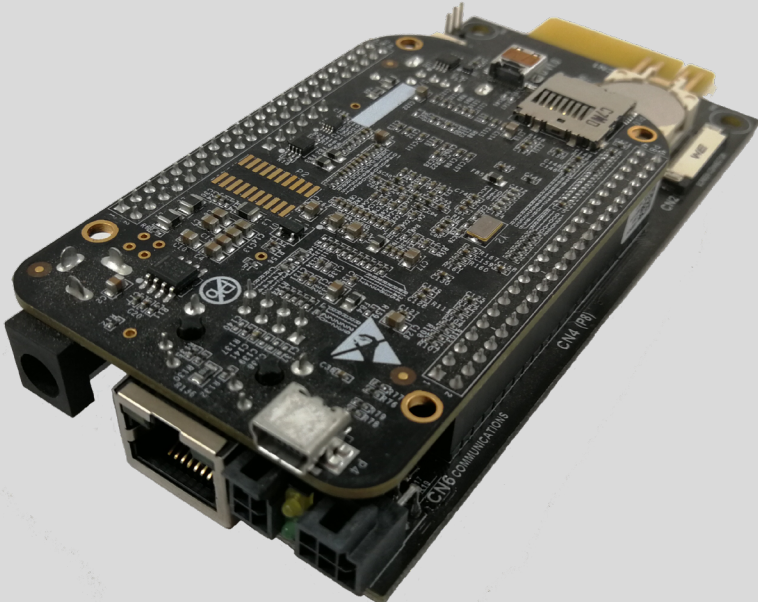


USER MANUAL



NIMBUS card

Contents

1. PRESENTATION.

- 1.1. VIEWS.
- 1.2. DESCRIPTION OF THE SYSTEM.
 - 1.2.1. Introduction.
 - 1.2.2. NIMBUS MAXI vs NIMBUS MINI compatibility.
 - 1.2.3. Features of the system.
 - 1.2.4. Optional systems.

2. INSTALLATION AND STARTUP.

- 2.1. INITIAL CONNECTION.
 - 2.1.1. Point-to-point connection (Ethernet cable).
- 2.2. INITIAL CONFIGURATION.

3. ONBOARD PANEL.

- 3.1. ACCESS TO THE PANEL.
 - 3.1.1. Import certificate.
 - 3.1.1.1. Internet Explorer.
 - 3.1.1.2. Mozilla Firefox.
 - 3.1.1.3. Chrome / Opera.
 - 3.1.2. Local connection (point-to-point).
 - 3.1.3. Remote connection.
 - 3.1.4. Supported browsers.
- 3.2. SCREEN LOGIN.
- 3.3. NAVIGATION TREE.
- 3.4. MONITOR.
 - 3.4.1. Diagram and measurements.
 - 3.4.1.1. ADAPT-X & ADAPT2 series.
 - 3.4.1.2. SLC CUBE4 7.5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2 and SLC TWIN RT2 series.
 - 3.4.2. Alarms.
- 3.5. DEVICE.
 - 3.5.1. Info (only for Engineer user).
 - 3.5.2. Register Settings (only for Engineer user).
 - 3.5.3. Measurements.
 - 3.5.3.1. ADAPT-X Series.
 - 3.5.4. Register Settings (only for Administrator and Engineer users).
 - 3.5.4.1. ADAPT-X Series.
 - 3.5.4.2. CUBE3 / CUBE3+ Series.
 - 3.5.4.3. X-PERT Series.
 - 3.5.4.4. DC-S Series.
 - 3.5.5. Metrics.
 - 3.5.6. Manage alarms (DC-S series only).

- 3.5.7. Actions (DC-S series only).
- 3.5.8. Logs (DC-S series only).
- 3.5.9. Backup (DC-S series only).
- 3.6. SYSTEM (ONLY FOR THE ENGINEER USER).
 - 3.6.1. Network.
 - 3.6.1.1. Through DHCP.
 - 3.6.1.2. Through static IP.
 - 3.6.2. Date and time.
 - 3.6.3. RCCMD (Optional service).
 - 3.6.4. Services.
 - 3.6.5. SNMP (Optional service).
 - 3.6.6. MODBUS.
 - 3.6.7. Select model.
- 3.7. LOGOUT.

4. INSTALLING THE RCCMD SOFTWARE.

- 4.1. INSTALLING THE SOFTWARE.
 - 4.1.1. Windows.
 - 4.1.2. Unix and Linux.
 - 4.1.3. MacOS.
- 4.2. SOFTWARE CONFIGURATION.
 - 4.2.1. Sender IP.
 - 4.2.2. Sender port.

5. ACTIVATION OF CONTRACTED SERVICES.

6. APPENDIX I. CONNECTIVITY

- 6.1. NETWORK FIREWALL REQUIREMENTS.
 - 6.1.1. Option 1 (recommended): full opening of ports 443 and 8883.
 - 6.1.2. Option 2 (not recommended): list of google hostnames and ports.
- 6.2. USE OF AND ACCESS TO THE REMOTE MAINTENANCE PORTAL.
 - 6.2.1. Creating an account.
 - 6.2.2. Registering the device in the cloud.
 - 6.2.2.1. Manual registration through the remote maintenance portal.
 - 6.2.2.2. Automatic registration with QR Code.
 - 6.2.3. Creating notifications associated with a device.
 - 6.2.3.1. Web notifications.
 - 6.2.3.2. Email notifications.
 - 6.2.3.3. SMS notifications.
 - 6.2.4. Password recovery.

