

USE AND MAINTENANCE MANUAL



UVIX USER MANUAL



Contents

1.	Introduction	3
1.1	Structure of the UVIX	3
1.2	Wireless connection	3
1.2.1	Wireless connection example	4
1.2.2	Wireless connection with gateway	5
1.3	USB connection	5
1.3.1	USB connection example	5
1.4	Coexistence of the types of connection	5
1.5	Camozzi USB Gateway	6
1.5.1	File	6
1.5.2	Tools	6
1.5.3	About	9
1.5.4	Commands	9
1.5.5	Open COMs	9
1.5.6	Main Page	9
1.5.7	Wi-Fi Configuration	9
1.5.8	Mapping	10
1.5.9	Data exchange	10
1.6	Detailed analysis	10
1.6.1	Communication between the UVIX components	10
1.6.2	Wireless connection to the FEP of a Camozzi device	10
1.6.3	Gateway USB	10
1.6.4	Database	11
1.6.5	Web Service	11
1.6.6	Web App	11
1.6.7	Detailed structure of the UVIX	11
1.7	Modification of communication parameters	12
1.7.1	Modification of communication parameters between FEP / Web Service and Web App	12
1.7.2	Modification of communication parameters between Web App and FEP	12
1.7.3	Web App port modification	12
2.	Installation	13
3.	Web App	16
3.1	Login	16
3.2	Navigating the web app	16
3.2.1	Top bar	17
	Notifications	17
	Setup	17
	Session/account management	19
	About	19
3.2.2	Left bar	21
3.3	User registry management	22
3.4	Device management	22
3.5	Slave management	23
3.6	Variables	23
3.7	Alarms	24
3.8	Commands	24
3.9	Set-up parameters configuration	26
	Reset	27
	Save on pc	28
	Send	28
	Save on device	28
3.10	Exclusive Device Management	28
4.	MqttCustomer messages sent by UVIX Web Service Ver 1.0.1	29
4.1	Enabling MqttCustomer messages	29
4.1.1	MqttOn	29
4.1.2	MqttConnectionHost	29
4.1.3	MqttConnectionPort	29
4.1.4	MqttClientId	29
4.1.5	MqttTopicPrefix	29
4.1.6	MqttReadClock	29
4.1.7	Example	29
4.2	Printed messages	30
4.2.1	Message fields	30
4.2.2	Topics	30
4.2.3	Examples	30
4.2.4	How to receive MQTT messages	30
4.2.5	Description of the variables	30
5.	Main problems and solutions	31
5.1	The Camozzi device does not communicate via USB	31
5.2	The Camozzi device does not communicate via wireless	31
5.3	The Camozzi USB gateway software does not send data to the FEP	32
5.4	Login failed on the UVIX web page	33
5.5	The web page is not visible	34
5.6	Not included in the previous	34

1. Introduction

The UVIX environment allows the user to monitor and configure all new generation Camozzi devices that support connection to it. This system has been implemented with a "web based" architecture in order to access information through a simple browser, with the possibility of installing it on a single PC/gateway/server and being able to access it from any device within the same network. Monitoring consists in the display of all the device parameters, whether they concern the operation, health status and parameterization. Archiving of this data is not performed and remains the responsibility of the user if necessary. The devices can be connected to the UVIX in two ways: wireless connection or USB connection. For more details on the type of connection available, refer to the manual of the specific product.

For the commissioning of this system it is necessary to have:

- At least one Camozzi device that supports connection to the UVIX: it is the device that can be monitored and parameterized.
- An access point (in case you want to use the wireless connection): has the task of establishing the wireless connection.
- A PC on which to install the UVIX environment: for the installation and configuration procedure, refer to the dedicated chapters.
- A gateway on which to install the UVIX environment: this performs the same tasks as the access point and the PC which will therefore no longer be needed.

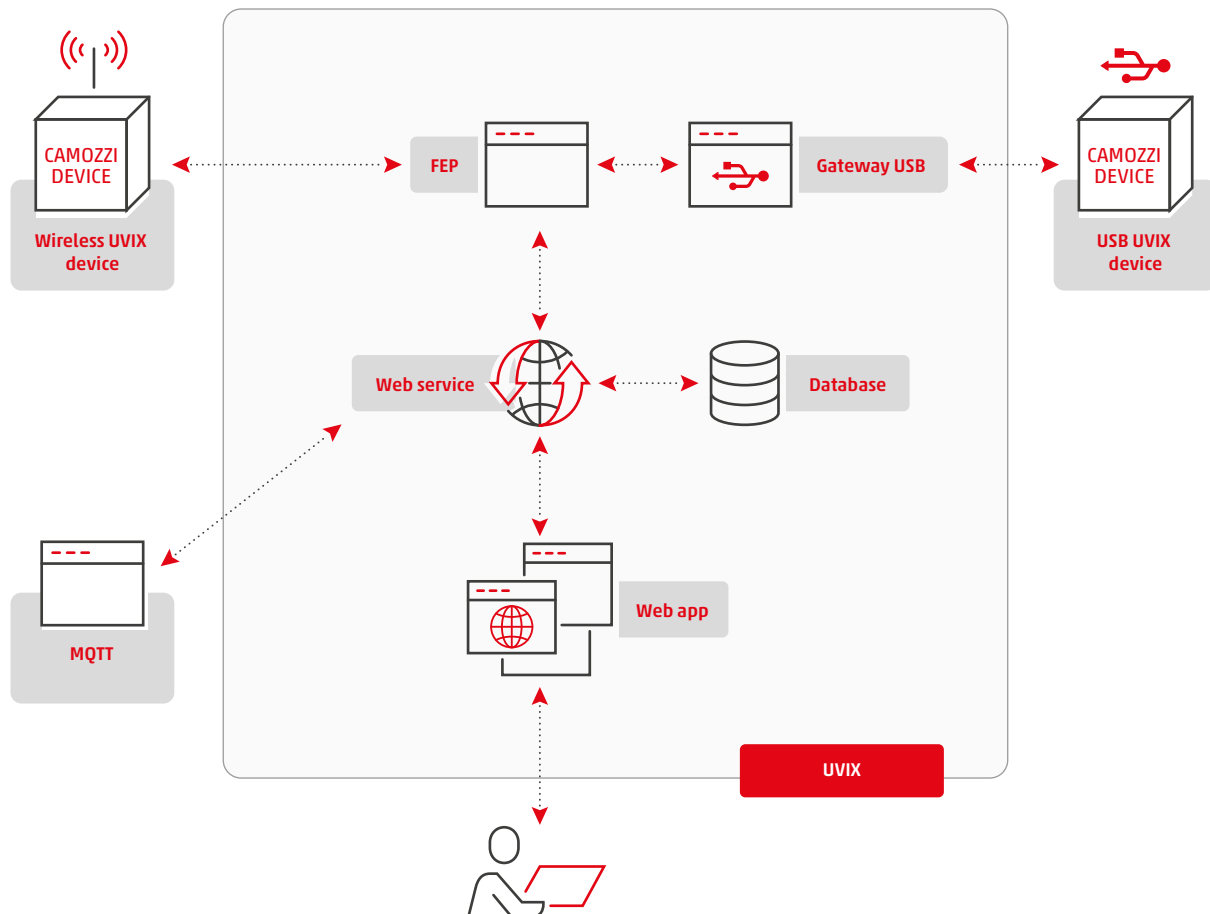
The main types of connection will be described in the following chapters.

1.1 Structure of the UVIX

The UVIX software comprises:

- Gateway-USB: manages the transmission via a USB connection, and is an optional component that is only necessary for devices that have this type of connection.
- FEP: manages the communication with the devices, in the case of USB connection the data passes through the Gateway-USB while in the case of wireless connection it arrives directly.

- Web Service: manages the communication between the various components.
- Database: contains the current data from devices and all configuration parameters available to the WebApp.
- Web App: manages the interface between the user and the UVIX system.



1.2 Wireless connection

In this configuration, the device connects via wireless connection to an access point which in turn communicates, via a LAN cable or wireless, with a PC where the UVIX is installed.

For the system to work properly, the access point that generates the network must be set with an SSID, a password and an IP address (the choice is arbitrary).

The PC must be set-up with a static IP address that must belong to the access point network.

The following parameters must be set on the Camozzi devices to be connected to the network:

- Network SSID: ID of the network to which the device is to connect.
- Network Password: password of the network to which the device is to connect.
- Destination IP address: IP address of the PC where the UVIX is installed and with which the device must communicate.

The IP address of the device, on the other hand, must be assigned via DHCP.

1.2.1 Wireless connection example

The default configuration of Camozzi devices foresees the following values:

- SSID: camozziUVIX.
- Password: camozziUVIX.
- IP Address: 192.168.0.5.

For simplicity of implementation, the network will be set up in a manner consistent with these data so as not to have to modify them.

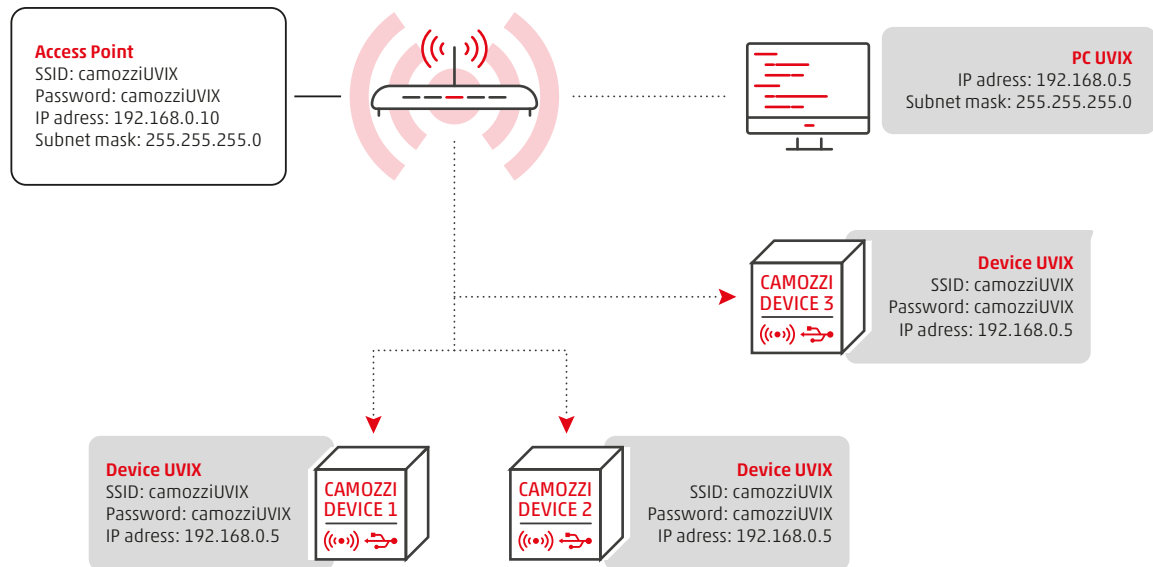
The access point is configured with the following information:

- SSID: camozziUVIX.
- Password: camozziUVIX.
- IP Address: 192.168.0.10.
- Subnet mask: 255.255.255.0.

The IP address and Subnet mask in this case have been set as static but could also be dynamic.

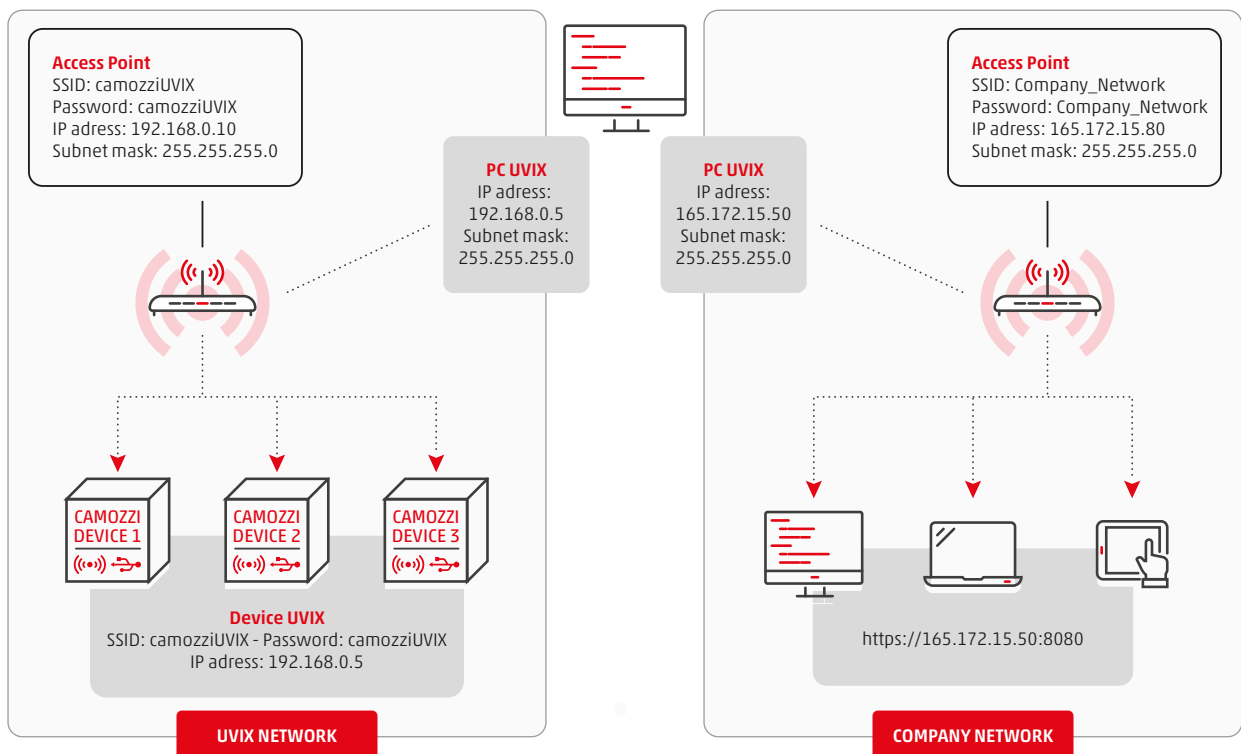
The PC on which the UVIX was installed (now called PC_UVIX) must have the same static IP address that was configured on the devices:

- IP Address: 192.168.0.5.
- Subnet mask: 255.255.255.0.



The system configured in this way is fully operational, but it is a closed system, that is, it allows the configuration and monitoring of any device that connects to the "camozziUVIX" network exclusively from PC_UVIX.

To overcome this limit, it is possible to enter the PC_UVIX into a network, a company one for example, so that any device entered in that network can directly access the UVIX and therefore it is not necessary to repeat the installation and configuration on each workstation.



1.2.2 Wireless connection with gateway

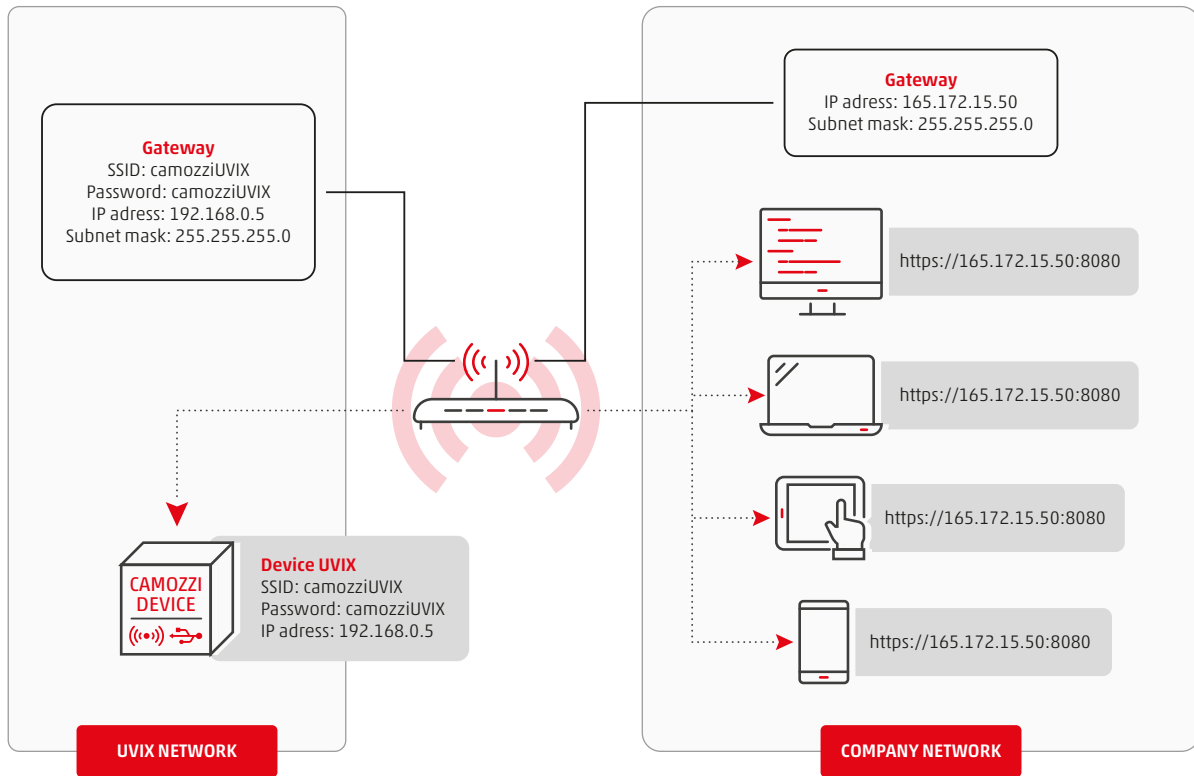
If a gateway is available, the entire configuration between the access point and PC_UVIX is not necessary and it is sufficient to set the information of the destination network.

Using the information from the previous example, in this case the gateway will be configured as follows:

- SSID: camozziUVIX.
- Password: camozziUVIX.
- IP Address: 192.168.0.5.
- Subnet mask: 255.255.255.0.

The other devices will keep the same configuration.

Similarly to that previous, it is possible to enter the gateway thus configured within a network in order to make the UVIX accessible to any PC in the same network.



1.3 USB connection

In this configuration, the Camozzi devices, if they support the connection to the UVIX and are equipped with a USB connector, can be monitored and configured without installing wireless communication.

To take advantage of this type of connection, it is necessary to run the Gateway-USB (start-up will be in background) present within the UVIX installation (for more details on installation and configuration, refer to the dedicated chapters).

1.3.1 USB connection example

Assume you have a PC (from now called PC_UVIX) with UVIX and Gateway-USB correctly installed and started.

The Camozzi devices that will connect via USB cable to the PC_UVIX can be monitored and configured on the same web page, accessible from the browser, used by the terminals connected via wireless.

Similarly to the type of wireless connection, the PC_UVIX, or a gateway, could be entered within a network so that any device within the same network can access the UVIX.

