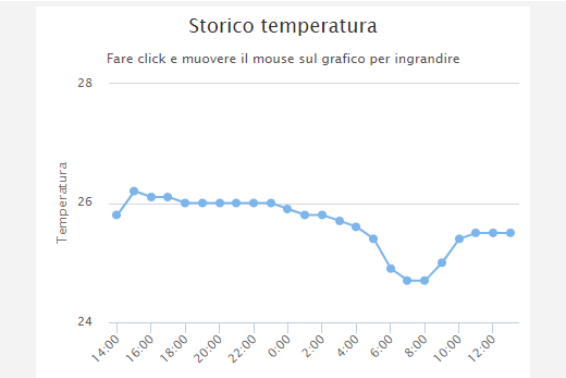
Click to write the chronothermostat configuration just set to the selected device.

This operation requires the user code.

▼ **Write all**

Click to propagate the chronothermostat configuration just set to all devices.

Graph



It shows the temperature trend over time.

Move the mouse pointer over a point to read the temperature detected at that time.

The graph may refer to the main or the secondary sensor and be limited to the last 24 hours, to the last week or to the last month: use the buttons to change it.

Click on the graph, drag and release to zoom on a specific time interval.

14 "INSTAVISION" PAGE

This section allows displaying the images captured by the VISIO2K detectors connected to the user's account.

Note: see the technical manual of VISIO2K for details about its operation.

The area above of the page shows VISIO2K devices learned to the control unit zones.

The preview of the last image downloaded will be displayed for each device.

To capture real time snapshots from the device: click on **Snapshot** button to start capturing an image.

The icon indicates that an image is being captured.

Click on an image to view its details:

- event type: event that triggered the image creation or "snapshot".
- source: device that has captured the image
- time: date and time of image creation

Buttons function:

▼ **Delete**

Click to delete the image.

▼ **Save**

Click to save the image to the PC.

▼ **Exit**

Click to close the window.

To the images (or image areas) a frame of various colours and size will be added according to the triggering event:

Event	Frame size	Frame colour	
		"day" mode (colour)	"night" mode (B/W)
Alarm	areas where motion is detected	green	white
Tamper	whole image	red	white
Masking	whole image	yellow	grey
Snapshot	no frame	-	-

If tracking mode is on, in case of alarm the image will show a line of points (blue in "day" mode, black in "night" mode)

corresponding to the movement detected.
All operations on images (view, save, delete) will be saved: click on **Access History** to open images log.
Each operation will be stored in this list for 6 months.

14.1 VISIO2K privacy settings

The **Settings** menu allows configuring the management of the images captured by VISIO2K.
To access it:

– click on icon  on top right (F)
– click on **Settings**

In detail, in this menu are available:

▼ **Allow installer to access InstaVision content**
If selected, the installer will have access to such user's images.

▼ **Keep InstaVision content for**
Select an interval from drop-down menu (from 1 to 180 days).
All images will be saved for such interval (default 180 days); after that time, images will be deleted automatically.

When finished, select **Save** to save changes and exit.

15 "TIME SCHEDULER" PAGE

Page to manage time scheduler:
- display of the programs set in the control unit;
- enabling/suspending and changing the schedule of user-manageable programs;
- request for overtime for programs that are not user-manageable (only for PROXIMA and SUPERIA series control units).

⚠ *The installer has to enable the user to manage the time scheduler. See installer manual.*

▼ **Program**
The name of the program set during the control unit configuration.

▼ **Activation time**
The time the program runs. In user-manageable programs, a clock icon appears. Click the icon to change the program's run time.

▼ **Status**

Active Program enabled. Click to suspend.

Suspended Program disabled. Click to enable.

Active Program activated and cannot be deactivated by the user.

16 PERIODIC MAINTENANCE

The service is periodically submitted to scheduled maintenance, usually on the first Wednesday of each month.
The maintenance session duration is kept as limited in time as possible; nevertheless, during such sessions it is not possible the access the service: a specific display message signals the state of unavailability, including also an estimate of the maintenance session duration.
Maintenance sessions may also be performed at other times due to binding technical necessities.

17 LIMITS OF THE SERVICE VIA GPRS

The e-Connect service, when enabled via GPRS, can suffer some limitations.
- Less speed: slower response time for the web interface operations and for the e-Connect remote assistance.
- Activation of the GSM dialler: the activation of the GSM dialler for voice calls or for remote assistance sessions might disconnect the control panel from the e-Connect service. The connection will be automatically restored at the end of the calls.
- Effect on SMS, GSM remote assistance and voice call services: the operation of these services is not guaranteed when the e-Connect connection is active; especially if an user is logged to the web interface. When the e-Connect connection

is active, it is recommended to use the e-Connect web interface to check your intrusion detection control panel.

18 LIMITS OF THE SERVICE WITH THE WI-FI MODULE

The e-Connect service, when enabled via a router connected to a MDWIFI module, can suffer of slower response times due to the latency of the used transmission services.
This slowness also shows when loading the e-Connect page from a PC, Tablet or Smartphone.

User manual - December 2024 edition **090040863**

EL.MO. Spa - Via Pontarola, 70 - 35011 Campodarsego (PD) - Italy
Ph. +39 049.9203333 - Fax +39 049.9200306 - Help Desk +39 049.9200426 - www.elmospa.com - international@elmospa.com