7. APPENDIX II. GENERAL TECHNICAL SPECIFICATIONS.

1. PRESENTATION.

1.1. VIEWS.

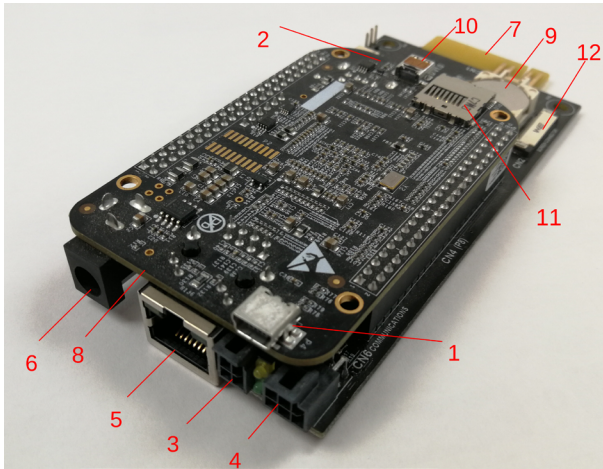


Fig. 1. View of the NIMBUS MAXI card.

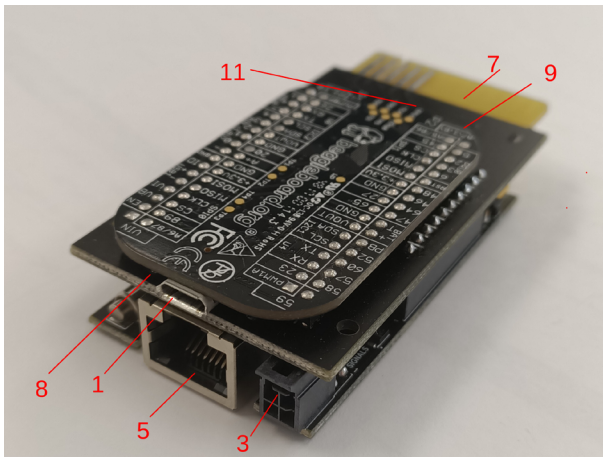


Fig. 2. View of the NIMBUS MINI card.

Description	Function
1 COM1 port	Serial interface to connect the card to other devices using a mini USB cable.
2 COM2 port	Serial interface to connect the card to other devices using a USB cable.
3 RS-232 port	Serial interface to connect the card using the RS-232 protocol.
4 RS-485 port	Serial interface to connect the card using the RS-485 protocol.
5 RJ-45 port	10/100Mbit Ethernet interface.
6 External DC input	Powered by a 5V adapter.
7 Modbus port	Serial interface for modbus communication with the device. Powers the card internally.
8 Power LEDs	Turned on when the card is powered with the DC input (internal or external).
9 RTC	Real-time clock to keep the time of the card updated in case of mains failure.
10 HDMI port	HDMI interface to connect the card using an HDMI micro cable.
11 MicroSD connector	Enables the NIMBUS card version to be updated using a MicroSD.
12 Display connector	Connector for flat bus cable to connect the card to an LCD.

Tab. 1. Description of the constituent parts

1.2. DESCRIPTION OF THE SYSTEM.

1.2.1. Introduction.

The SALICRU devices are usually installed in locations far away from the area of production, which means that information provided by the device about its status can often be overlooked. The NIMBUS card solves this problem by offering a remote maintenance service that provides real-time information about the current status of the device.

Remote communication with the device enables maintenance and repair work to be carried out without the need to travel to the installation site to find out about its status.

The functionalities of the NIMBUS card are specially designed to work with SALICRU devices, making it currently compatible with the following series:

- DC POWER-S
- DC POWER-L
- SLS CUBE3 / CUBE3+
- SLC CUBE4
- EMI3
- SLC ADAPT/X
- SLC ADAPT2
- SLC X-PERT
- SLC X-TRA
- SLC TWIN RT2
- SLC TWIN PRO2
- SLC TWIN/3 PRO2

1.2.2. NIMBUS MAXI vs NIMBUS MINI compatibility.

Depending on the type of device, either a NIMBUS-MAXI card or a NIMBUS-MINI card is required. Both have the same functionalities and the same operating mode. To determine how each card corresponds to the different compatible series, please refer to the following table:

	Nimbus MAXI	Nimbus MINI
UPS 3x400/230 V		
SLC CUBE3/3+	X	-
SLC X-PERT	X	-
SLC X-TRA	X	-
SLC ADAPT-X	-	X
SLC ADAPT2	-	X
SLC CUBE4	-	X
SLC TWIN RT2	-	X
SLC TWIN PRO2	-	X
SLC TWIN/3 PRO2	-	X
DC Systems		
DC POWER-S	X	-
DC POWER-L	X	-
Voltage stabiliser		
EMi3	X	-

Tab. 2. Compatibility table (X Compatible, - Not compatible)

1.2.3. Features of the system.

The NIMBUS card features various basic integrated services to enable basic connection to the device.