1.4 Coexistence of the types of connection

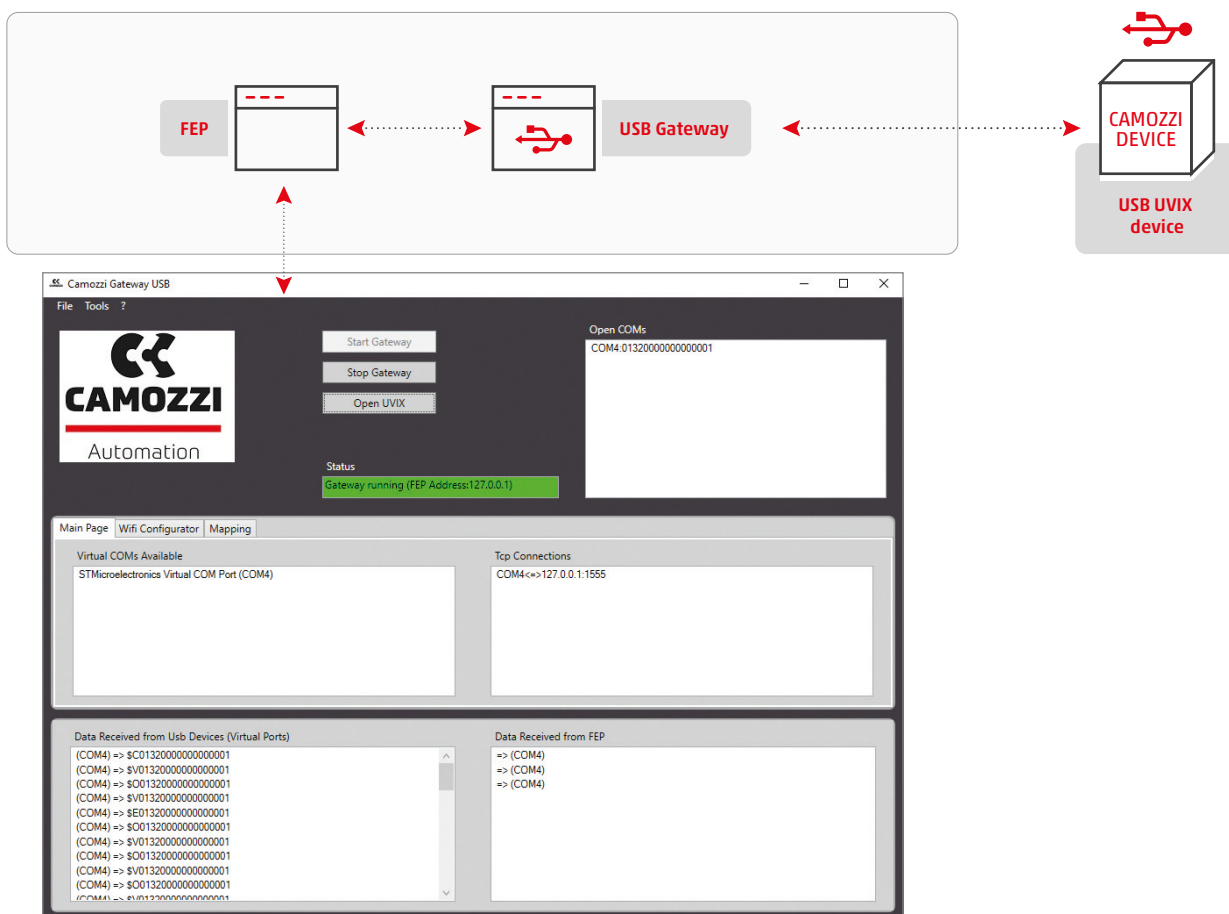
The two types of connection can coexist perfectly; in fact, the type of connection is completely transparent in the web page opened by the browser.

Therefore, since the Camozzi device is connected via wireless or USB connection to the PC (or gateway) where the UVIX has been installed, each terminal within the network will see this device without distinction.

1.5 Camozzi USB Gateway

As anticipated in the chapter on the UVIX structure, the Camozzi USB Gateway software manages the communication between a Camozzi device and the FEP via a USB connection. All features and possible configurations will be described below.

In order to work correctly, the USB gateway must always be running, for this reason it can be left active in background, and its icon is shown in the taskbar.



1.5.1 File

- **"Hide"**
Move the execution of the USB Gateway in background.
- **"Exit"**
Close the USB Gateway.

1.5.2 Tools

• Settings

This tool allows to:

1. Set the address of the FEP. In the event that the USB Gateway and FEP are installed on the same PC, it is possible to set the default local address using the "Set as localhost" command.

2. Set the web page address to access UVIX. If the default one is used, it can be set automatically using the quick command "Set default URI".

• Device Upgrade

This tool allows to update a Camozzi device equipped with a USB connection.

Before starting the update procedure make sure you have: device, power cable, USB cable and firmware.

For all information regarding cables and/or connectors, refer to the manual of the product you wish to update.

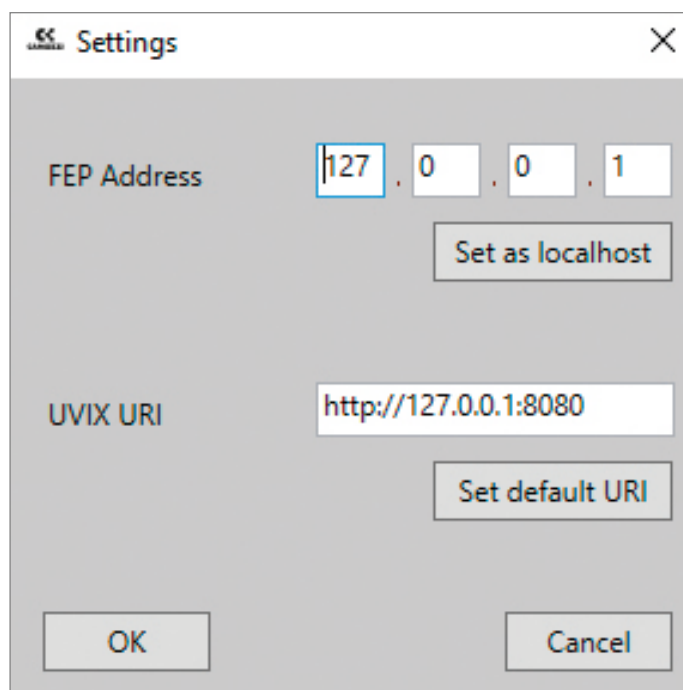
The firmware is a file with extension .hex and is unique for each product, make sure to have the correct file and if necessary contact Camozzi assistance.

To make the update available, Camozzi devices are equipped with two firmware:

Application firmware: manages all product functions such as communication with the other modules and with the PLC.

Firmware bootloader: this verifies that the application firmware is the correct one and manages the updating phase.

The firmware update only includes the application firmware and it is sufficient to have the Camozzi USB Gateway software.



To perform the upgrade, proceed as follows:

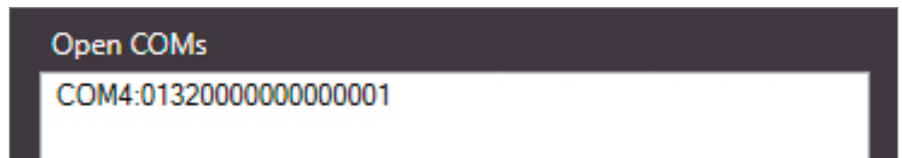
1. Turn on the device and connect to it via the USB cable.
2. Start the Camozzi USB Gateway software.



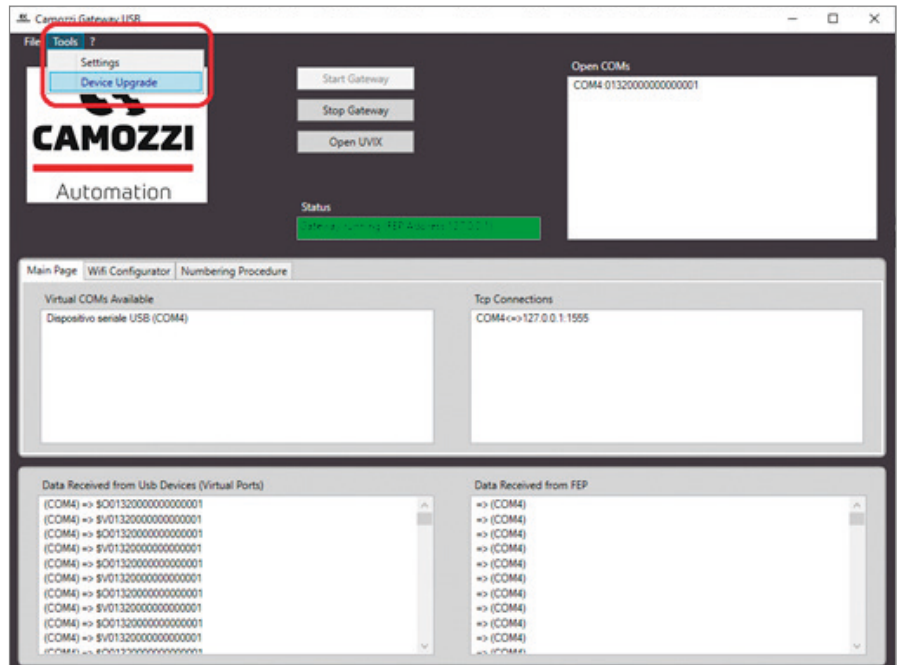
If the window does not appear, check that it is not running in background, and if necessary click on the icon in the bottom right bar.



If the device is connected correctly, the virtual COM and the univocal serial number will appear in the upper right section.

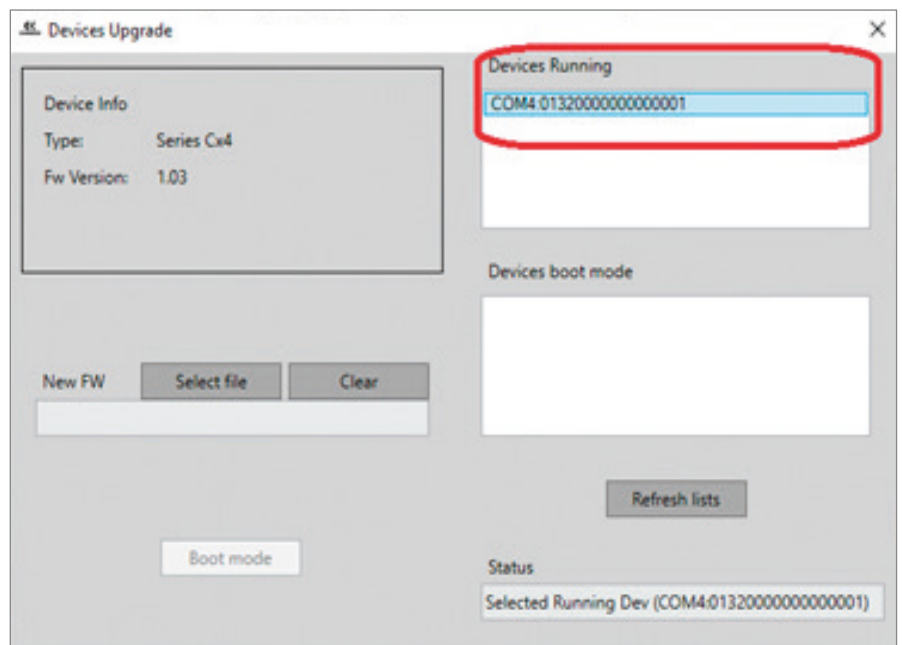


3. Start the "Device Upgrade" tool

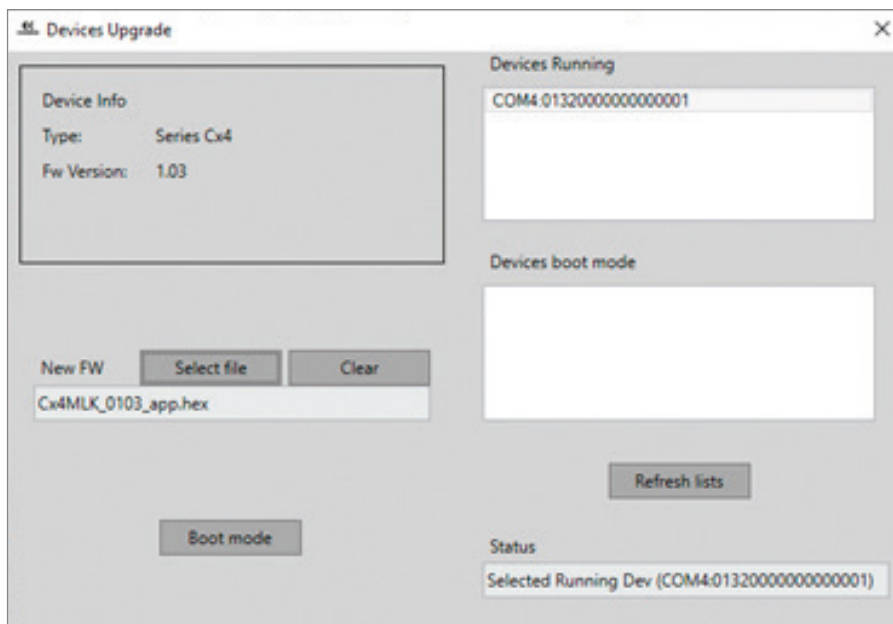


4. Once the tool has been started, select the device you want to upgrade in the "Devices Running" section, if it is not visible, try to upgrade the list using the "Refresh lists" command.

The "Device Info" section indicates the family of the selected product and the current version of the application firmware.

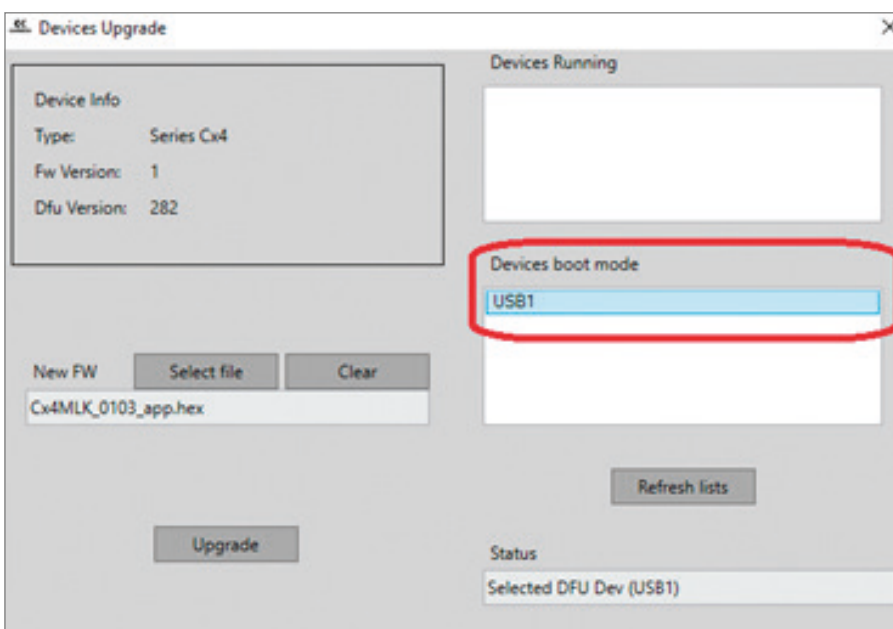


5. Select the new firmware using the "Select file" command, contact Camozzi assistance for more information. If the selected file is correct the "Boot mode" command will become available.

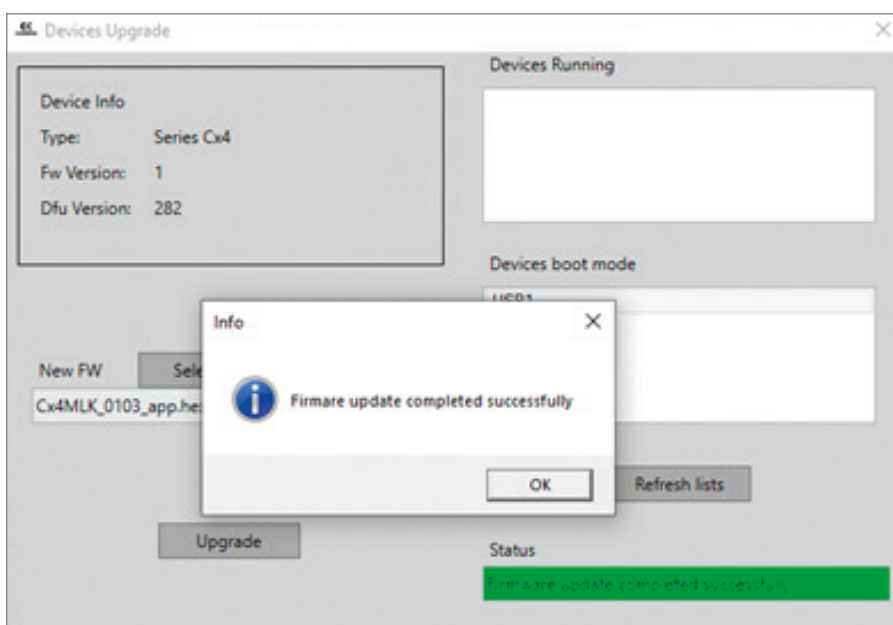


6. Using the "Boot mode" command, send the device to the reprogramming status. This phase is irreversible therefore it is recommended to carry it out only if you have the new firmware to load.

7. If the previous phase is successful, a new device indicated with "USB1" will be available in the "Devices boot mode" list, if it is not visible try to upgrade the list using the "Refresh lists" command. Selecting the device in the "Device Info" section, the product family, the bootloader firmware version and the version of the libraries used will be displayed.

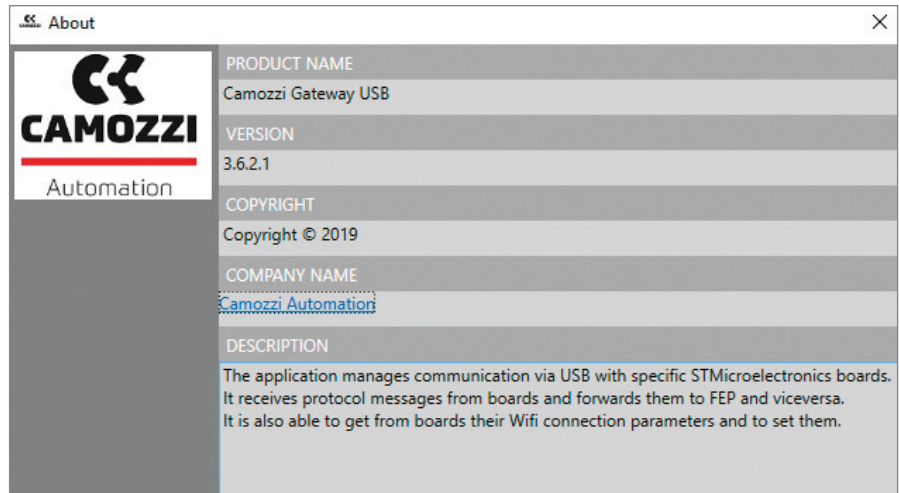


8. Select the device and click on the "Upgrade" command. If the upgrade ends successfully, a confirmation message will appear. Click "OK" and close the tool.



1.5.3 About

Clicking on "?" and "About" a window is displayed containing all the information relating to the software.

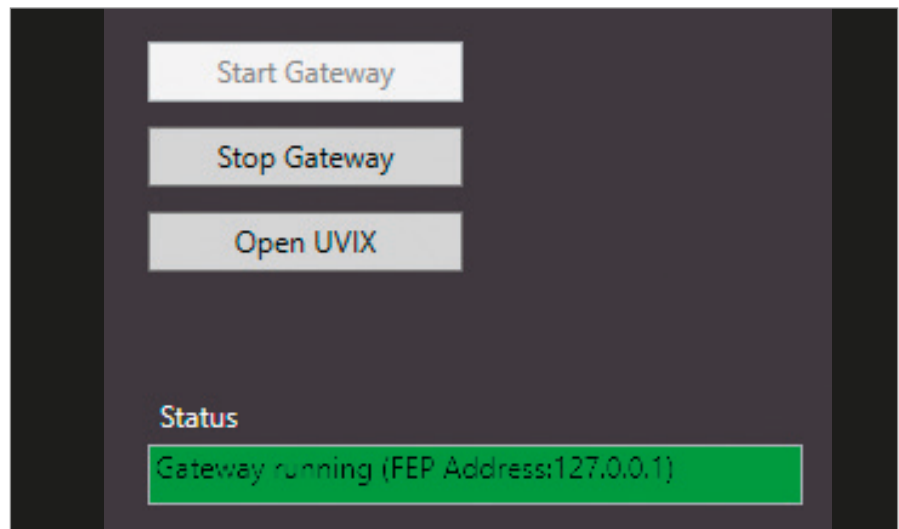


1.5.4 Commands

A series of commands are present in the upper central part:

- Start Gateway: allows to start communication between the USB device and FEP, by default the communication is active at start-up.
- Stop Gateway: allows to block communication between the USB device and FEP.
- Open UVIX: opens the UVIX web page via the default browser.

The status of the USB Gateway can be verified in the lower section at the "Open UVIX" command.



1.5.5 Open COMs

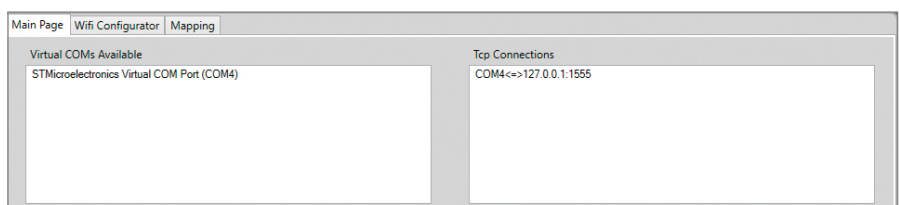
A list of all the Camozzi devices currently connected is present in the upper right part, indicated with the COM assigned by the operating system followed by the univocal serial number of the device.



1.5.6 Main Page

There are three pages in the central part of the software, the first is called "Main Page" and contains information on the data traffic managed by the USB Gateway.

- Virtual COMs Available: indicates the virtual COMs available, as seen by the operating system.
- Tcp Connections: indicates the active communications between COM and FEP, indicating the IP address and port for the latter.

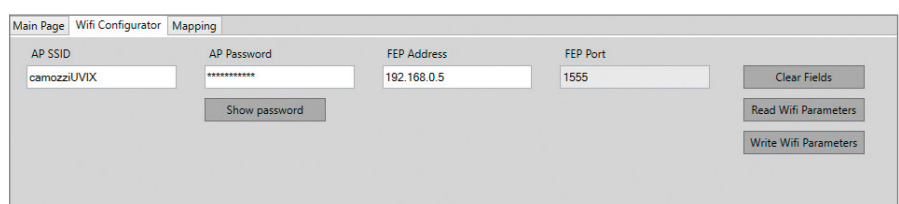


1.5.7 Wi-Fi Configuration

This page allows to configure the parameters for the wireless connection.

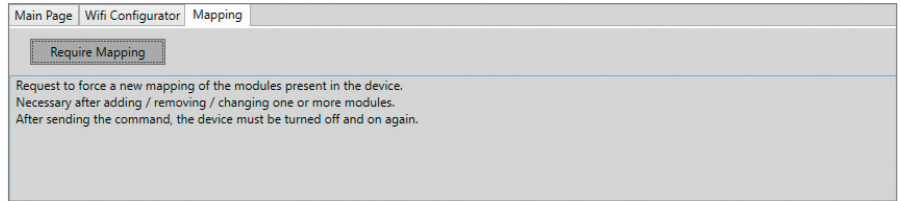
- AP SSID: SSID of the network to which the device must connect.
- AP Password: password of the network to which the device must connect.
- FEP Address: IP address of the FEP to which the device must send data.
- FEP Port: port of the FEP to which the device must send data.

There are three commands next to these fields to clean the fields (without writing them on the device), to read or write the parameters. If the connected device does not have a wireless connection, these parameters will not be available.



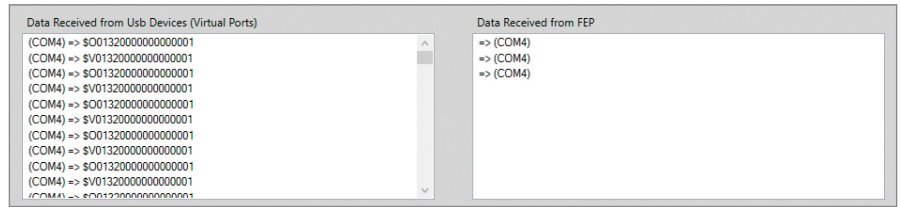
1.5.8 Mapping

This page allows to send the mapping command to a Camozzi device, this command is only available for devices that require it. For further information on mapping, refer to the manual of the Camozzi device.



1.5.9 Data exchange

In the lower part, the data passing through the USB Gateway are indicated in greater detail.
 - Data Received from Usb Devices (Virtual Ports): shows the data arriving from the device stating the COM, the type of data (\$ C, \$ V etc.) and the serial number of the device.
 - Data Received from FEP: indicates the data arriving from the FEP stating the destination COM.



1.6 Detailed analysis

In the following chapter, the various components of UVIX and their interconnections will be reported in greater detail.

The information contained in this chapter is useful in cases such as the installation of UVIX on the company server or changes to the communication ports.

1.6.1 Communication between UVIX components

All UVIX components use the TCP/IP protocol, communication takes place through the establishment of a socket that requires to indicate the IP addresses and the port.
 In the most common case, all UVIX components are installed on the same machine, therefore the IP address is common to all components.
 To ensure correct communication, the ports used by UVIX must not be used by other components or blocked by firewalls.
 In the specific case of Windows operating systems, during installation the necessary permissions are automatically entered on the system firewall, permissions are not automatically added to any third-party firewalls that remain the responsibility of the user.

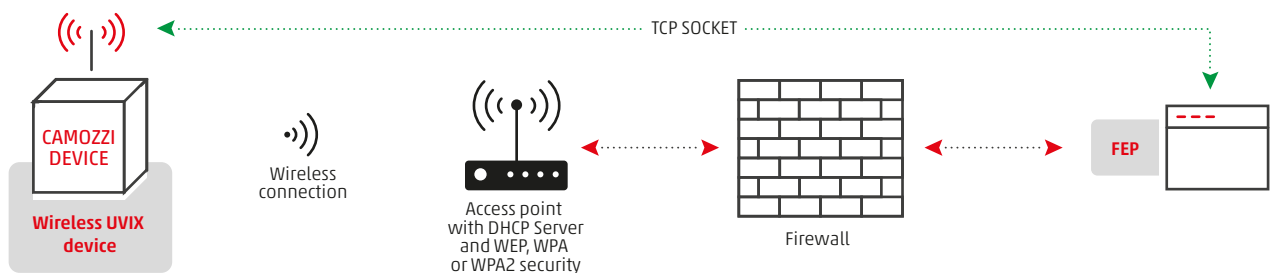
The table below shows the ports used by the UVIX components.

Communicating components	Communication port	Editable
Device - FEP	1555	No
FEP - Web Service	5000	Yes
Web Service - Web App		
Web App - FEP	12345	
Web App - Users	8080 Windows / 80 Linux	

1.6.2 Connection of a Camozzi device to the FEP with wireless connection

When turned on, a generic Camozzi device, if equipped with a wireless connection, attempts to connect to the network that has been indicated (by default SSID: camozziUVIX and password: camozziUVIX). Once the credentials have been verified (the password supports WEP, WPA or WPA2 security standards), the device requests an IP address which must be assigned by a DHCP server.

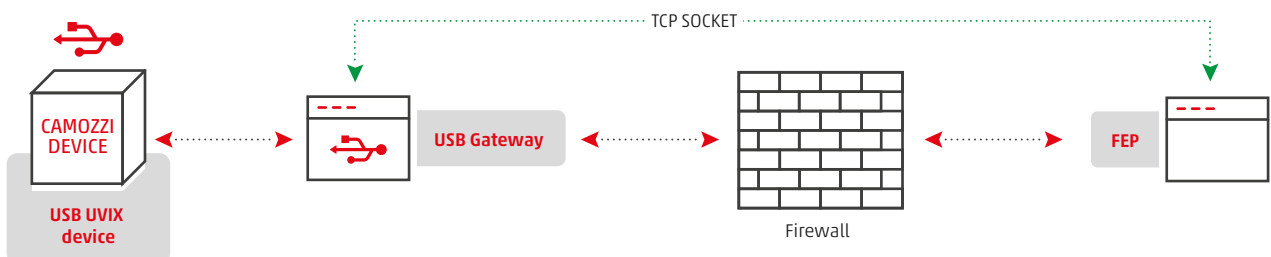
If the device connects correctly to the network it will attempt to create a communication channel with FEP, a TCP socket, using the IP address of the FEP (default 192.168.0.5) and port 1555 as connection parameters. In the event that another device attempts to communicate, it will use the same TCP socket created since the latter can manage multiple connections.



1.6.3 USB Gateway

The USB Gateway is required when connecting a Camozzi device via USB connection.

The Gateway's task is to take the data arriving from a virtual COM and transmit them to the FEP by establishing a TCP socket with the same parameters as in the previous case (default IP 192.168.0.5 and Port 1555 not editable).



1.6.4 Database

The database is the component that has the task of storing all the data managed by UVIX.

The database communicates directly with the Web Service, in this case there is no TCP socket therefore it is not possible to separate these two components.

1.6.5 Web Service

The Web Service deals with managing the data contained within the databases and making them available to other components, exchanging data with the FEP and then sending them to devices and the Web App to make them available to users.

Similarly to the other components, the Web Service has an IP address (by default 192.168.0.5) and remains in "listening mode" on port 5000, and both the FEP and the Web App communicate with the Web Server via TCP socket with this port.

1.6.6 Web App

The Web App is a web page managed by a web server (IIS for Windows operating systems) and has the task of managing the interface with the user.

The TCP socket established between the Web App and the Web Service uses port 5000.

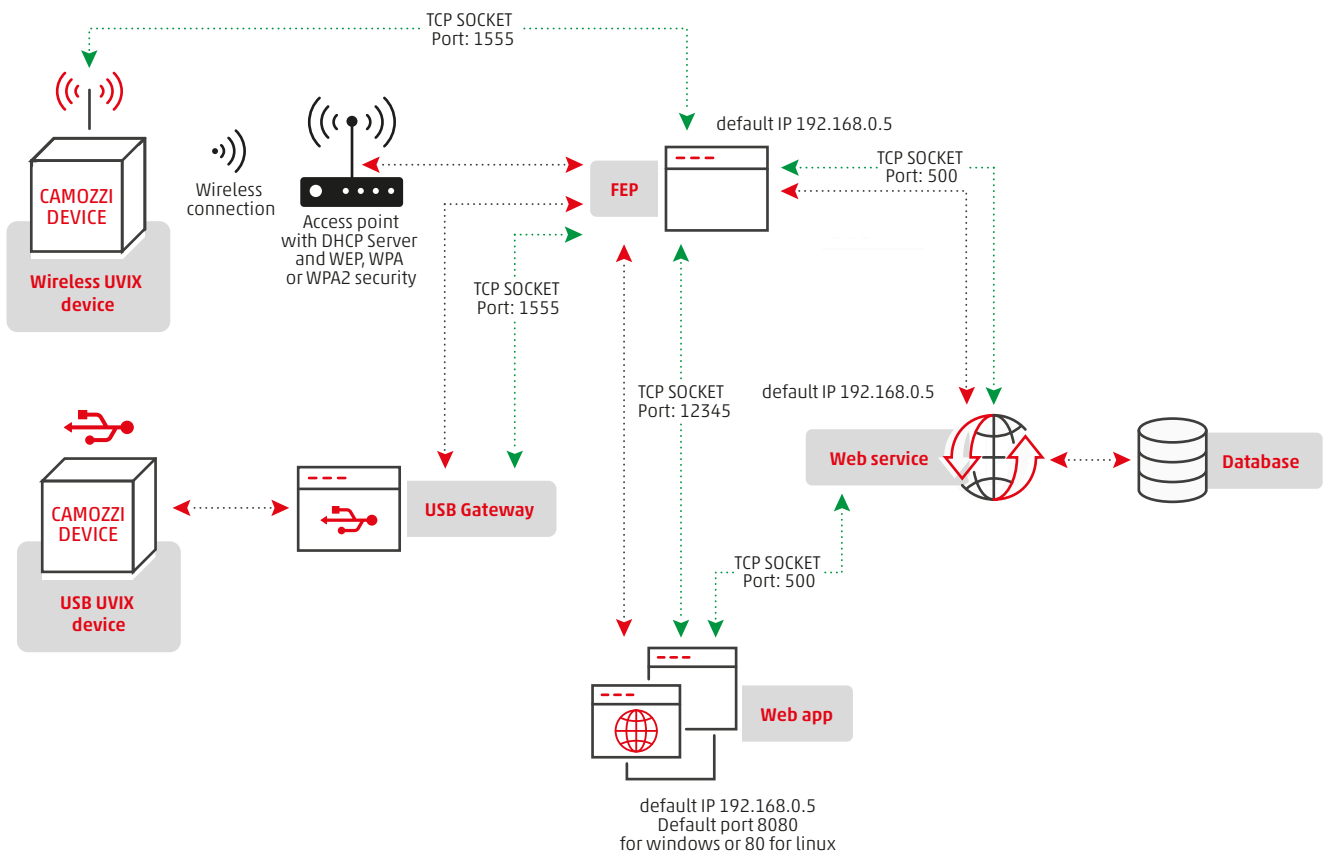
The web server manages the communication of the Web App to the outside, user access to the UVIX web page takes place via port 8080 for Windows operating systems or port 80 for Linux operating systems. The default Web App IP address is 192.168.0.5 while the ports are all editable.

The Web App, although not indicated in the introductory diagram, is able to communicate directly with the FEP and happens only when it has to send a command to a device.

In this case a TCP socket is opened from Web App to FEP, this communication, unlike the others, is unidirectional and uses port 12345.

1.6.7 Detailed structure of the UVIX

The following image shows the detailed UVIX structure also considering the content of this chapter.



1.7 Modification of communication parameters

We have seen in detail in the "Detailed analysis" chapter how the various components communicate with each other, in this chapter we will see how to modify the communication parameters operationally. It may be necessary to change the ports and IP addresses if they are already occupied by other services or if the components must reside on different machines, for example on servers due to company policies.

The ports that can be modified are:

- Communication port between FEP, Web Service and Web App.
- Communication port between Web App and FEP.

The files to be modified are accessible in the installation folder, if not modified, "C:\Program Files(x86)\CAMOZZI\UVIX".

1.7.1 Modification of communication parameters between FEP/ Web Service and Web App

To modify these configuration parameters (by default IP 192.168.0.5 and Port 5000) it is necessary to:

1. Copy the file "config.xml" from "C:\Program Files (x86)\CAMOZZI\UVIX\WebService" to "C:\Program Files (x86)\CAMOZZI\UVIX\WebService\Config", in this last folder the software checks if there are user configurations for the Web Service, otherwise it takes the default data.

2. Edit the following line in the "config.xml" file

```
<!--Url su cui lanciare Web Service-->
<StrServiceUrl>http://0.0.0.0:5000</StrServiceUrl>
```

Indicating the new IP address and/or the new port.

3. Edit the file "config.js" in the folder "C:\Program Files (x86)\CAMOZZI\UVIX\WebApp\js":

```
var ip = window.location.hostname;
[...]
apis: {
  url: "/" + ip + ":5000/api/web/",
  [...]
  apisFepWeb:
  {
    url: "/" + ip + ":5000/api/fep/",
    setup:{
  [...]
}
```

Replacing port 5000 with the new one where indicated.

To change the IP address, replace "window.location.hostname" at the beginning of the file with the address of the machine where the Web Service is located. Make sure that the machine corresponding to the IP address of the FEP is the same that corresponds to the IP address of the Web Service (i.e. the variable "ip" is the same).

1.7.2 Modification of communication parameters between Web App and FEP

To modify these configuration parameters (by default IP 192.168.0.5 and Port 12345) it is necessary to:

1. Modify the file "config.js" in folder "C:\Program Files (x86)\CAMOZZI\UVIX\WebApp\js":

```
var ip = window.location.hostname;
[...]
apisFep: {
  url: "/" + ip + ":12345/fep/",
  comandi:{
  [...]
}
```

Replacing the port 12345 with the new one.

To change the IP address, replace "window.location.hostname" at the beginning of the file with the address of the machine where the Web Service is located.

Make sure that the machine corresponding to the IP address of the FEP is the same that corresponds to the IP address of the Web Service (i.e. the variable "ip" is the same).

1.7.3 Web App port modification

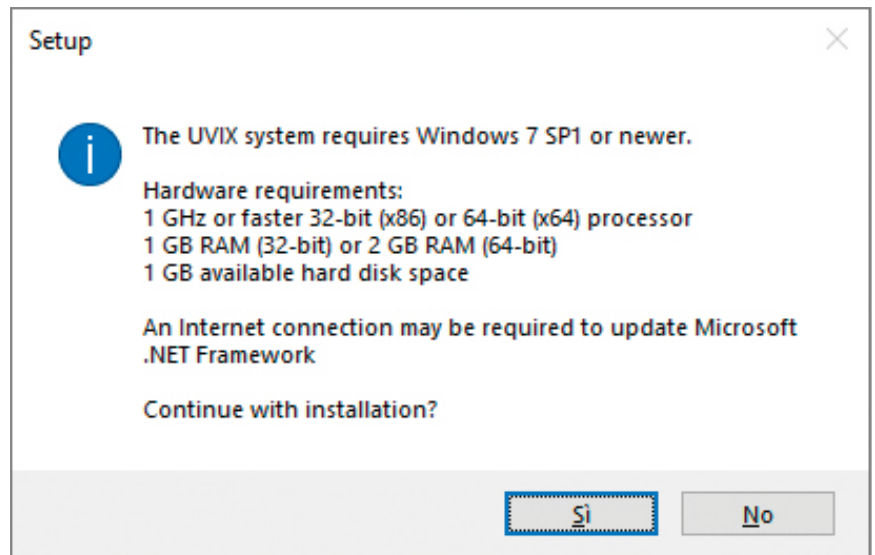
The Web App, as mentioned, is managed by a web server which makes it available to users via port 8080 in the case of a Windows operating system or 80 for a Linux operating system.

To modify this port it is necessary to modify it via the web server (IIS in the case of a Windows operating system).

2 Installation

Administrator privileges are required to perform the installation, if you do not have these privileges, the installation will ask for the credentials of a user who has them.

At start-up, the installation will show the minimum system requirements, it is up to the user to verify that they are met and if so, click "Yes" to continue.

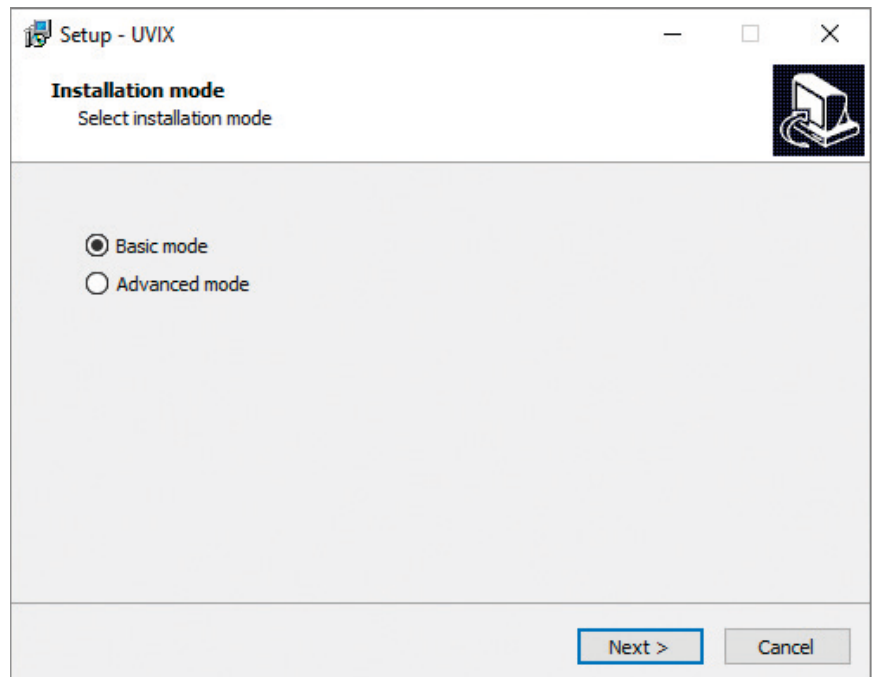


Once clicked, you will be asked which installation to perform:

- Basic: the installation will continue independently by installing all the necessary components and configuring the UVIX with the default data.
- Advanced: the installation will ask at each step if and how to configure all the components necessary for the operation of the UVIX.