Basic service	Description
Onboard panel	Web panel that enables remote monitoring of the device. As it is dependent on the NIMBUS card, if it is not connected it will not be possible to access the panel.
Communication through MODBUS	Reading data through MODBUS.
RTC	The card's internal real-time clock.
Auto-configuration of the device	When installing the card in any of the compatible devices, it will automatically detect which device it is.
Alarm notification	Notification alert through the onboard panel in real time.
DNS server	Possibility of assigning domain names to the device.
IP address	Choice of DHCP or static web address.

Tab. 3. Basic integrated services

1.2.4. Optional systems.

Although the NIMBUS card is already capable of providing remote maintenance with the basic features of the system and access to device data, these optional systems make it more effective.

There are two types of optional systems:

- **Communication protocols:** improve the adaptability and compatibility of the card with different industrial communication protocols.
- **Web panel in the cloud:** it allows you to monitor all devices from a single web page, without having to go through them one by one to detect problems. It allows you to receive more advanced notifications: web push, email or SMS.

The **remote maintenance with the web panel** also offers faster technical support in real time as it is a web page to which SALICRU's professionals have access. This reduces the average time it takes to repair a device in unexpected cases.

Optional service	Description
Communication protocols	
Modbus TCP	Secondary communication protocol derived from MODBUS (main communication protocol).
Modbus API-REST	By enabling the external connection of the card, it is possible to make calls to the communication services without having to access the inside of the card.
RCCMD	This service enables you to perform a controlled shutdown of the servers, in the event that certain conditions are detected by the device.
SNMP	Secondary communication protocol. This enables notifications to be sent to the user's IP when an alarm is activated.
Web panel in the cloud	
Panel	Web panel in the cloud with access to all contracted devices with active NIMBUS card.
Alarm notification	Notification alert via web page, email and SMS.

Tab. 4. Optional services available

2. INSTALLATION AND STARTUP.

1. Remove the protective plastic from the battery from the NIMBUS card.

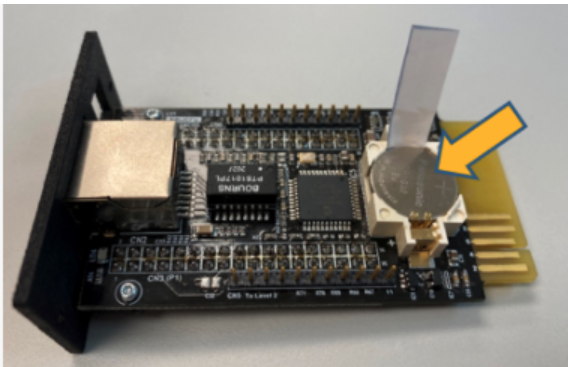


Fig. 3. Unlocking the battery of the NIMBUS card

2. Insert the NIMBUS card into the appropriate slot of the device. It needs to be well inserted.

The card will be powered directly by the device, meaning that no external power is necessary. If the card has been correctly inserted, the power LEDs will light up. See the red box in Fig. 4.

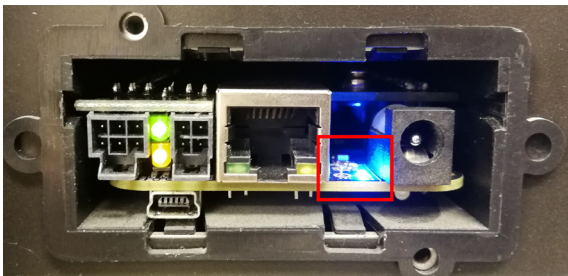


Fig. 4. NIMBUS card inserted into its slot

3. Connect one end of an RJ45 cable to the card and the other end to the Ethernet socket. The RJ45 port lights on the card should light up. See the red box in Fig. 5.

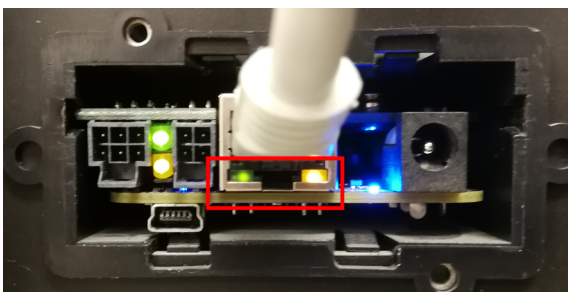


Fig. 5. Connection of the RJ-45 cable

4. Once the NIMBUS card is correctly powered by the device, it will be ready for use. The NIMBUS card will come with the latest available version already installed by default.

Once the NIMBUS card protective cover is in place, it should look like the image shown in Fig. 6.

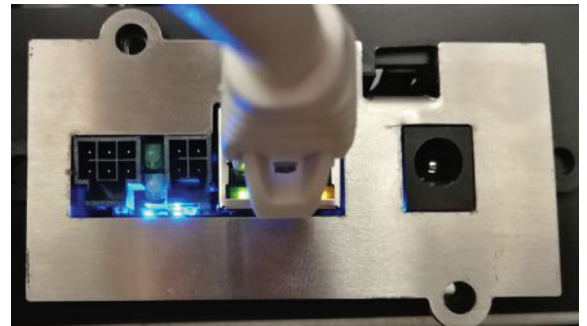


Fig. 6. The NIMBUS card with protective cover in place.