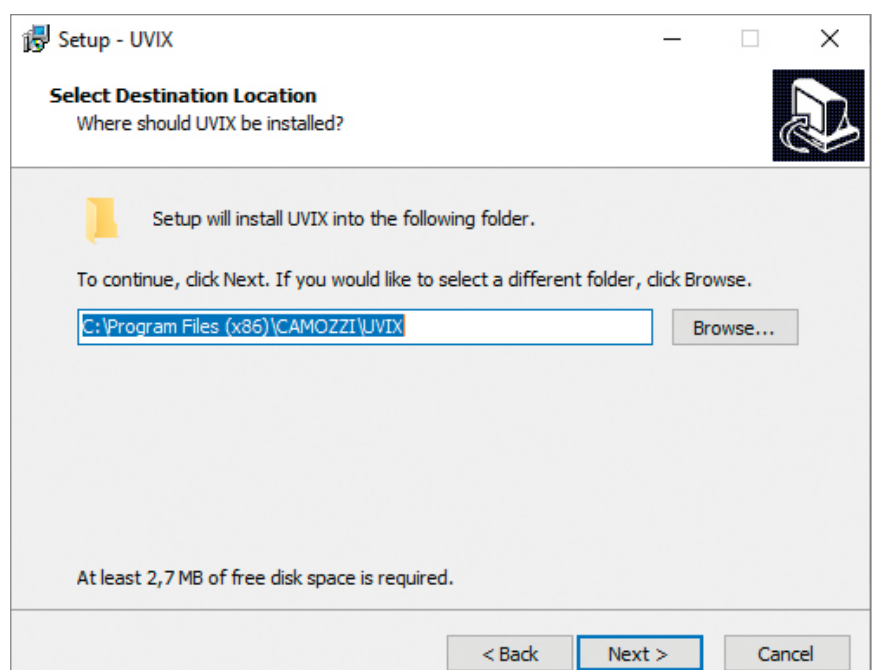
It is recommended to use the Advanced installation only in case of environment use in dedicated situations, for example on a company server or systems that require the use of particular network ports or management of network services.

Select the desired mode and click on "Next>".



If you have chosen the basic mode, wait for the installation to finish.

In the case of the advanced mode, however, a window will appear asking you to select the installation path, initially indicating the default one.



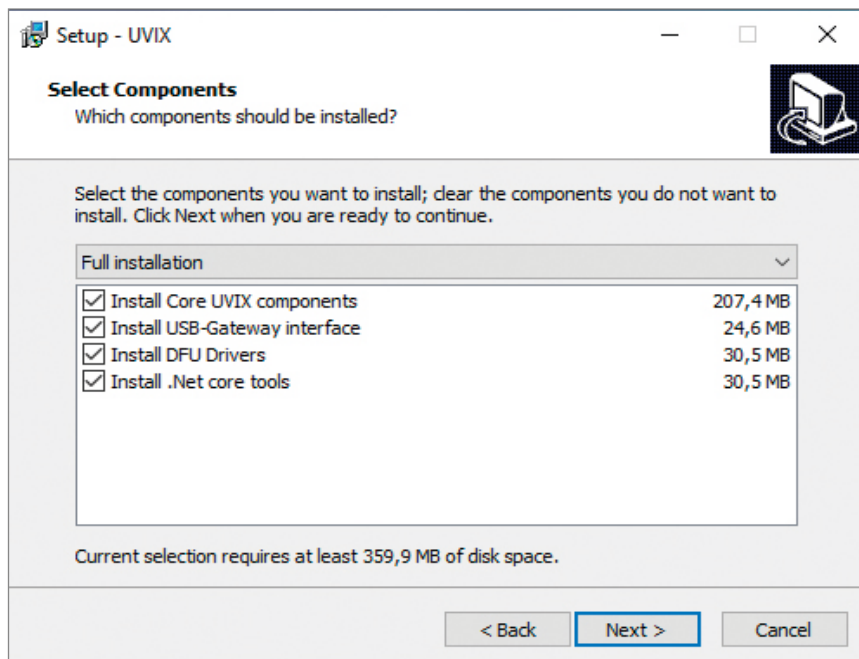
Once you click on "Next>" select which components to install:

- Core UVIX components: these are all the components necessary for the operation of the UVIX.
- USB-Gateway interface: this is the USB gateway to be able to connect devices via USB cable.

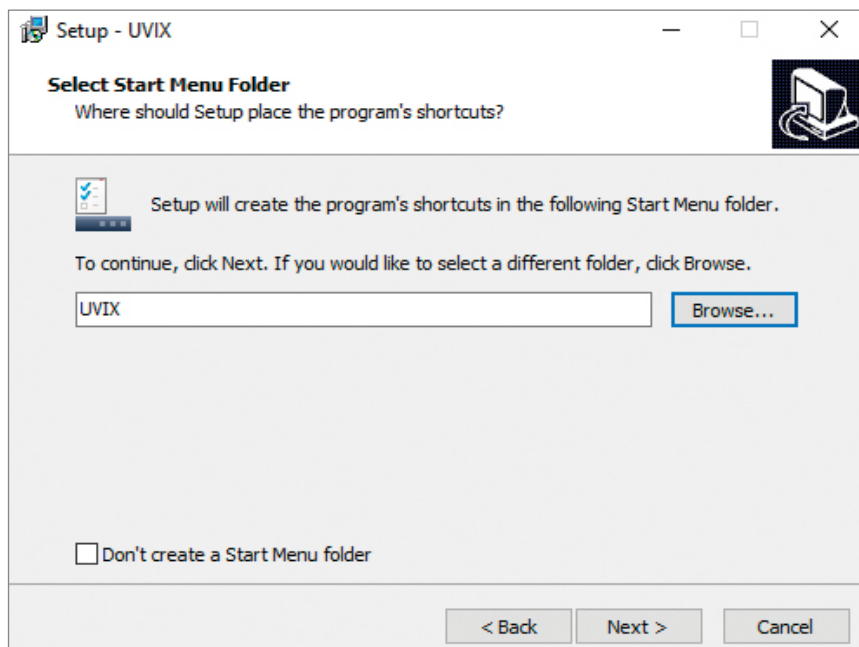
It is possible to select whether to perform a "full", "compact" or "custom" installation and depending on the choice, the installation will respectively select both components, only those required or those selected by the user.

The full installation is selected by default.

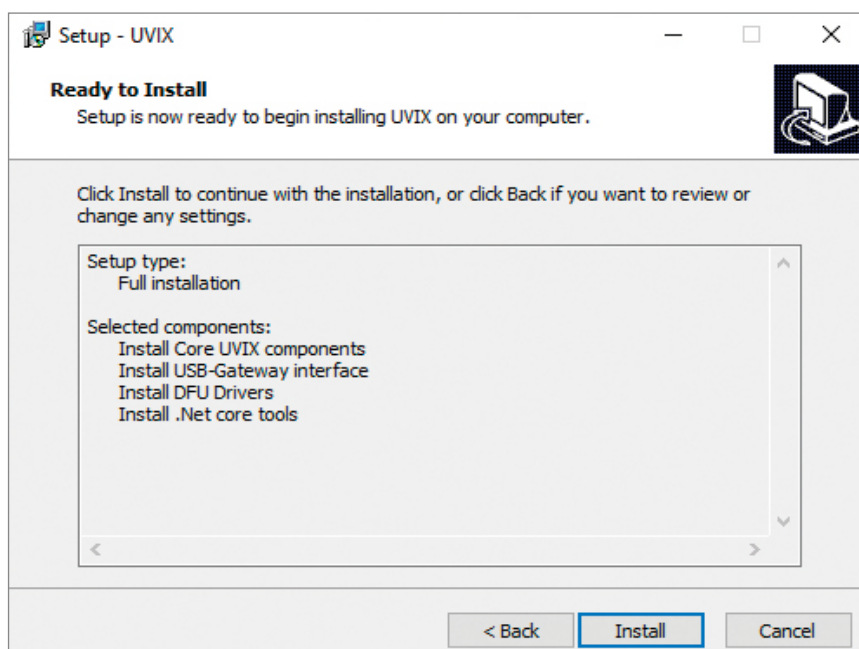
If you want to install the "Core UVIX" separately from the "USB-Gateway", only the one you desire can be selected at this stage.



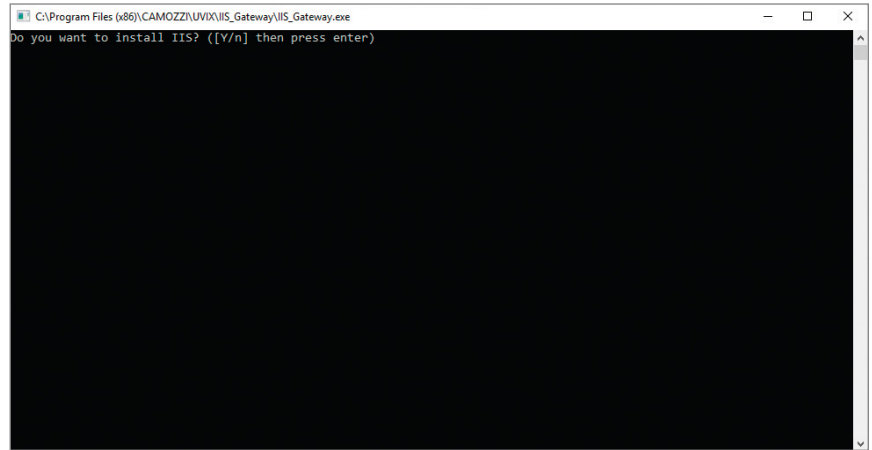
Once you click on "Next>" you will be asked if and where to create the connection to the UVIX and the default setting will be indicated.



Click on "Next>" and in the subsequent window check that the settings are the desired ones, if so, click on "Install" to start the installation.

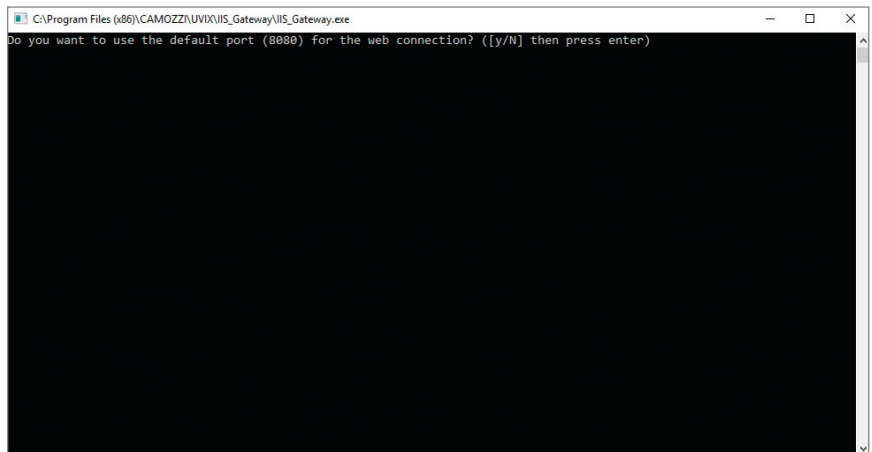


Once the installation is complete, a window will appear asking if you want to install the IIS (Internet Information Services), a service necessary for the correct operation of the UVIX. If the IIS is already installed, the installation will configure the part necessary for the operation of the UVIX, this phase can be skipped if you want to use a different http server and in this case the configuration will be entirely borne by the user.

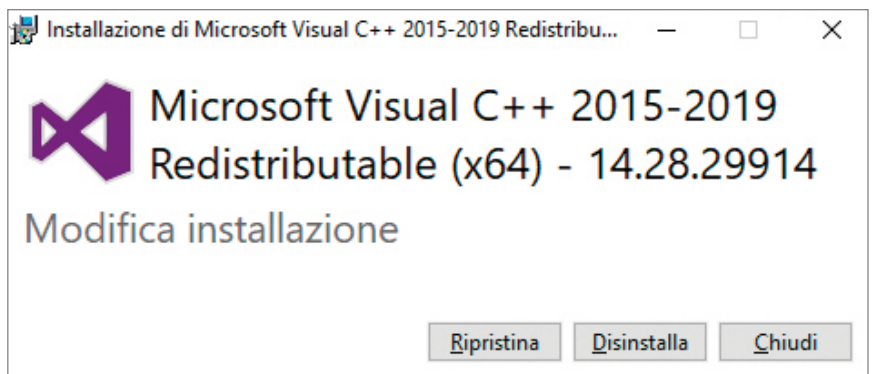


Wait for the installation to finish and press any key to continue.

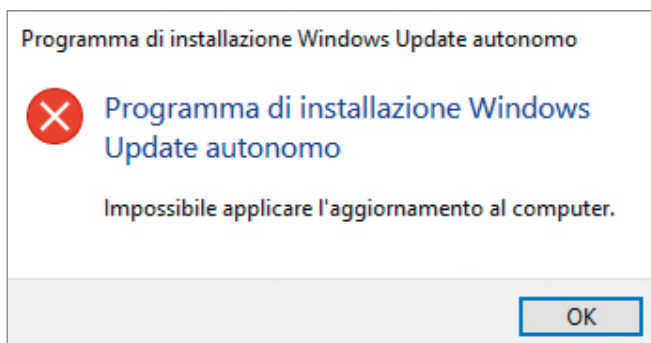
In the next window you will be asked to decide whether to use the default port (8080) and if not, to enter the desired one.



With the setting of the port completed, you will be asked if you want to install "Microsoft Visual C++", an essential Microsoft component. The possible choices are: Install, Uninstall, Reset or Close.



In the case of Uninstall or Install, the next step will try to perform an update which will fail but will not affect the outcome of the installation.

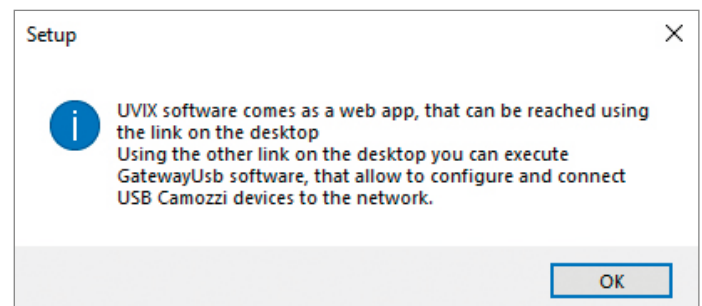


In the case of reset, at the end it will ask you to restart the PC, which will eventually interrupt the installation of the remaining components, it is recommended not to restart it and wait for the UVIX installation to finish. The advanced installation is intended for expert users, it is advisable to close this window and manage the add-on manually.

This option is useful if port 8080 is already being used by other services on the PC.

When finished, a window will appear asking if you want to restart the computer now or at a later time (to be able to use the UVIX, a restart is necessary).

Once you have clicked on "Finish", a window will appear that will summarize how to access the UVIX, once you click on "OK" the installation will be finished.



3. Web App

Later on this chapter will list the websites made available by the UVIX system's web app, alongside their respective functions.

3.1 Login

The connection to the application is made using an internet browser via the URL configured by the system administrator.

In order to log in to the system, the user must enter their credentials, consisting of a username and password.
When logging in for the first time, there are two login levels available:

LOGIN LEVEL	USERNAME	PASSWORD	DESCRIPTION
USER	enduser	enduser	Basic, read-only access level with limited features
INSTALLER	user	customer	Complete access level with the possibility of editing some parameters

Once logged in, it is possible to add or remove other users and edit the relative authorisations. For more details, refer to the paragraph "User Registry Management".

If the user does not enter their credentials correctly, the following error message will be displayed:

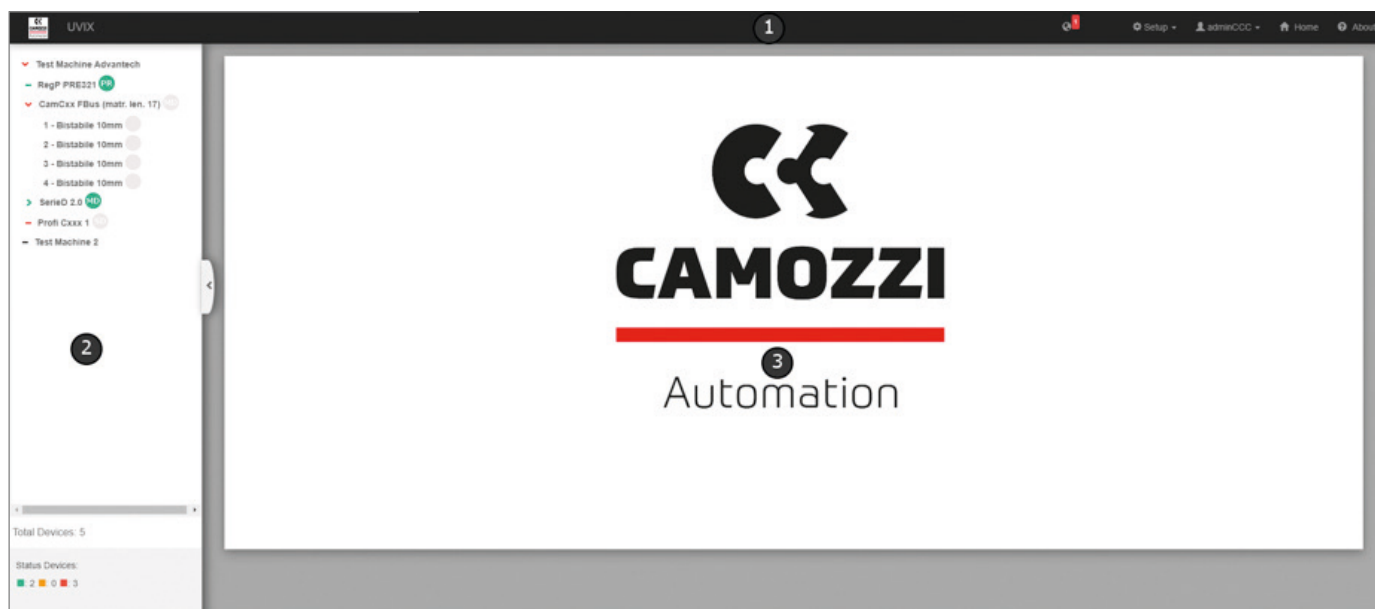
When the user is successfully logged in, the homepage of the web app is displayed.

3.2 Navigating the web app

In this paragraph, we will explain how the web app is structured and how to navigate within the app in order to access the different sections and features.

The web app is divided into three functional areas:

- Top bar [1]
- Left bar [2]
- Work page [3] (the page concerning the selected feature is displayed via the menus in the top bar and left bar)



3.2.1 Top bar

The top bar provides the following features:

- Link to the Camozzi Automation website homepage [1]
- Notification of new devices to be added to the relevant registry [2]
- Set-up of user registry [3]

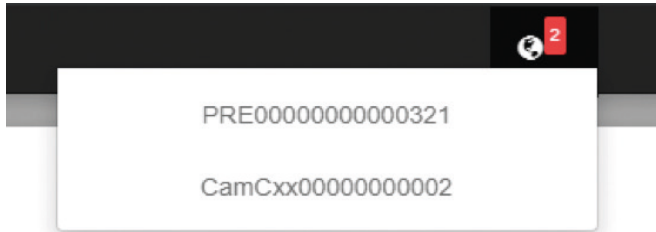
- Session and account management [4]
- Home page [5] (allows you to return to the initial page)
- Information about the UVIX system [6]




Notifications

When the UVIX system recognises a new device for the first time or the device has not yet been entered in the respective registry, a notification is displayed in the top bar.

The number displayed on the notification icon indicates the number of devices that need to be added to the registry.

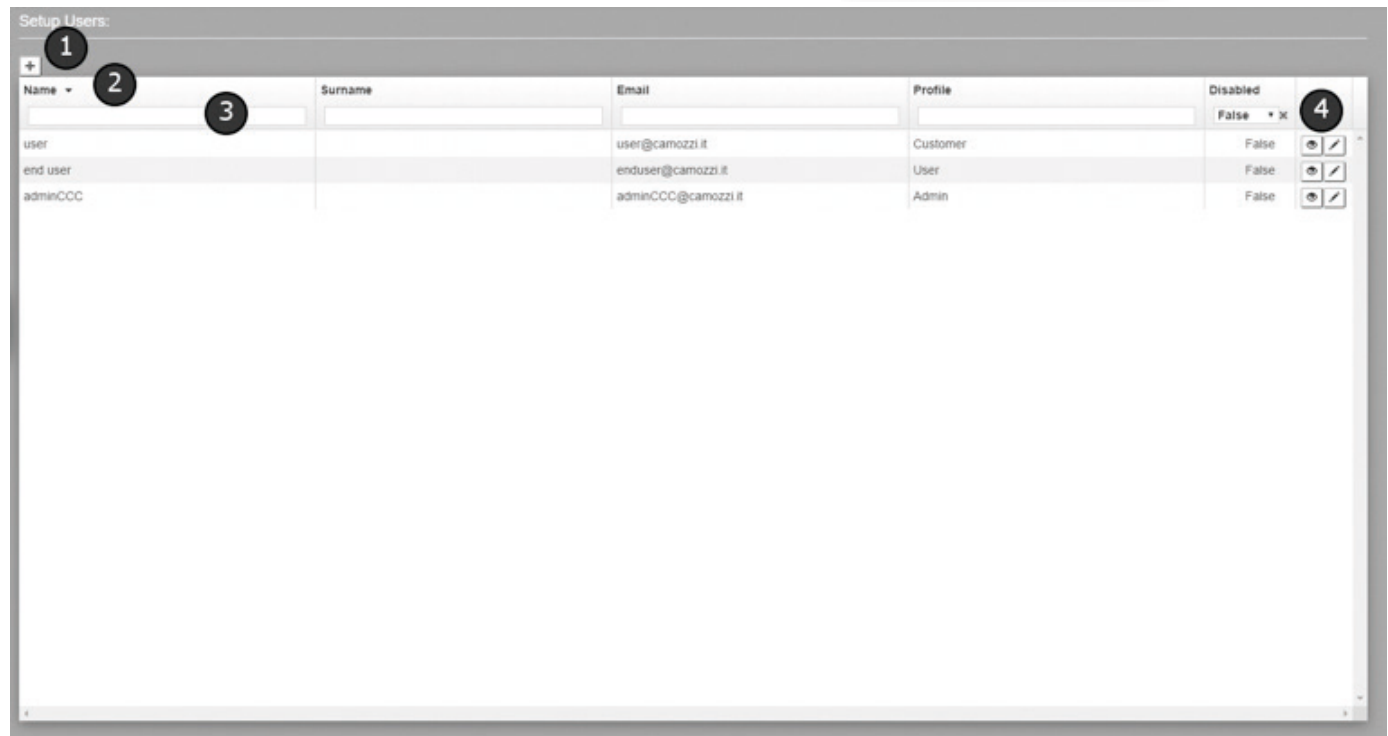
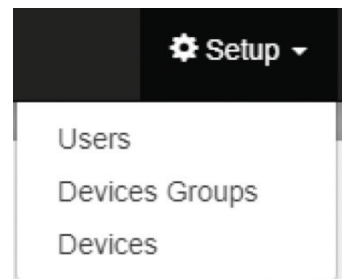


By clicking on the symbol , the list of devices is displayed and, in particular, their Device Number is shown (unique identification code of each Camozzi device). By hovering over a device with the cursor, a tool tip is shown, containing the family name to which it belongs. Clicking on a device in the list will open the device registry section, where a pop-up will be automatically opened, allowing you to insert it into the device registry. The user will have to assign it a name (it is advisable to associate a name which refers to the role of the device within the system/machine into which it will be inserted) and decide which device group to connect it with (for example, the name of the system/machine into which it will be inserted or one of its subsystems). Once the device has been registered, the notification counter of devices to be added to the registry will decrease. For more details on inserting a new device, refer to the "Setup-Device" paragraph.

Setup

Via the set-up menu, you are able to access sections to manage the registries of:

Users: it is possible to add new users by specifying various information (mandatory information is indicated with "*"), or to view and/or edit the user profiles already present in the registry. For more details about user profiles and authorisation, refer to the paragraph "User Registry Management".



DESCRIPTION
1 Button for creating a new device group
2 Button for ascending/descending alphabetical order
3 Filter of the values contained in the relative column
4 Buttons to view details of the device groups and edit their properties

By pressing the button [1], the following screen will be displayed:

After entering the required information (mandatory information is indicated with "*"), you can enter the new user by pressing the button "Save" located on the bottom right.

Before saving the changes, check that all the data entered is valid, otherwise the incorrect fields are highlighted and a note appears describing the problem.

By selecting "TRUE" under "Disabled", the selected user will no longer be available (and therefore will no longer be able to access the system) despite remaining in the registry.

By pressing the display and/or edit buttons [4], a screen similar to the previous one will be displayed.

Devices Groups: you can add new groups of devices by specifying their name, or view and / or edit the groups of devices already

present in the registry.

Setup Devices Groups:		
Name	Decommissioned	
Test Machine Advantech	False	
Test Machine 2	False	

DESCRIPTION

- 1 Button for creating a new device group
- 2 Button for ascending/descending alphabetical order
- 3 Filter of the values contained in the relative column
- 4 Buttons to view details of the device groups and edit their properties

Once the [1] button has been pressed, the following screen will be displayed:

After entering the required information (mandatory information is indicated with "*"), you can enter the new device group by pressing the "Save" button located on the bottom right.

Before saving the changes, check that all the data entered is valid, otherwise the incorrect fields are highlighted and a note appears describing the problem.

By selecting "TRUE" under "Decomissioned", the selected device group will no longer be available (and, therefore, will no longer be displayed in the left bar) despite remaining in the registry.

By pressing the display and/or edit buttons [4], a screen similar to the previous one will be displayed.

Devices: it is possible to view and/or edit the devices already present in the registry.

Setup Devices:

Device Number	Family Name	Name	Devices Group	Decomissioned	
PRE0000000000000321	Series PR1	regolatore 1	Test Machine Advantech	False	👁️ ✎️
CamCxx000000000002	Isola serieD multipolare 25/44 poli	CamCxx FBus (matr. len. 17)		False	👁️ ✎️
CamCxx000000000001	Isola serieD ProfiNet	Profi Cxxx 1	Test Machine Advantech	False	👁️ ✎️

DESCRIPTION

1 Button for ascending/descending alphabetical order

2 Filter of the values contained in the relative column

3 Buttons to view device details or edit their properties

After entering the required information (mandatory information is indicated with "*"), you can enter the new device by pressing the "Save" button located on the bottom right.

Before saving the changes, check that all the data entered is valid, otherwise the incorrect fields are highlighted and a note appears

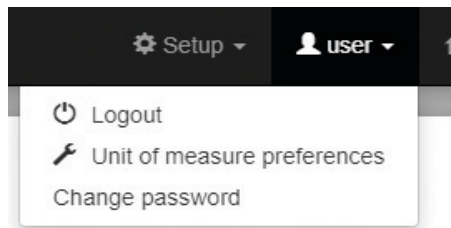
describing the problem.

By selecting "TRUE" under "Decomissioned", the selected device will no longer be available despite remaining present in the registry.

By pressing the display and/or edit buttons [3], a screen similar to the previous one will be displayed.

Session/account management

It displays the username of the active user profile and allows the user to log out of the application or change the password of the active user profile.



 A screenshot of a 'Change Password' dialog box. The title bar says 'Change Password' with a close button. The form contains three input fields: 'Old password', 'New password', and 'Repeat new password'. At the bottom right, there are two red buttons: 'Save' and 'Cancel'.

By pressing "Unit of measure preferences" you can select the desired unit of measurement.

 A screenshot of a 'Unit of measure preferences (user)' dialog box. The title bar says 'Unit of measure preferences (user)' with a close button. The form is divided into two sections: 'Pressure' and 'Temperature'. Under 'Pressure', there are three radio button options: 'Bar (bar)', 'KiloPascal (kPa)' (which is selected), and 'Pounds per square inch (psi)'. Under 'Temperature', there are two radio button options: 'Degree Celsius (°C)' (which is selected) and 'Degree Fahrenheit (°F)'. At the bottom right, there are two red buttons: 'Save' and 'Cancel'.

About

By pressing About, a popup appears containing information about the release of the web app. The information relating to the version that allows you to understand if you are using an updated or obsolete version is particularly useful.

 A screenshot of an 'About' dialog box. At the top, it features the Camozzi Automation logo and the text 'UVIX'. Below this, it says 'Camozzi Automation Universal Visual Interface Solution.' The main section is titled 'UVIX software versions' and lists the following information:

Web App:	2.0.2.1
FEP:	1.7.0.0
Web Service:	1.10.0.0
DataBase Setup:	3.1.1.3

 Below this, it lists:

Date of release:	2020-05-25
Copyright:	2019 - 2020 Camozzi Automation

 At the bottom right, there is a red 'Close' button.

3.2.2 Left bar

The left bar provides a comprehensive view of the state of the system/machine into which the various devices are inserted.

The **left bar** uses a hierarchical treeView to represent the status of the groups of active devices (e.g. those not disabled) present in the registry and the status of the devices inserted into these groups.

At the outermost level, there are device groups [1] that may contain any number of devices. A device [2] in turn may contain, if required by the selected device, any number of slaves [3].

Initially, a group of devices does not contain any device [4]: it will be up to the user to connect the devices to a specific device group when the device is added to the registry, or edit it later by accessing the management of the device registry.

You can expand (▶) and reduce (◀) the various sub-levels independently of each other; initially the level of detail is set to Device Groups.

The overall status of the various elements is highlighted using 4 colours:

- Green: OK
- Orange: WARNING
- Red: ALARM
- Gray: NOT CONNECTED

The 3 types of objects are represented in the treeView as follows:

- Device groups:
 - Button to show/hide the devices belonging to the group, coloured according to the overall status of the device
 - Name assigned to the device group
- Device:
 - Button to show/hide the slaves belonging to the device, coloured according to the overall status of the device
 - Name assigned to the device
 - A dot with the initials of the device family to which the device belongs, coloured according to the overall status of the device.
- Slave:
 - Slave ID - Description of type
 - A dot, coloured based on the overall status of the slave

Un dispositivo mostrerà lo stato peggiore tra i suoi slave, analogamente A device will show the worst status among its slaves, similarly for the device group in relation to the devices contained within it.

Assuming that a device group has three devices in three different states (OK, WARNING and ALARM), the status of the device group will be the most severe of the 3, e.g. ALARM.

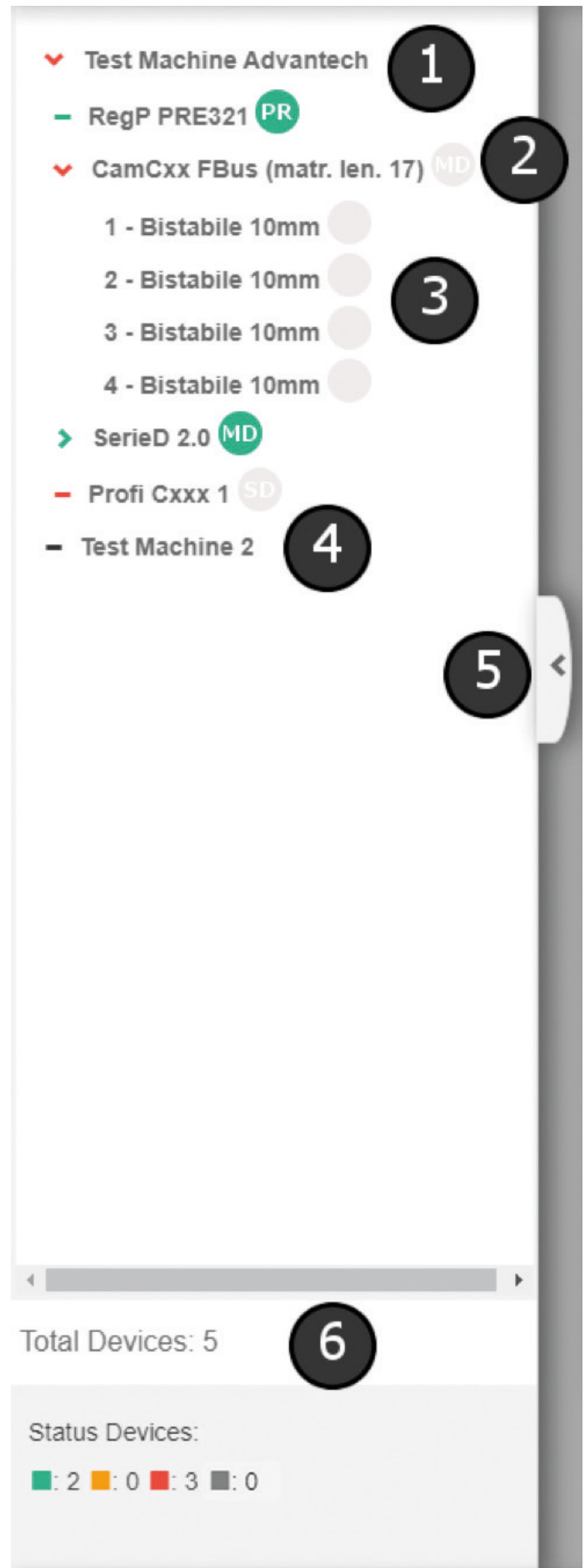
For devices the mechanism is similar, with the difference that they themselves have their own status, so consequently, the overall status is the worst between their own and that of the slaves.

The NOT CONNECTED status is a special case. A device which is not connected is shown by the web app using a grey dot next to it and its slaves (if it has them). In this case, however, the colour of the button to show/hide its subsection will be red, which indicates an ALARM status.

Selecting a device or a slave will open a page in the functional area "Work page" which will allow you to monitor, if required, configure and/or send commands to the selected element.

You can show or hide the left bar using the [5] button.

In the lower part of the left bar [6] there is a summary of the total number of devices present and their overall status.



3.3 User registry management

Before describing how to manage the user registry effectively, it is necessary to understand how to correctly configure users to ensure that they can only access the required features. In order to limit/control access to certain features, the UVIX system uses two different concepts: Profiles and Authorisations.

PROFILES

Users can have two profiles:

1. **User:** profile for users intending to only monitor devices or perform limited functions.
2. **Installer:** profile to be assigned to the system managers who must make adjustments and device configurations.

AUTHORISATIONS

The authorisations instead allow you to specify which of the available features are assigned to a specific user. The authorisations available are:

- **Manage registries:** permission to manage registries of users, devices and device groups
- **Manage command:** authorisation to send commands
- **Manage setup parameter:** authorisation to configure device and slave setup parameters

The following explains how some basic features of the web app are influenced by profiles and authorisations.

Variables

Each variable can only be viewed by users with a specific profile. Therefore, some variables can be seen by both users belonging to the User and the Installer profiles, while other variables can only be viewed by users belonging to the Installer profile.

Registries of Machines and Device groups:

A user can create or edit these registries if they have authorisation to Manage registries. The profile to which a user belongs is insignificant.

User registries

A user can create or edit users if they have authorisation to Manage registries. Furthermore, a user will only be able to manage users with a profile lower than or equal to their own: a user belonging to the User profile can create or edit users with a User profile. A user belonging to the Installer profile can create or edit users with both a User and Installer profile.

Device registries

For complete access to device registry management, you must have authorisation to Manage registries, but instead, in order to add a device via notifications on the top bar, you do not need to have any particular authorisation.

Commands

A user must have Manage command authorisation in order to send commands. The commands, unlike the variables, do not have a level and, therefore, the profile to which the user belongs is irrelevant.

Configuration

In order to view/edit the configuration of a device or a slave, a user must have Manage setup parameter authorisation. The setup parameters, similarly to the variables, are associated with a level. A parameter can only be viewed and/or edited by users with a profile greater than or equal to the level of the parameter itself. Therefore, a level 1 parameter can be viewed and/or edited by users belonging to the User and Installer profile, whereas a level 2 parameter can only be viewed and/or edited by users belonging to the Installer profile.

3.4 Device management

In order to access device management, you have to select it from the treeView in the left bar.

The device management page is divided into 3 macro-areas:

- **Header [1]:** the name assigned by the user to the selected device and the name of the device group to which it belongs are displayed.
- **Status information [2]:** the following fields related to the selected device are displayed.
 - An image which represents it with a coloured border based on its overall status.
 - *Name:* name assigned by the user.
 - *Family name:* description of the type.
 - *Firmware:* firmware version.
 - *Last transmission:* date and time of the last data received.
 - *Master status:* overall status.
 - *Slaves status:* status of the slaves (only if the device has slaves).
 - *Operational status:* operational status.

- *Connection:* indicates whether the device is transmitting or more precisely whether the FEP is receiving data from it. The indication is shown by the colour of the dot which turns green if the device is connected or red if not.
- Under the image of the device, there may be a "Configuration" button, if required, which allows the user to open the configuration window of the selected device.
- **Details [3]:** it is divided in turn into three tabs:
 - *Variables:* consisting of a table showing the variables sent by the device accompanied by their value and the date of receipt. For more information, see the paragraph "Variables".
 - *Alarm:* consisting of a table showing all possible alarms that the device may trigger. For more information, see the paragraph "Alarms".
 - *Commands:* allows the user to send commands and see the command history. For more information, see the paragraph "Commands".

3.5 Slave management

In order to access slave management, if present, it is necessary to select it from the treeView present in the left bar.

The screenshot shows the Slave Management interface for a device named 'SerieD 2.0' (Slave: 1 - Bistabile 10mm). The interface is divided into three main sections:

- Header [1]:** Displays the device name, slave ID, family name, and firmware version.
- Status information [2]:** Shows a slave image with a 'Configuration' button, and fields for 'Last transmission', 'Status' (green dot), and 'Operational status' (Work).
- Details [3]:** Contains two tabs: 'Variables' and 'Alarms'. The 'Variables' tab is active, showing a table of device variables and their values.

Name	Value	Received
Temperature Subbase	36 °C	2019-06-12 16:50:36
Number of Cycles Solenoid 1	1	2019-06-12 16:50:36
Number of Cycles Solenoid 2	1	2019-06-12 16:50:36
Health Status Solenoid 1	100 %	2019-06-12 16:50:36
Health Status Solenoid 2	100 %	2019-06-12 16:50:36
Status Solenoid 1	Off	2019-06-12 16:50:36
Status Solenoid 2	Off	2019-06-12 16:50:36
Time MAX Solenoid 1	0 us	2019-06-12 16:50:37
Time MAX Solenoid 2	0 us	2019-06-12 16:50:37
Time MIN Solenoid 1	0 us	2019-06-12 16:50:37

On the right side of the details section, there are two gauge indicators for 'Health Status Solenoid 1 [%]' and 'Health Status Solenoid 2 [%]', both showing 100% health.

The slave management page is divided into 3 macro areas:

- **Header [1]:** displays a description of the slave, formed by the Slave ID and the description of the type, as well as the group of devices to which it belongs.
- **Status information [2]:** displays the following fields related to the selected slave.
 - An image which represents it with its coloured border based on its overall status.
 - *Slave ID*: identification of the slave within the device.
 - *Family name*: description of the type.
 - *Firmware*: firmware version.
 - *Last trasmission*: date and time of the last data received.
 - *Status*
 - *Operational status*
 - Under the image of the slave, there may be a "Configuration" button, which allows the user to open the configuration window of the selected slave.