2.1. INITIAL CONNECTION.

Important: The card has a preset IP address to enable initial connection. This address is fixed and always available; however, it is necessary to configure a secondary IP address in order to use the card correctly.

Once the NIMBUS card has been correctly installed in the device via the corresponding slot, an available IP address must then be correctly configured in order to gain remote access to the card's onboard panel. There are two ways to do this.

2.1.1. Point-to-point connection (Ethernet cable).

The fixed IP is always available at the address 100.0.0.1. To access it, connect one end of the Ethernet cable to the dedicated slot on the NIMBUS card and the other end to your computer.

Configure the point-to-point connection by accessing network connections and creating a new connection with the following parameters:


Address	Netmask	Gateway	Metric
100.0.0.2	255.255.255.0	100.0.0.1	

Fig. 7. Network parameters for point-to-point connection.

After you have correctly created the point-to-point connection, you should be able to access the NIMBUS card via this IP address. If you access the card via this address in the web browser (<https://100.0.0.1>), change the card's final address in the panel's 'Network' section (3.5.1 Network).

2.2. INITIAL CONFIGURATION.

The NIMBUS card comes already configured with the necessary parameters so that you can immediately use the onboard panel and all of its functionalities.

These are the following:

- Auto-configuration of the device into which it is installed.
- NTP servers.
- Active communication services (**Modbus**).
- IP address by DHCP (**default**).
- Active RTC.
- Slave modbus address default to 1 and other communication parameters adapted to the needs of each device.

Any of these parameters can be modified at any time. For more information, see section 3.5 System.



Keep in mind that modifying some parameters could cause the panel to behave incorrectly. Do not modify them if you are unsure of your actions.

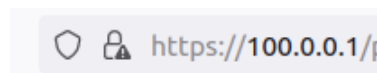
3. ONBOARD PANEL.

This service allows you to monitor the status of the device remotely and in real time, enabling you to directly access the device without having to be at the installation site.

3.1. ACCESS TO THE PANEL.

Once the card is correctly installed in the device, follow the steps detailed below. After making the initial connection between the card and the device, wait around five minutes before accessing the card via the panel.

Access to the panel is through `https://`, meaning that you need to write it before the card's IP address every time you wish to access the panel. Otherwise, correct connection will not occur. If you have not yet configured the card correctly for your network, please refer to section "2.1 Initial connection". You must use the following IP address:



Access to the panel is through a self-signed https certificate, meaning that the browser will identify it as not secure. To remove this warning, follow the steps described below.

3.1.1. Import certificate.

Depending on the browser you use for access, you will see one of the following messages. Refer to the corresponding section according to your browsing preferences.

i It is only necessary to import the certificate once with any of the browsers. The system will save the certificate for all of them. If the certificate has already been imported into the computer and an attempt is made to reimport it, the option will be shown as locked (Fig. 8).

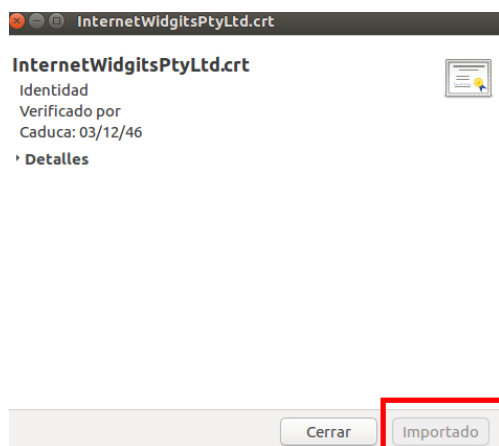


Fig. 8. Screen for importing the certificate locked.

3.1.1.1. Internet Explorer.

Run Internet Explorer as administrator. To do this, search for 'Internet Explorer' using the system search function, right click and select the 'Run as administrator' option, as shown in Fig. 9.

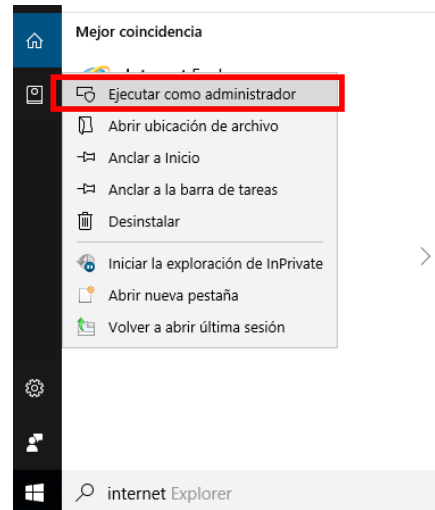


Fig. 9. 'Run as administrator' screen

- Access the panel normally. An error window will be displayed. Click on 'Continue to website (not recommended)'.
- The web page of the panel will load normally. In the address bar, it will appear a message with 'Certificate error'; you must click there (Fig. 10).

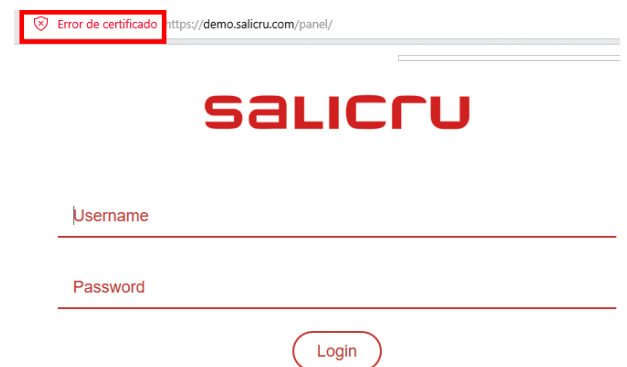


Fig. 10. Certificate error.

- A window will be displayed. Click on 'View certificate' and then on 'Install certificate'. Lastly, click on 'Yes' to confirm the installation.
- Restart the browser and access the panel. This time, the warning message will not be displayed.

3.1.1.2. Mozilla Firefox.

- The first time you access the panel, you will see the following screen. Click on 'Advanced...' to display more options.

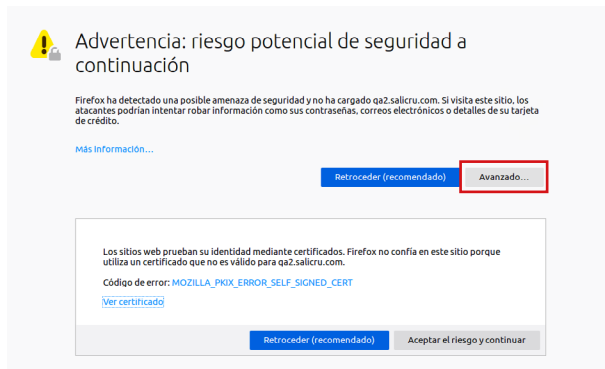


Fig. 11. Mozilla Firefox panel

Once all the options have been displayed, click on 'View certificate'.

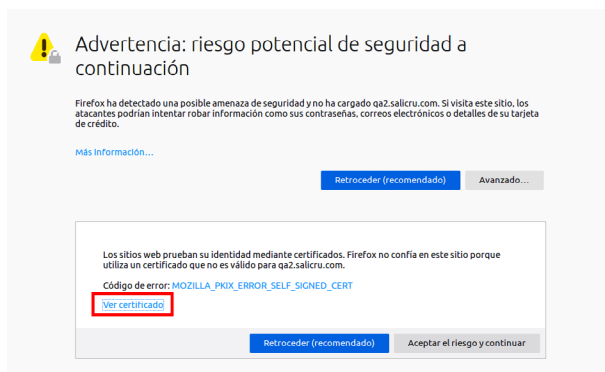


Fig. 12. Mozilla Firefox panel

- A new screen will appear with all of the information about the site certificate. Click on the 'Details' tab and select the 'Export...' option that appears at the end of it.

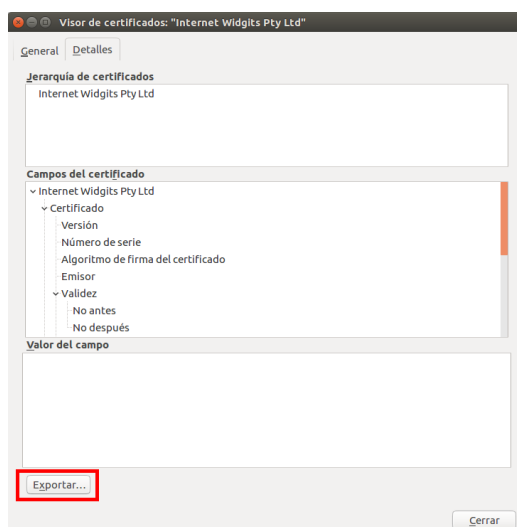


Fig. 13. 'Export ...' window

- Save and download the file to the desired location, then run it. A screen similar to the one shown in Fig. 14 will appear. Click on 'Import...'

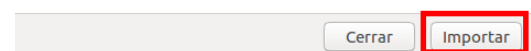
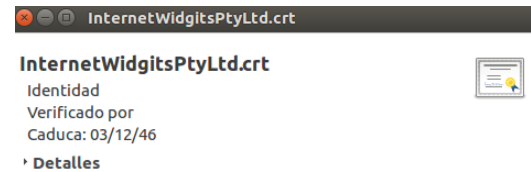


Fig. 14. 'Import...' window

- The system will require the password of your computer before proceeding. When prompted for the label, enter 'Nimbus' and click on 'OK'.

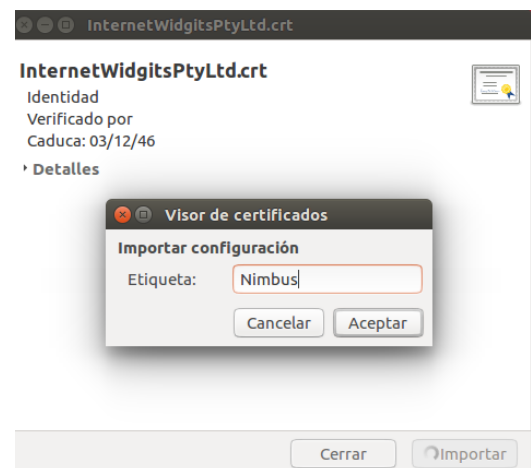


Fig. 15. 'Label' window.