• **Details [3]:** it is divided into two tabs:

- *Variables*: consisting of a table showing the variables sent by the device accompanied by their value and the date of receipt. For more information, see the paragraph "Variables".
- *Alarm*: consisting of a table showing all possible alarms that the slave may trigger. For more information, see the paragraph "Alarms".

3.6 Variables

The variables section is accessed from the device/slave management page by clicking on the Variables tab [1].

The screenshot shows the 'Variables' tab selected in the details section. It displays a table of variables and their values, along with two gauge indicators for 'Charge coil health status [%]' and 'Exhaust coil health status [%]'.

Name	Value	Received
Hardware Version	1	2019-09-17 09:45:28
Product Code	00000000000000000000000000000000	2019-09-17 09:45:28
Type	Analog voltage	2019-09-17 09:33:47
Temperature	30 °C	2019-07-12 12:49:53
Supply Voltage	25.6 V	2019-07-12 12:49:53
Set Pressure	0.51 bar	2019-09-17 10:24:05
Regulated Pressure	4.13 bar	2019-09-17 10:24:05
Number of Cycles Solenoid 1	0	2019-06-26 17:31:28
Number of Cycles Solenoid 2	0	2019-06-26 17:31:28
Efficiency Solenoid 1	100 %	2019-06-26 17:31:28

On the right side, there are two gauge indicators for 'Charge coil health status [%]' and 'Exhaust coil health status [%]', both showing 100% health.

The variables are listed in the form of a table and the following information is shown for each variable:

- **Name:** name of variable.
- **Value:** value taken by the variable.
- **Received:** date/time at which the last information relating to the variable was received.

Some variables, if considered particularly important, may have a dedicated display through the use of indicators [2].

3.7 Alarms

The alarm sections are accessed from the device/slave management page by clicking on the Alarms [1] tab.

It is possible to see if there is an active alarm from the colour of the icon present on the Alarm tab:

- *Grey icon*: no active alarm.

- *Orange icon*: at least one warning level alarm (but no error level alarms).
- *Red icon*: at least one error level alarm is active (this does not exclude the presence of active warning level alarms).



Event Name	Status	Event Onset
Unregulated Pressure	⚠	2019-09-03 16:00:20
Under Voltage	⚠	
SPI Sensor	⚠	
Diagnostic Sensor	⚠	
Alarm ADC	⚠	
Alarm Eeprom	⚠	
Unregulated Pressure	⚠	
Wrong Analog Signal	⚠	
Problem Eeprom	⚠	
Wrong Calibration	⚠	
No Activation Valve	⚠	

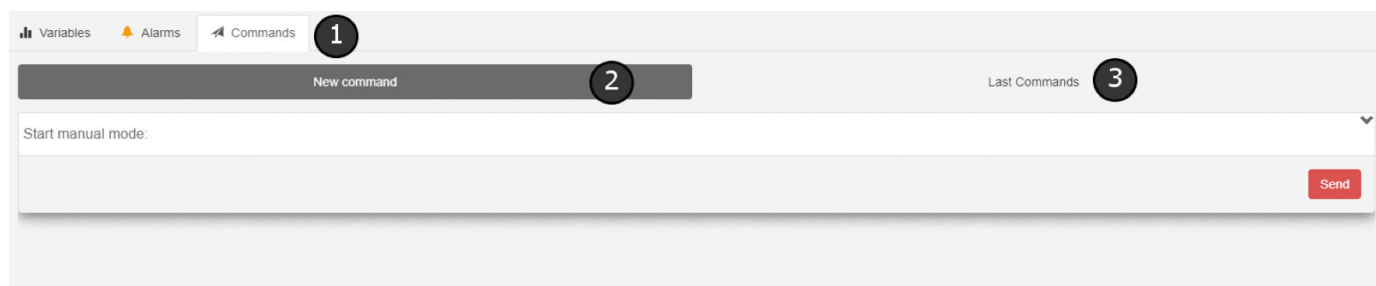
The alarm table contains all the possible alarms that the device/slave can trigger, but only the alarms that have a coloured icon other than grey in the status column are indeed active. The Event Onset column shows the date when the alarm was detected.

The alarms can be at one of two levels:

- ⚠ Warning (turns orange when active)
- ⚠ Error (turns red when active)

3.8 Commands

The command section is accessed from the device management page by selecting the commands tab [1] in the *Details* section.



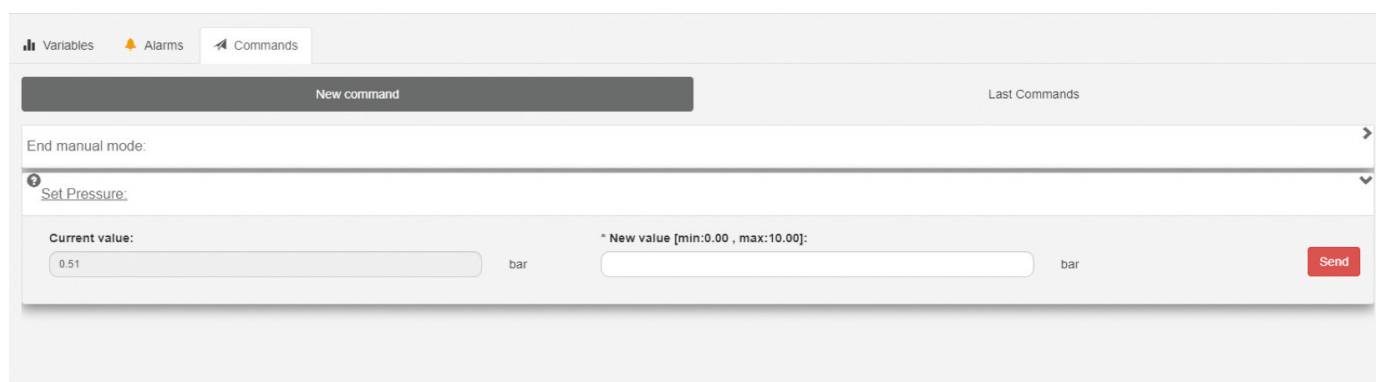
Within the command section, you can open the section to send *new command* [1] or see the history of commands sent by pressing on *Last Commands*.

If the device is not connected, it will only be possible to view the command history.

If you want to send commands to the device, it is always necessary to first put the device in manual operating mode. If the device is not in this mode, the web app only suggests the Start Manual Mode command. Only once the device has effectively switched to manual operating mode will the other controls be visible, which vary based on the type of device selected. Furthermore, the command will always be displayed in order to exit manual mode, which should always be sent when a command sending session ends.

Depending on the type of command which has to be sent (numeric, on-off, ...), the web app has a different interface to allow the user to set the desired value and send it. Independent of the graphical aspect, both the desired value and the current value are shown for each command.

A command has only been received by the device/slave when the two values coincide. If the desired value is not acceptable, an error will be shown on the screen: the field containing the incorrect value will be highlighted and accompanied by a message describing the cause of the error.



It is possible to open the command sending section in a dedicated window in order to allow the user to see other information at the same

time, such as alarms or variables. In order to open a dedicated window, double click on the *New command button*.



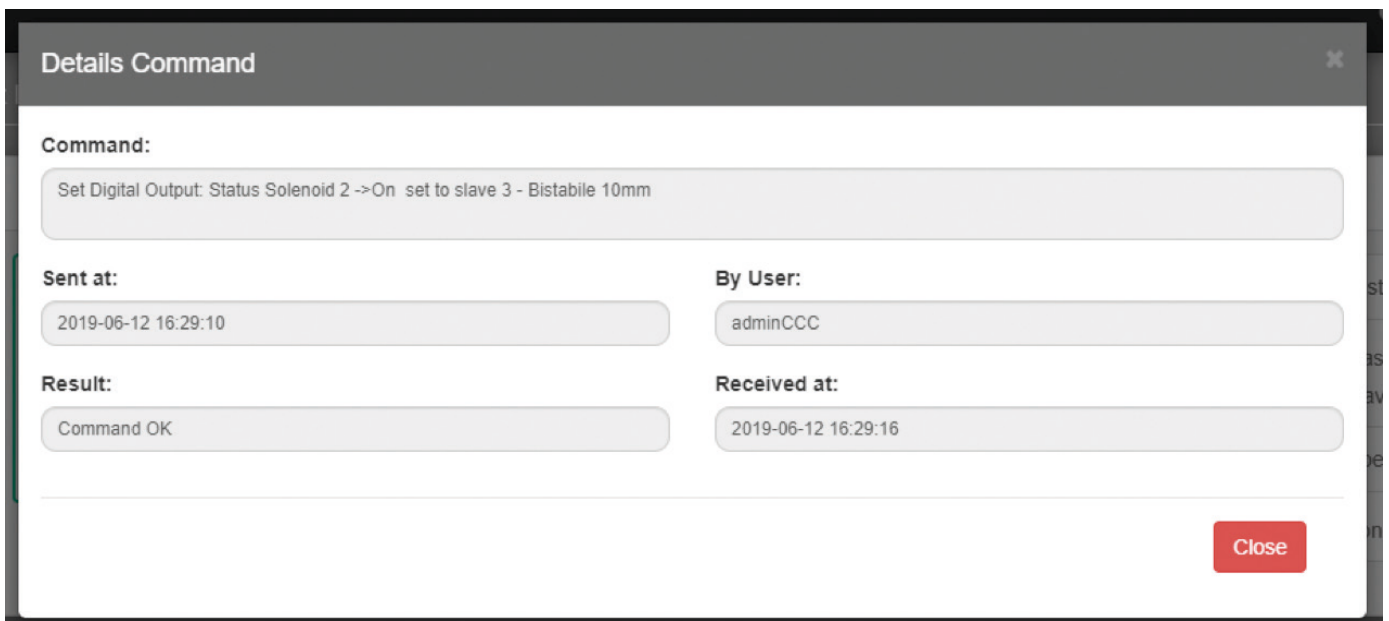
Clicking on *Last commands* will display a table with the list of commands sent to the device.

New command		Last Commands			
User	Command	Slave	Result	Sent at	Received at
user	End manual mode		Command OK	2019-09-13 11:45:57	2019-09-13 11:45:59
user	Start manual mode		Command OK	2019-09-13 11:45:43	2019-09-13 11:45:44
adminCCC	End manual mode		Command OK	2019-09-12 15:14:19	2019-09-12 15:14:24
adminCCC	Start manual mode		Command OK	2019-09-12 15:14:00	2019-09-12 15:14:01
adminCCC	End manual mode		Command OK	2019-09-12 14:47:21	2019-09-12 14:47:26
adminCCC	Start manual mode		Command OK	2019-09-12 14:47:02	2019-09-12 14:47:03
adminCCC	End manual mode		Command OK	2019-09-12 12:07:08	2019-09-12 12:07:10
adminCCC	Start manual mode		Command OK	2019-09-12 12:07:00	2019-09-12 12:07:02
adminCCC	End manual mode		Command OK	2019-09-12 12:01:57	2019-09-12 12:02:02

This table shows:

- *User*: username of the user that sent the command.
- *Command*: description of the command sent.
- *Slave*: in the event that the command is sent to a particular slave, its ID is shown followed by a description of the type.

- *Result*: outcome of the command.
- *Sent at*: date and time of sending the command.
- *Received at*: date and time of receiving the command.
- Clicking on the button in the last column [1] opens a pop-up, which shows a greater level of detail regarding the command sent.



3.9 Set-up parameters configuration

The set-up configuration parameters section is accessed from the management page of the device/slave you want to configure by clicking


on the "Configuration" button under the image of the device/slave.

DESCRIPTION



- | | |
|---|--|
| 1 | Selector to enable (left selector) or disable (right selector) the modification of parameters |
| 2 | Icon indicating whether the device is in manual mode |
| 3 | Buttons to expand or close the window |
| 4 | Parameters to be configured (they vary according to the type of device/slave selected) |
| 5 | Button to send the reset command (restore to factory default settings). Also available with selector [1] configured on the right |
| 6 | Button to save a configuration without sending it to the device |
| 7 | Button to send the configuration |
| 8 | Button to Send the command in order to finalise the current configuration on the device/slave |

Upon accessing the system for the first time after connecting a new device, since no configuration has been saved yet, the parameters sent by the device will be shown on screen regardless of the type of display selected.

Even if a device is not connected, it is still possible to access its configuration, but only the display of the parameters will be enabled and the only possible option will be to save the configuration without sending it to the device.

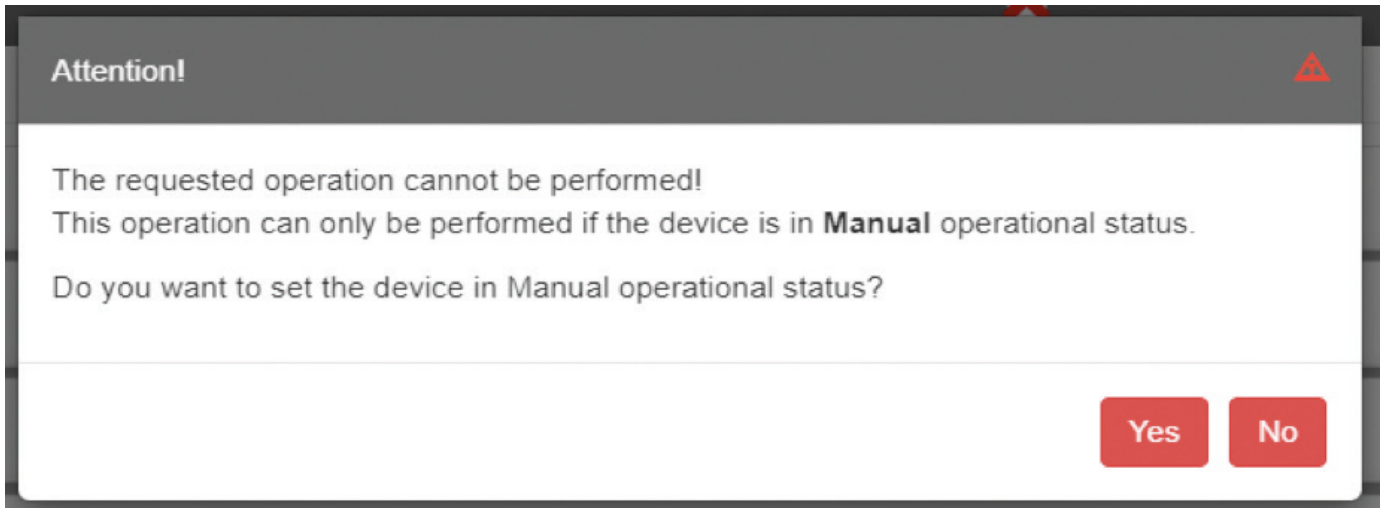
If the value of a parameter displayed on the screen differs from that in the connected device/slave, the symbol  will be displayed next to the parameter. By clicking on it, the value displayed on the screen is aligned to the current value on the connected device/slave.

To be able to send the Reset, Send and Save on device commands to the selected device/slave, the device must be in manual operating mode. You can see if the device is in manual mode by checking the icon [2].

-  device in manual operating mode
-  device not in manual operating mode

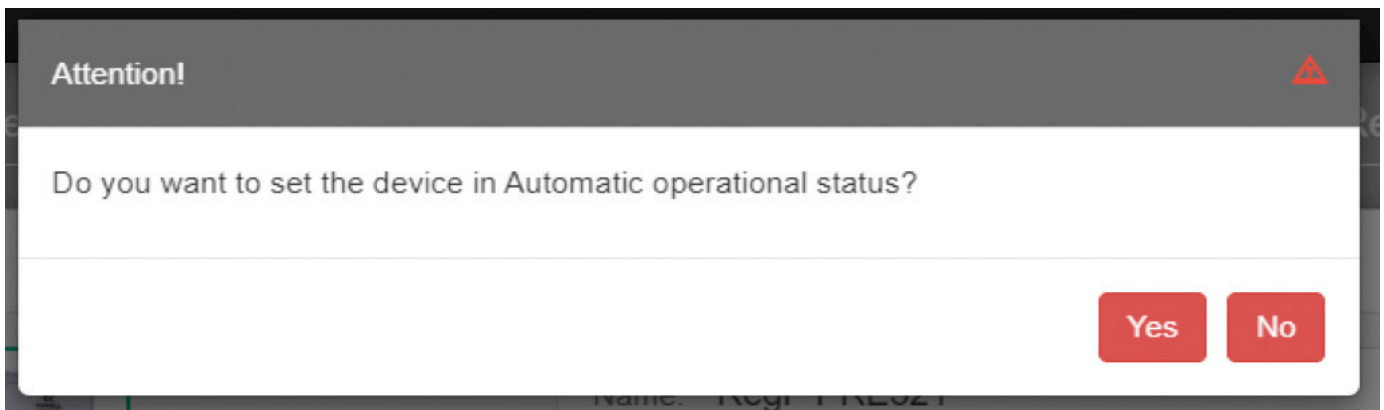
In the event that a user requests to carry out a task which is admissible only if the device is in manual operating mode, but the device is not in

this mode, the web app will alert the user via a pop-up, allowing them to put the device into manual operating mode.



Similarly, when the user closes the configuration window and the device is still in manual operating mode, they will be asked via a

pop-up if they want to return to automatic mode.

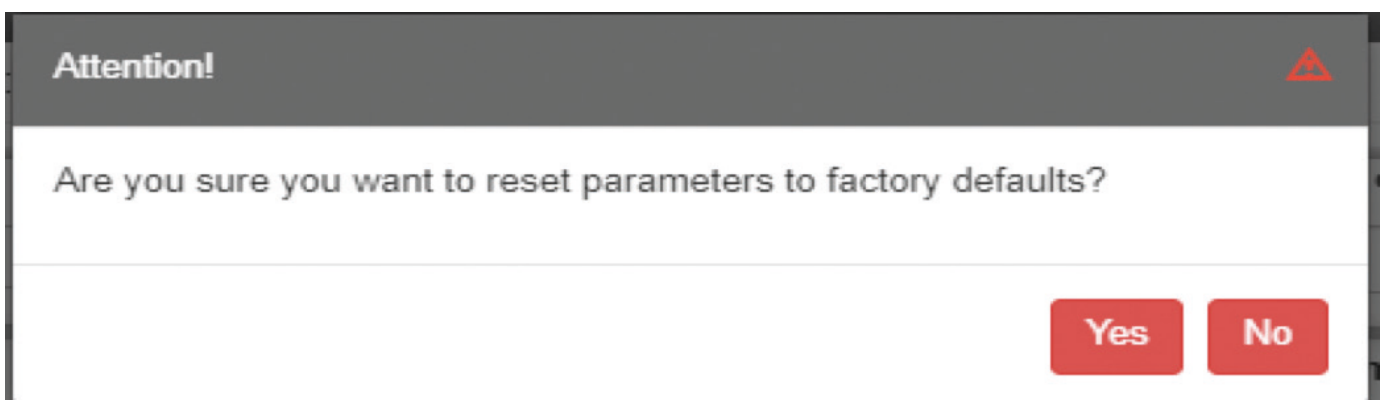


When we talk about manual operating mode, we are always referring to a device: in the case of slave configurations, the operating status of

the device to which the slave belongs is taken into consideration.

Reset

It is possible to restore the device/slave to its factory settings by pressing the *Reset* button.



As it is an irreversible operation, the web app asks the user for confirmation via a pop-up before carrying out the operation.

Save on pc

By pressing save on pc, the entire configuration shown on the screen is saved in the local database.


A configuration can be saved only if it is correct, that is, if all the parameters are set with a valid value. Otherwise, an error message is displayed on the screen indicating the first parameter with an invalid


value that was detected. All fields with invalid values are highlighted and a message appears under them with the reason why the value assigned is not considered valid.

This operation is transparent to the device, as no data exchange takes place with it.

Send

By pressing send, the parameters with the values present on the screen that have a different value with respect to the value saved in the device are sent to it.

The parameters sent will, therefore, be only those highlighted by the symbol . If the sending procedure is not successful due to connectivity problems or invalid values, an error message will be displayed on screen. Any invalid parameters will be highlighted and a message will describe the problem.