- Once this step is completed, the certificate will have been imported correctly. Start the browser to confirm it. In 'Preferences', click on the left-hand side menu to navigate to 'Privacy & Security'. Navigate to the end of the tab until you find the section of 'Certificates'. Click on 'View certificates...' (Fig. 16).

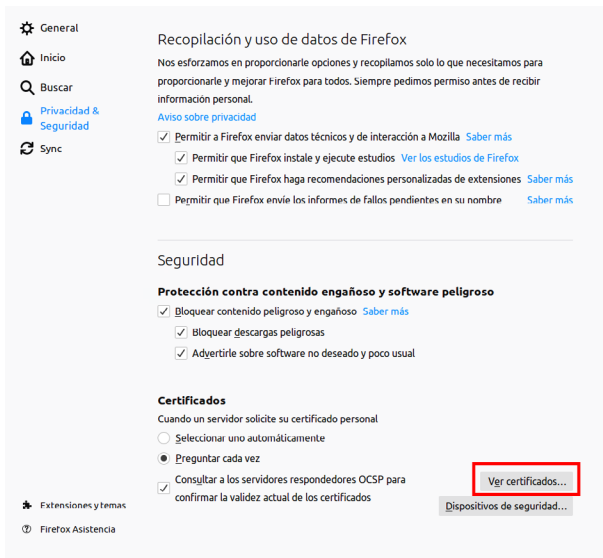


Fig. 16. Firefox 'Privacy & Security' menu

- Look for the name of the installed certificate on the list to check that it was correctly imported:



Fig. 17. 'Certificate manager' window.

- Restart the browser, access the panel and click on 'Accept the risk and continue'. The next time you access the panel, the warning message will no longer be displayed:

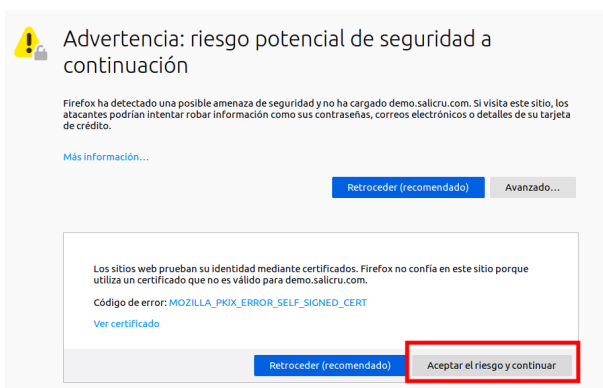


Fig. 18. 'Accept risk and continue' window

3.1.1.3. Chrome / Opera.

- The first time you access the panel, the following screen will be displayed:

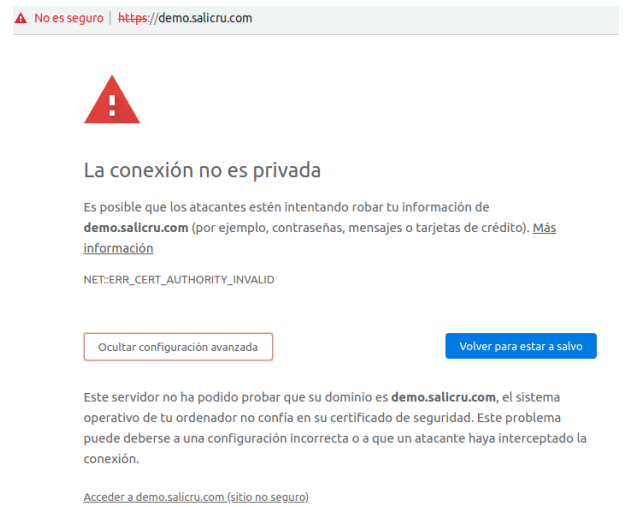


Fig. 19. Chrome / Opera browser home screen.

- In the address bar, click on the 'Not secure' button to display the available options. Click on 'Certificate'.



Fig. 20. Available options window

- A new screen will appear with all of the information about the site certificate. Click on the 'Details' tab, followed by the 'Export ...' button that appears at the end of it (Fig. 21).

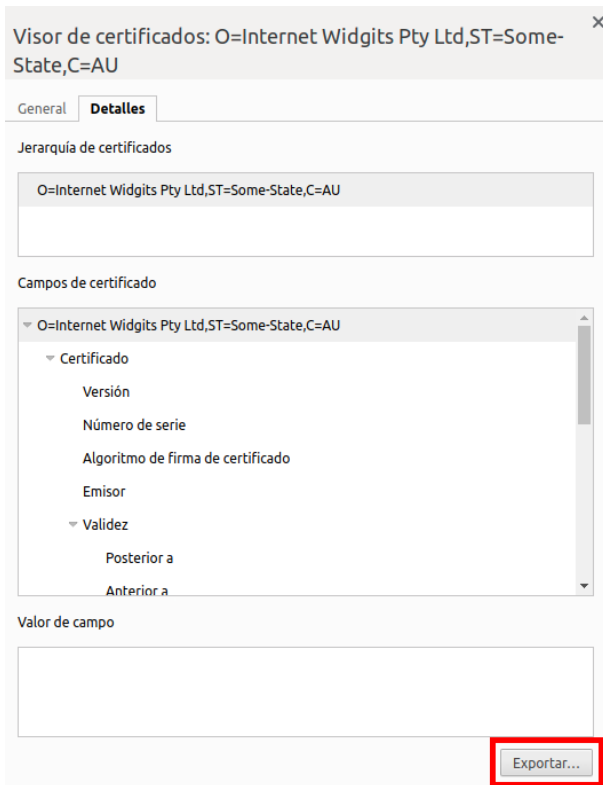


Fig. 21. 'Certificate viewer - Export' screen

- Save and download the file to the desired location, then run it. It will appear a screen similar to the one shown in Fig. 22. Click on 'Import...'

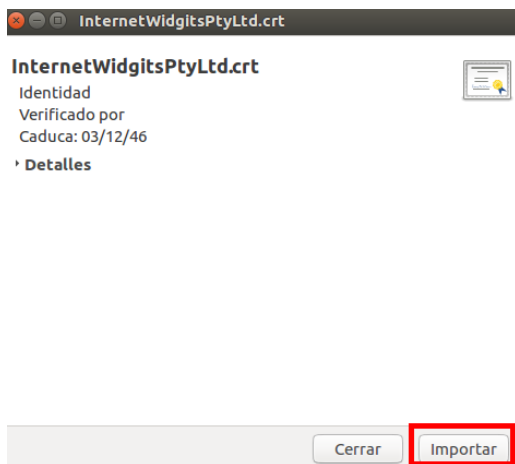


Fig. 22. 'Import ...' screen.

The system will require the password of your computer before proceeding. When prompted for the label, enter 'Nimbus' and click on 'OK', as shown in Fig. 23.

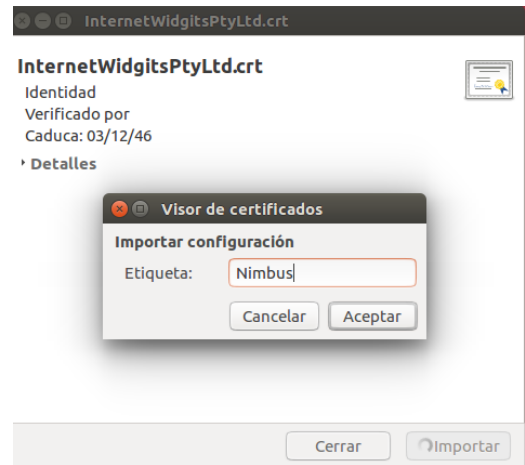


Fig. 23. 'Certificate viewer' screen

- Once this step is finished, the certificate will have been imported correctly. Restart the browser to confirm it. In 'Settings' navigate to the bottom of the page, access the advanced options and click on the 'Manage certificates' button. The certificate should appear in this section.

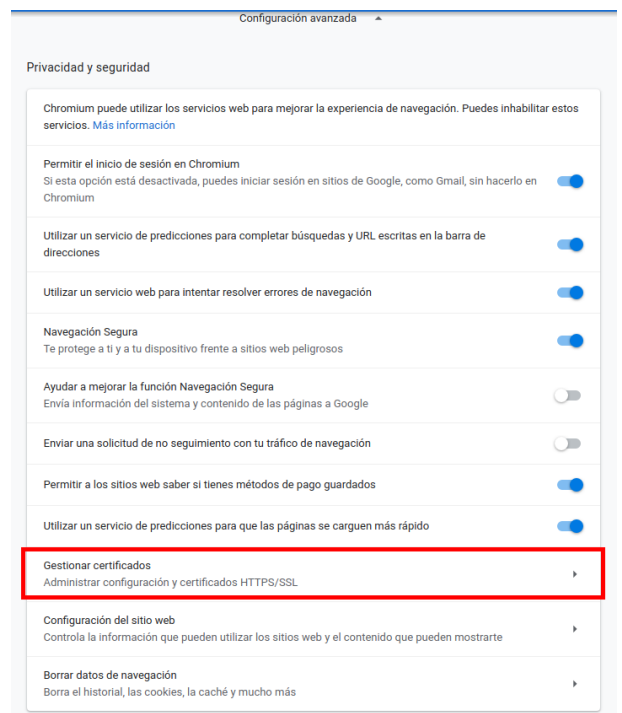


Fig. 24. 'Advanced settings - Manage certificates' screen.

- Restart the browser, access the panel and click on the 'Accept the risk and continue' button. The next time you access the panel, the warning message will no longer be displayed. (Fig. 25).



La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de **demo.salicru.com** (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET:ERR_CERT_AUTHORITY_INVALID

Ocultar configuración avanzada

Volver para estar a salvo

Este servidor no ha podido probar que su dominio es **demo.salicru.com**, el sistema operativo de tu ordenador no confía en su certificado de seguridad. Este problema puede deberse a una configuración incorrecta o a que un atacante haya interceptado la conexión.

Acceder a demo.salicru.com (sitio no seguro)

Fig. 25. 'Warning message' screen.

There are two ways of connecting to the panel depending on the accessibility of the device.