The configuration change is accepted by the device when the symbol  disappears from next to the parameters sent: this means that the values of the parameters present on the screen correspond to the values saved on the device.

However, these changes will not be permanent, but will remain active only until the device is next restarted. In order to make these changes permanent, use the command *Save on device*.

The data sent is also automatically saved in the local database, as is the case by clicking the command *Save on pc*.

Save on device

By pressing the Save on device command, the parameters are not sent to the device (and therefore, the values of the parameters shown on the screen and those saved on the device/slave might not be aligned),

but a command is sent which makes the current configuration on the device permanent.

3.10 Exclusive Device Management

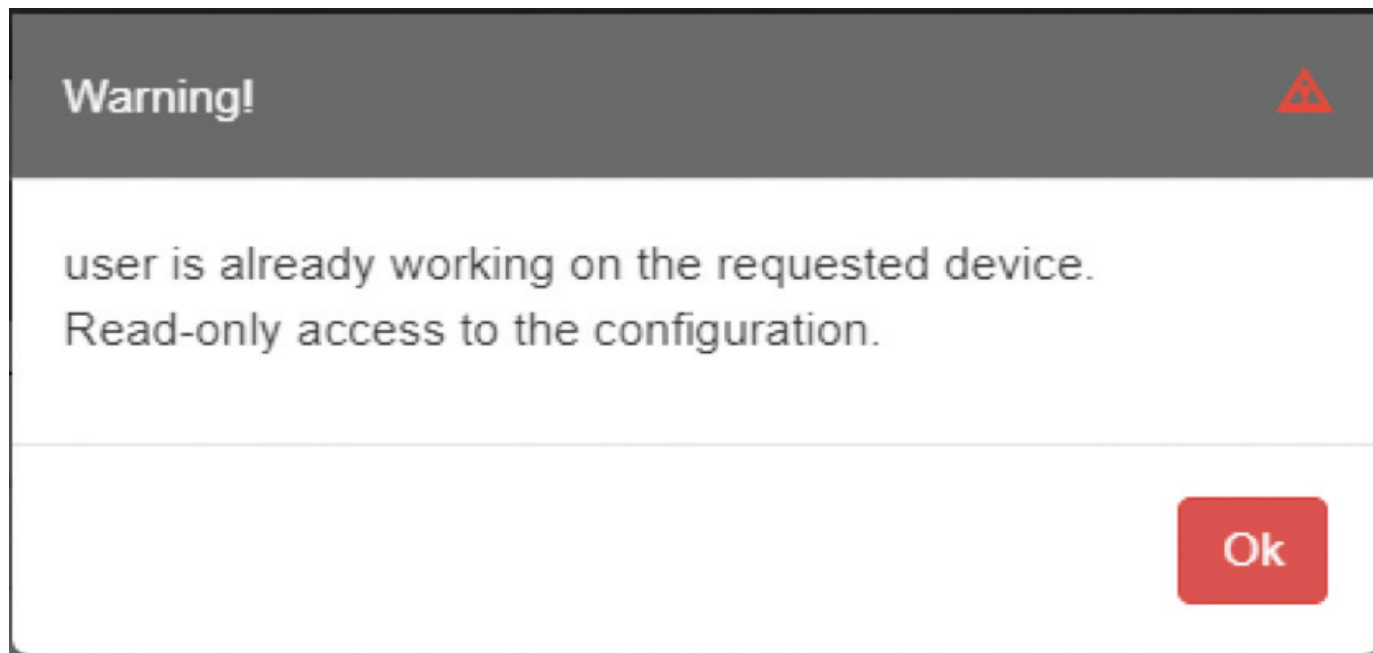
The web app allows the simultaneous display of a device/slave for several users, but, in order to avoid conflicts, it does not allow several users to configure and send commands to the same device and its slaves at the same time.

In the event in which user A attempts to enter the configuration section of a device/slave in which user B has already entered:

- User A will be notified via a message that the device is already in use by user B.
- User A accesses the configuration section without being able to make changes or send commands, but will only be allowed to view the data.

In the event in which user A attempts to enter the command sending section of a device in which user B has already entered:

- User A will be notified via a message that the device is already in use by user B.
- User A will not be able to access the command sending section but will only be able to view the history.



On the other hand, the web app allows several users to use all of the read-only features (variables, alarms, device status) and manage registries: in other words, all those features that do not directly affect the behaviour of the device/slave.

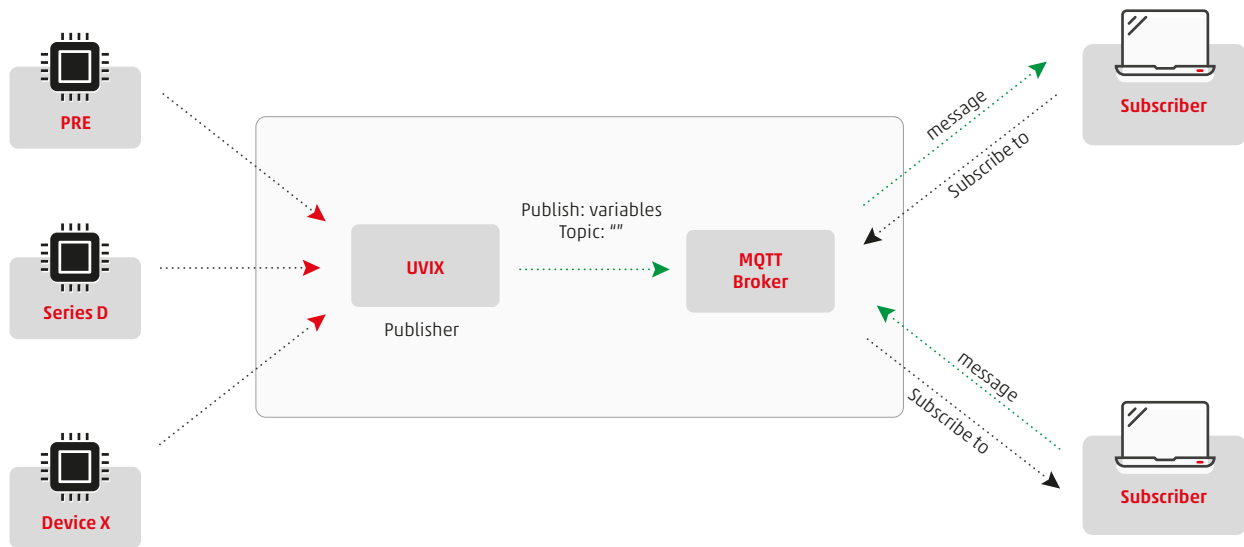
Note: If the user closes the browser or the tab without first exiting one of the exclusive management features of the device, the system will take a few minutes to realise that the device is, in fact, free to be used by other users. So it is advisable that, after configuring or sending commands to a device, the user exits these features.

4. MqttCustomer messages sent by UVIX Web Service Ver 1.0.1

The main objective of this manual is to describe how MQTT messages are sent by UVIX Web Service when the latter receives variable values

from devices connected to the system.

The MQTT (MqttCustomer) function may or may not be enabled.



4.1 Enabling MqttCustomer messages

To change the default configuration of UVIX Web Service, the configuration file ("config.xml"), correctly modified, should be placed in the "config" folder where the Web Service is installed.

The file path is: "C:\Program Files (x86)\CAMOZZI\UVIX\WebService\". The original "config.xml" file must be copied to the "config" folder and only subsequently modified.

4.1.1 MqttOn

The "MqttOn" parameter is used to enable / disable the management of the MqttCustomer.

The default value (0) indicates that the MQTT is disabled. To enable MqttCustomer the parameter must be set to 1.

4.1.2 MqttConnectionHost

The "MqttConnectionHost" parameter is used to configure the address of the device where the MQTT is installed. The default value (localhost)

is correct, assuming that the MQTT Broker is installed on the same machine where the UVIX Web Service is running.

4.1.3 MqttConnectionPort

The "MqttConnectionPort" parameter is used to configure the port on which the MQTT Broker is listening.

The default value (1883) is correct, assuming that the Web Service is attempting to connect to the MQTT Broker "Mosquitto", running with the default configuration.

4.1.4 MqttClientId

The "MqttClientId" parameter is only information sent by the MQTT Broker, when the connection is established, to identify the entity's connection.

It is suggested to maintain this default value.

4.1.5 MqttTopicPrefix

The "MqttTopicPrefix" parameter is the first part of the topic in which MQTT messages are printed.

The next chapter will better explain the topics used.

4.1.6 MqttReadClock

The "MqttReadClock" parameter is used for an alternative management of the MQTT, which will not be dealt with in this manual.

It is suggested to maintain by default the value of this parameter.

4.1.7 Example

Below is an example of the configuration section of the MQTT "config.xml" file where the MqttCustomer is enabled to send messages to the MQTT Broker when both are running on the same machine where the Web Service is present.

```

<!-- Mqtt -->
<!--Mqtt task enabled/disabled (0=disabled, 1=MqttCustomer enabled,
default:0)-->
<MqttOn>1</MqttOn>
<!--Host address for connection to Mqtt broker-->

```

```

<MqttConnectionHost>localhost</MqttConnectionHost>
<!--Port for connection to Mqtt broker-->
<MqttConnectionPort>1883</MqttConnectionPort>
<!--Client ID used when Mqtt messages are published-->
<MqttClientId>CamoZZiWebService</MqttClientId>
<!--Prefix of topics used for publishing messages-->
<MqttTopicPrefix>machine_data</MqttTopicPrefix>
<!--Value to assign to field ReadClock in Mqtt messages-->
<MqttReadClock>1000</MqttReadClock>

```

4.2 Printed messages

Assuming that the MQTT Broker is correctly running and that the UVIX Web Service is properly configured (see chapter 2) with the MqttCustomer and enabled to connect with the Broker, when the Web Service receives

variable values from devices connected to the UVIX system, it creates an MQTT package for each variable whose meaning follows very precise rules that are explained later in this chapter.

4.2.1 Message fields

Each MQTT message sent is made up of the following fields:

- TS: Date / Time of the message sent.
- DevGr: Name of the group to which the device belongs (e.g.: Totem, Pick&Place, Open Frame ..).
If no Device Group is assigned to the device, this field will automatically set to "Default Machine".
- DevSerNum: Serial Number of the Device (max 17 characters).
- DevName: Name of the device (empty if no name is assigned).
It can be assigned / changed using the UVIX WebApp.
- SlvId: Slave ID (0 if the variables refer to the master)
- SlvType: Code type of the slave (e.g.: Drcs, DSer, RegP, Bis, Mon...).
If the variables refer to the master, this field assumes the same value as "DevType".

- SlvName: Name of the Slave (empty if not previously assigned). It can be assigned / changed using the UVIX WebApp.
If the variables refer to the master, this field takes on the same value as "DevName".
- VarId: ID of the variable.
- VarVal: Value of the variable. This is the value received by the device, without any conversion.
For example, a DSer type device sends the value of the supply voltage of 242 for 24.2 Volts.

4.2.2 Topics

The topics on which MQTT messages are printed depend on two parts linked to a single topic:

- Prefix
- Device Group

The Prefix field can be set by modifying the configuration of the "MqttTopicPrefix" parameter (see chapter 2).

The Device Group corresponds to the "DevGr" field of MQTT messages. Device Group names can be added or changed using the UVIX WebApp which can also be used to assign devices to the chosen Device Group. Basically there will be a topic for each Device Group.

4.2.3 Examples

Below is an example of an MQTT message sent after the receipt of a variable with ID 6 relating to a "RegP" type device, which has been assigned to the Device Group "MqttTestDevGroup".

```
{ "TS": "2020-04-07T09:10:25", "DevGr": "MqttTestDevGroup", "DevSerNum": "PRE000000000000321", "DevType": "RegP", "DevName": "DevicePRE321", "SlvId": "0", "SlvType": "RegP", "SlvName": "DevicePRE321", "VarId": "6", "VarVal": "413" }
```

If the configuration of the "MqttTopicPrefix" parameter is set by default (machine_data /) the topic in which the previous message was printed will appear as: "machine_data / MqttTestDevGroup".

The following example will concern an MQTT message sent after receiving a variable ID 2 of the slave (Bis) with ID 1 belonging to a "DSer" type device (assigned to the Device Group "DSerDevices").

```
{ "TS": "2020-04-07T09:10:35", "DevGr": "DSerDevices", "DevSerNum": "DSER00000000000001", "DevType": "DSer", "DevName": "Multipolar 1", "SlvId": "1", "SlvType": "Bis", "SlvName": "Slave Bis number 1", "VarId": "2", "VarVal": "31" }
```

If the configuration of the "MqttTopicPrefix" parameter is set to its default value (machine_data /) the topic in which the previous message would be printed would appear as "machine_data / DSerDevices".

4.2.4 How to receive MQTT messages

To receive MQTT messages sent by the Web Service, an MQTT Client should be running and connected to identical MQTT Brokers where the messages are printed.

The MQTT client should subscribe to each topic used (one for each device group, as stated earlier).

If, for example, we have a UVIX system where all devices are assigned to both Device Groups "MqttTestDevGroup" or "DSerDevices" (or assigned to

no Device Group) and the configuration of the "MqttTopicPrefix" parameter is set by default (machine_data /), the MQTT Client should subscribe to the following topics:

- "machine_data/MqttTestDevGroup"
- "machine_data/DSerDevices"
- "machine_data/Default machine"

4.2.5 Description of the variables

For DevType: DSer

ID	Description
ID 1	Firmware version
ID 2	Temperature (°C)
ID 3	Supply Voltage (V)

For DevType: Cx04

ID	Description
ID 1	Firmware Version
ID 2	Temperature °C
ID 3	Supply Voltage V
ID 4	Supply Voltage logic V

For SlvType: Bis

ID	Description
ID 1	Firmware Version
ID 2	Sub-base temperature °C
ID 3	Cycles coil 14
ID 4	Cycles coil 12
ID 5	Health status coil 14 %
ID 6	Health status coil 12 %
ID 7	Status coil 14
ID 8	Status coil 12
ID 9	Internal Not Used
ID 10	Internal Not Used
ID 11	Internal Not Used
ID 12	Internal Not Used
ID 13	Temperature coil 14 °C
ID 14	Temperature coil 12 °C
ID 15	Errors coil 14
ID 16	Errors coil 12
ID 17	Communication retries
ID 18	Internal Not Used
ID 19	Internal Not Used
ID 20	Internal Not Used
ID 21	Internal Not Used

For DevTypes: RegP

ID	Description
ID 1	Firmware Version
ID 2	Hardware Version
ID 3	Product code
ID 4	Command signal
ID 5	Temperature °C
ID 6	Supply Voltage V
ID 7	Target pressure kPa
ID 8	Regulated pressure kPa
ID 9	Cycles charge coil
ID 10	Cycles exhaust coil
ID 11	Health status charge coil
ID 12	Health status exhaust coil
ID 13	Internal Not Used
ID 14	Internal Not Used
ID 15	Internal Not Used
ID 16	Internal Not Used
ID 17	Total work time charge coil
ID 18	Total work time exhaust coil

5. Main problems and solutions

The following chapter will address the main problems that may arise during or after installation, also indicating the main solutions that the

user can perform independently in order to get back up and running as quickly as possible.

5.1 The Camozzi device does not communicate via USB

This case includes the situation in which the Camozzi device is powered, the USB cable is connected, the Camozzi USB gateway software is started but no data arrives.

In this case, the device to be connected is not present in the "Open COMs" list of the USB gateway.

Open device manager and try to disconnect and reconnect the USB cable, if:

- The device management window does not update, this means that the system does not recognize any connected devices.

The problem may be due to the USB cable, it may not ensure suitable contact with the connector on the device.

It is recommended that you try another cable.

- The device management window updates but the correct driver is not recognized:

- virtual COM port

- ▼ Porte (COM e LPT)

- STMICROELECTRONICS Virtual COM Port (COM4)

- Firmware update (in the case of reprogramming, device in boot mode).

- ▼ Dispositivi USB (Universal Serial Bus)

- STM32 DownLoad Firmware Update

In this case the drivers have probably not installed correctly, and they can be installed manually.

In the case of the firmware update, launch the "STM32Bootloader.bat" file in the "DriversDFU" folder in the UVIX installation path.

In the case of virtual COM there is a difference based on the operating system. With windows 10 no drivers are needed and for this reason they are not present, with windows 7 or 8 there is a folder called "drivers" within the UVIX installation path.

If the problem persists, contact Camozzi assistance.

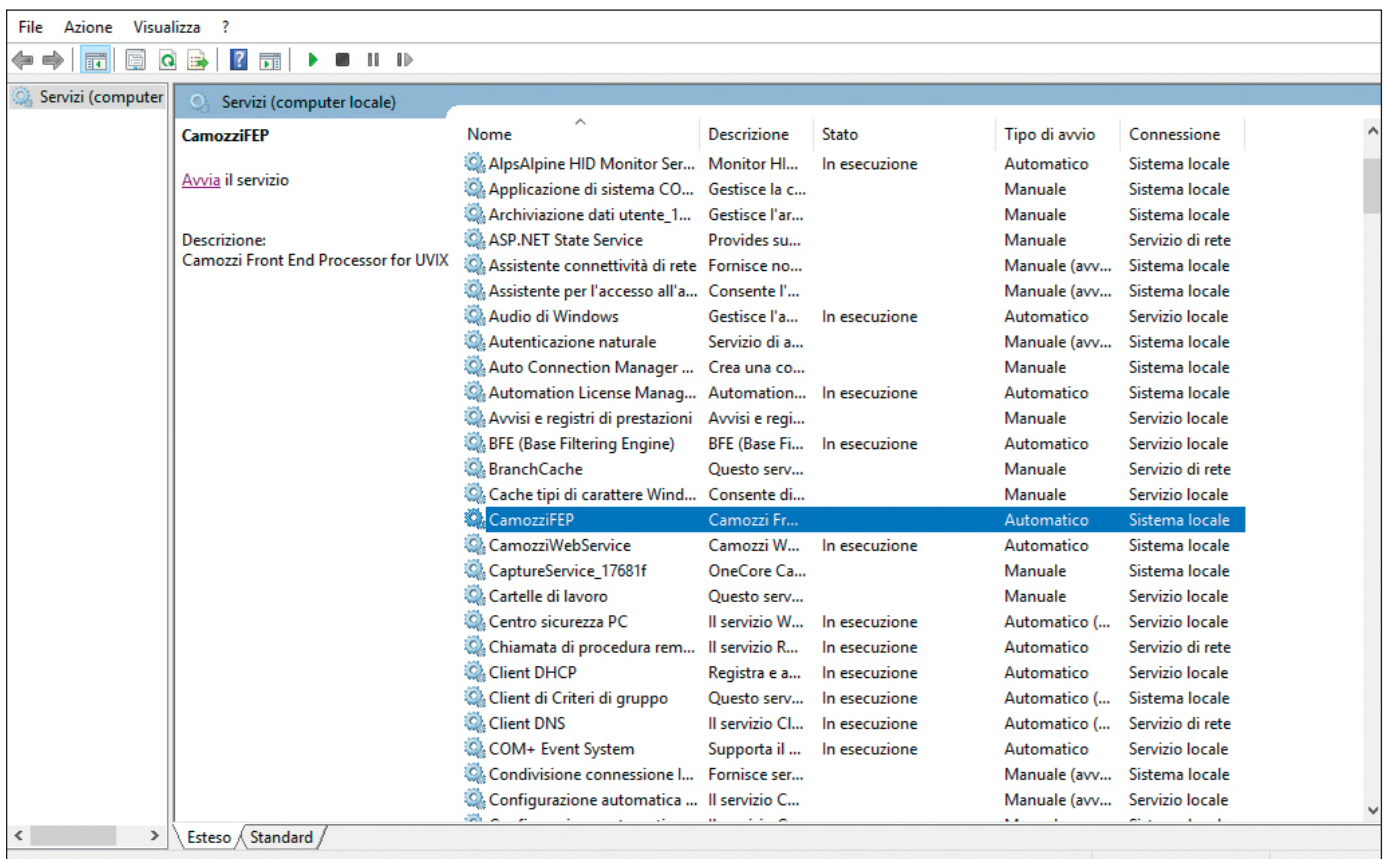


5.2 The Camozzi device does not communicate via wireless

If the device is equipped with a wireless module but does not communicate with the UVIX, check the following points:

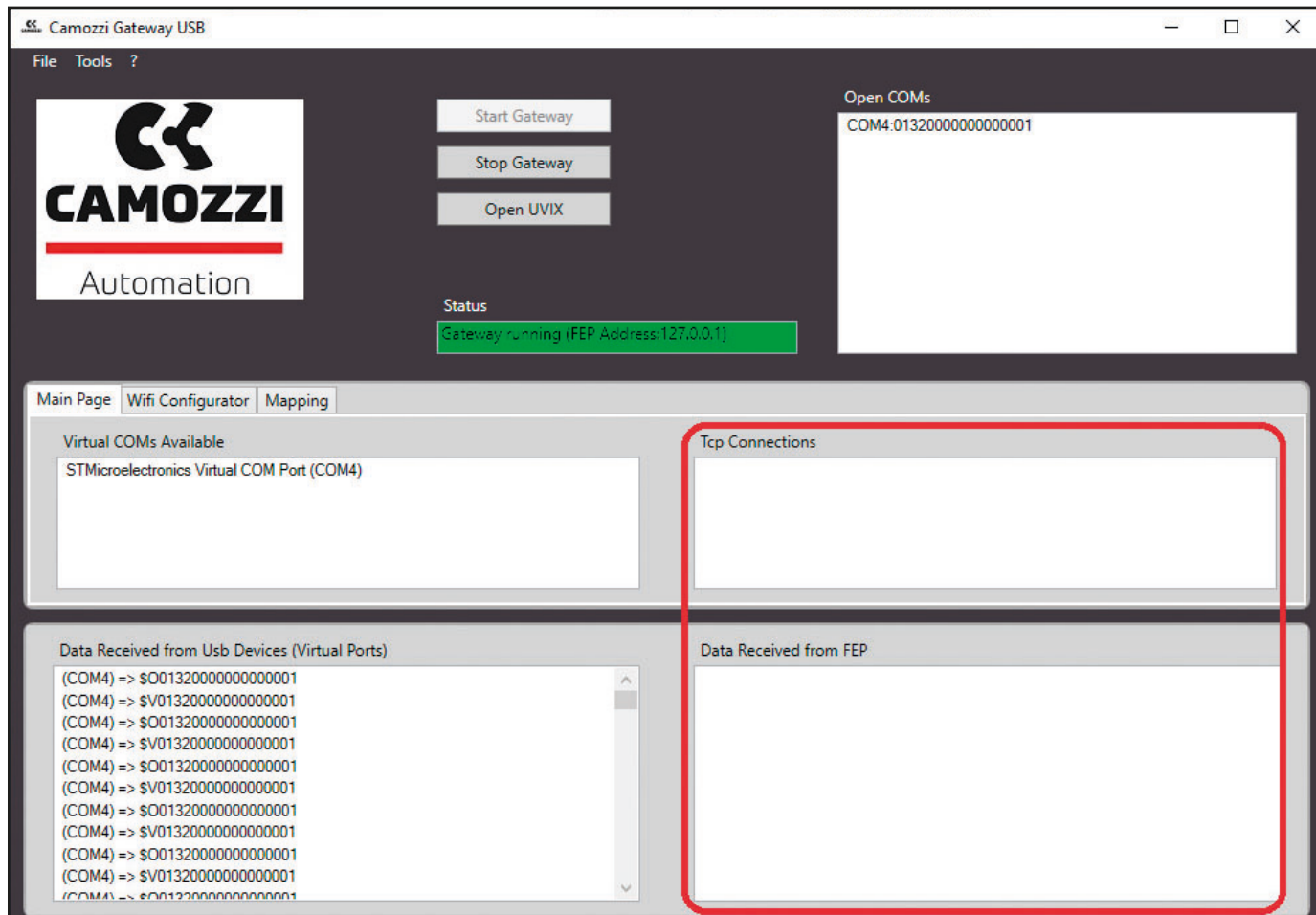
- The wireless network is present, and the signal is not too weak
- The SSID and password login credentials are set correctly on the device.
- The FEP address is set correctly on the device, (the IP address of the FEP must be static).

- Check that there are no firewalls or antivirus blocking the communication port.
- Check that the status of the "CamozziFEP" service is running from the system services.



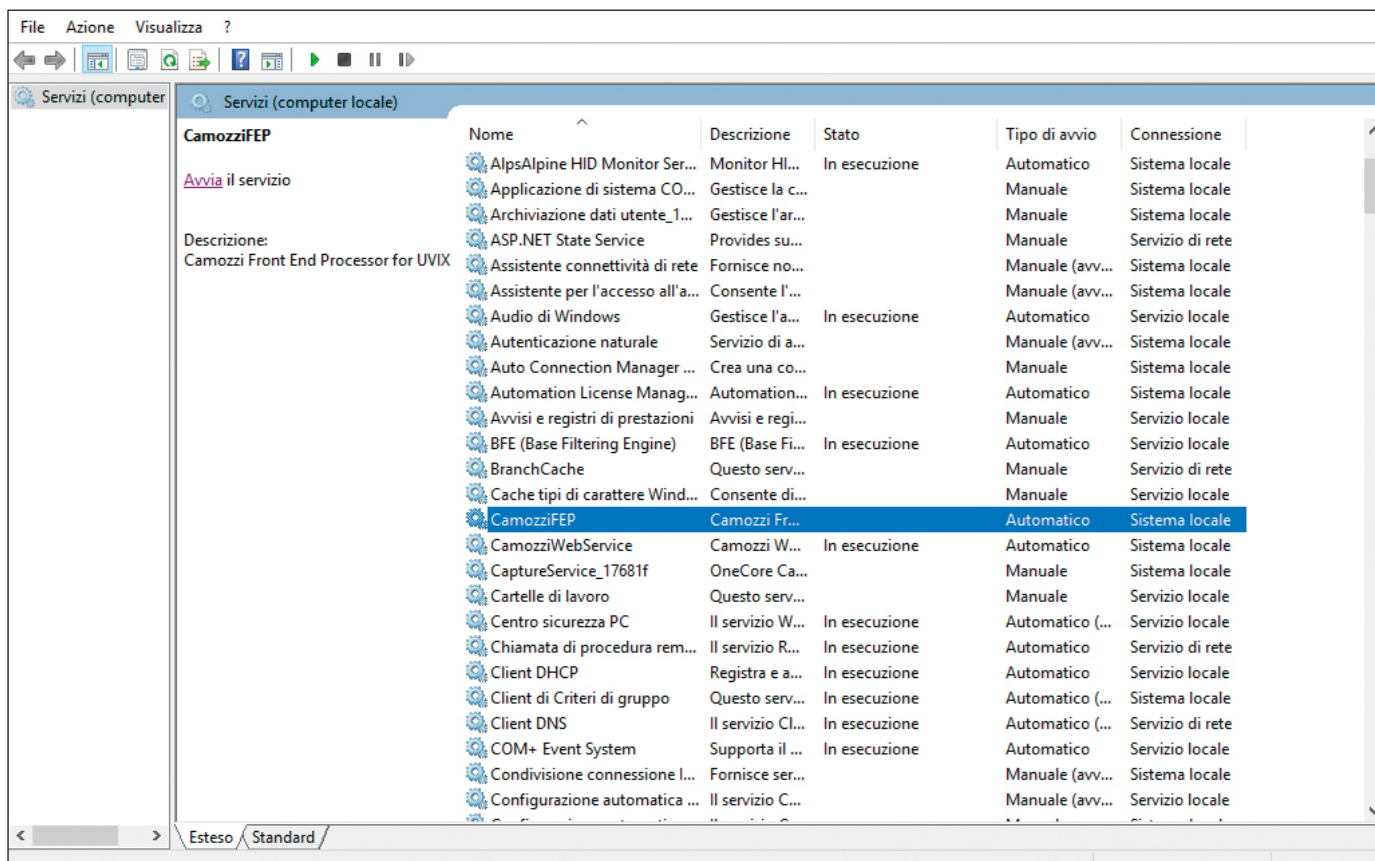
5.3 The Camozzi USB gateway software does not send data to the FEP

If the "Camozi USB Gateway" application is running, the COM of the device is detected correctly, and the data arrives correctly but the data is not sent to UVIX.



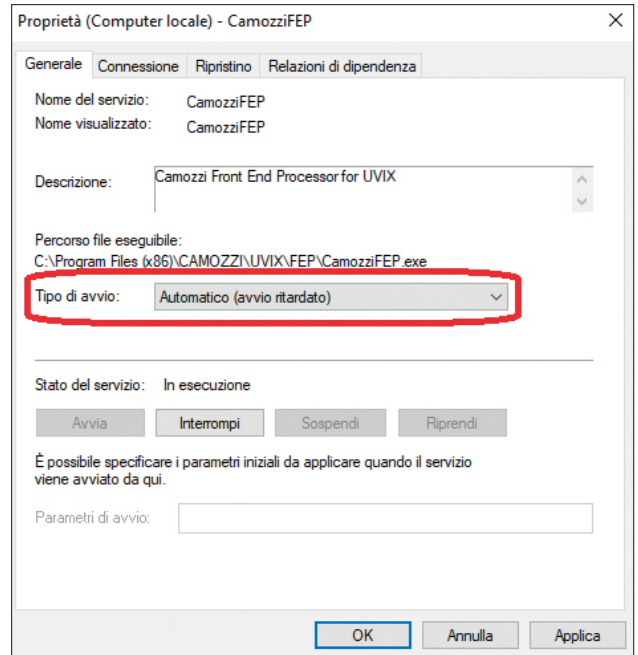
Check that the FEP address in "tools-> Settings" has been correctly configured.

Check that the status of the "CamoziFEP" service is running from the system services.



If the "Status" column is empty it means that it is not started, open the services with administrator privileges and try to start it manually.
 If the FEP does not start manually, a problem has occurred during the installation phase which must therefore be repeated.
 If the FEP must be started manually at each machine start-up, open the properties of the service (right mouse button and properties) and change the start-up type to "Automatic (delayed start)".

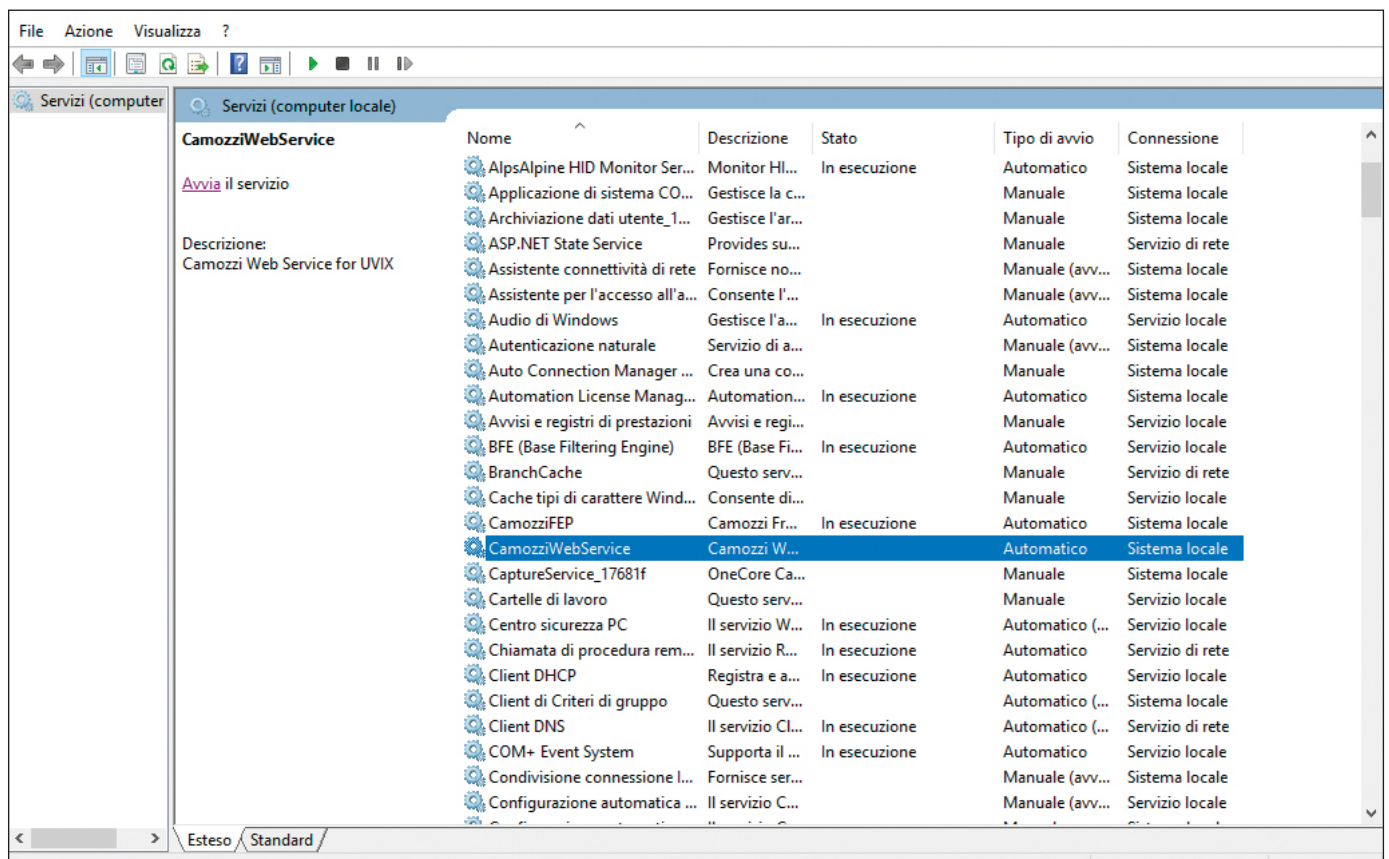
If the problem persists, contact Camozzi assistance.



5.4 Login failed on the UVIX web page

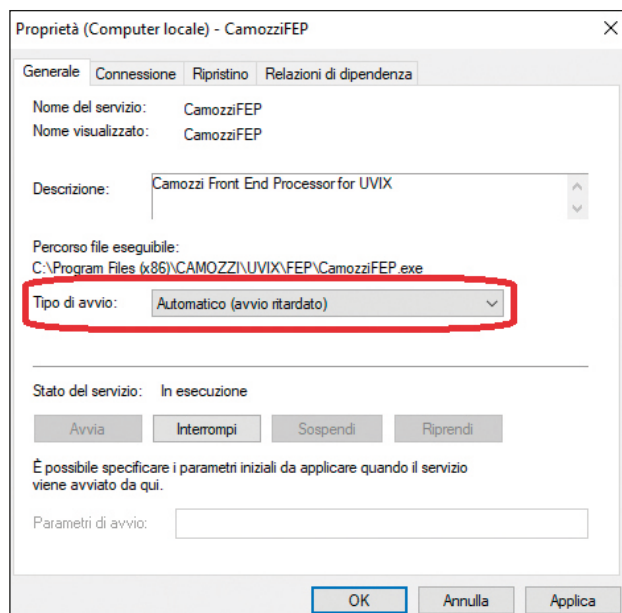


If the browser fails to access the UVIX login page, first check the credentials entered, then check that the status of the "CamozziWebService" is running.



If the "Status" column is empty it means that it is not started, open the services with administrator privileges and try to start it manually.
 If the Web Service does not start manually, a problem has occurred during the installation phase which must therefore be repeated.
 If the Web Service must be started manually at each machine start-up, open the properties of the service (right mouse button and properties) and change the start-up type to "Automatic (delayed start)".

If the problem persists, contact Camozzi assistance.



5.5 The web page is not visible

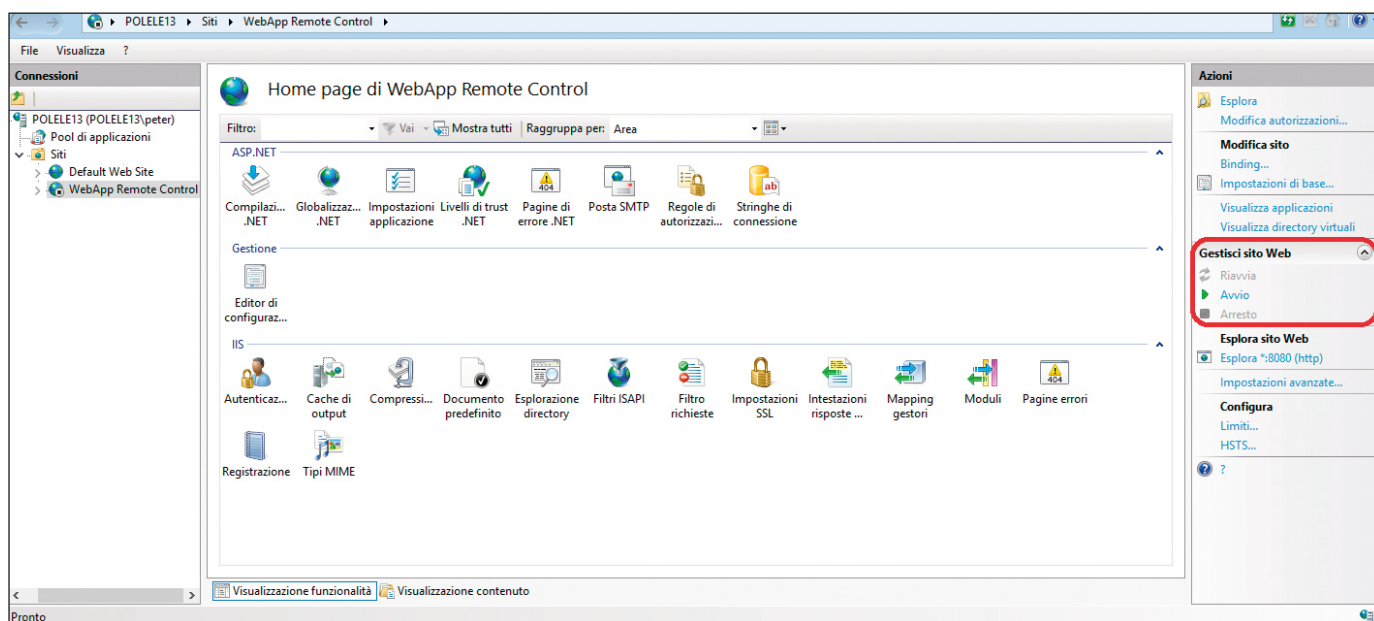
If you are unable to view the UVIX page from the browser



First make sure you have written the url correctly, then check the correct functioning of the web server used (windows IIS by default).
 Once the IIS has been opened in the "Sites" item, the "WebApp" must be present, if it is stopped it can be started manually using the "Start" command in the "Manage Website" menu.

In the event that the "WebApp" is not present in the "Sites" item, the installation was not successful and must be repeated.

If the problem persists, contact Camozzi assistance.



5.6 Not included in the previous

If all the services are running and the component settings are correct but despite the data are not being displayed on the Web App, then the problem could be on one or more ports used by UVIX which is occupied by another process or blocked by a firewall.

To resolve the problem, you need to add the necessary permissions on the firewall or modify the occupied port, for more details see the chapter "Detailed analysis".

If the problem persists, contact Camozzi assistance.

Contacts

Camozzi Automation S.p.A.

Via Eritrea, 20/I
25126 Brescia - Italy
Tel. +39 030 37921
www.camozzi.com

Customer Service

Tel. +39 030 3792790
service@camozzi.com

Product Certification

Information concerning
product certifications, EC standards,
conformity declarations and instructions
productcertification@camozzi.com



Automation