3.1.2. Local connection (point-to-point).

Choose this option if the card has no external access to the network.

1. The card's IP address is always set to 100.0.0.1. To connect to your subnet, you must create a new network connection with the following parameters.

Address	Netmask	Gateway	Metric
100.0.0.2	255.255.255.0	100.0.0.1	

Fig. 26. Network parameters for point-to-point connection.

2. Connect the Ethernet cable from the communications card directly to your computer, or to a switch that allows you to use it as an access point.
3. Once the network is correctly configured on your computer, and without any other possible internet source (disconnect the wifi if necessary), enter the address (<https://100.0.0.1>) in your browser.

3.1.3. Remote connection.

Use this option if the Ethernet connection is available or if you wish to access the panel remotely.

1. Start the web browser of your choice. If you use IE11, refer to section 3.1.3 Supported browsers.
2. Enter the IP address assigned to the card, previously assigned and established using the method described in section "2.1 Initial connection".
3. If the card has a dynamic address and the connection to the panel is not successful, make sure that this address is correct. To do this, follow the steps described in the previous section (3.1.1 Local connection).

3.1.4. Supported browsers.

All browsers are supported for displaying the onboard panel.



Only if you use Internet Explorer 11 you should follow these steps to ensure full functionality:

1. Click on the button in the top right-hand corner.
2. From the menu, select 'Internet Options'.
3. Locate the section 'Search History', in the general tab, and click on 'Options'.
4. In the tab 'TemporaryInternetFiles', Fig. 27, confirm the option shown in the image.

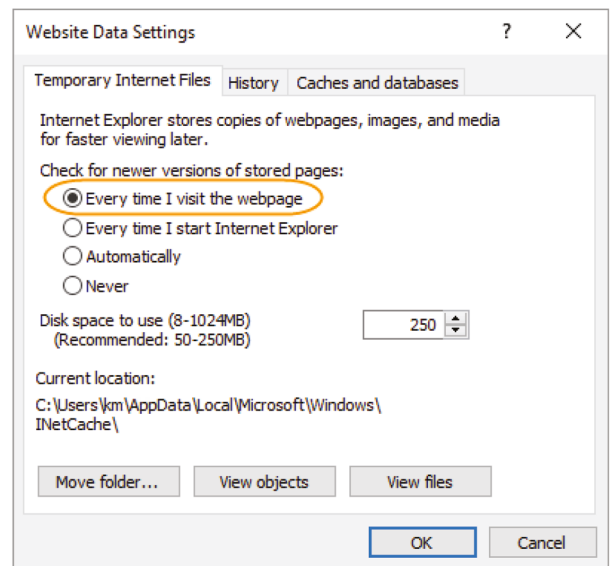


Fig. 27. Temporary settings menu

5. In the tab 'Cache and databases', Fig. 28, verify that the option indicated in the image is not selected.

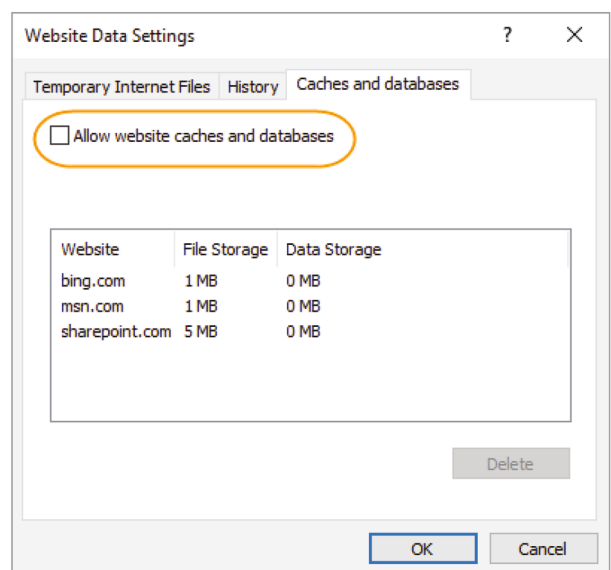


Fig. 28. Cache and Databases menu

6. Confirm all of your changes by clicking on the 'OK' button.
7. Delete the browser's cache memory.

3.2. SCREEN LOGIN.

Once the card's web address has been entered in the browser, the following page will be displayed:

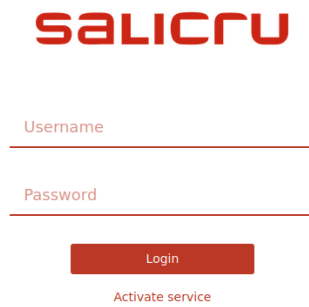


Fig. 29. Login and password screen

To log in, enter the corresponding credentials according to who will be using the panel.

	Engineer	User
Username	engineer	guest
Permission	<ul style="list-style-type: none"> - Modify some device parameters. - Modify NIMBUS card parameters. - Measurements display. 	<ul style="list-style-type: none"> - Only display device measurements.

Tab. 5. Credentials and permissions.

Once any of the passwords have been correctly entered, it will be shown the main page of the panel described in 3.4 Monitor.

3.3. NAVIGATION TREE.

You will find the navigation tree on the left-hand side of the screen. It will be displayed like this after logging in **as an engineer**. The System section will not be visible if you access the panel as User.

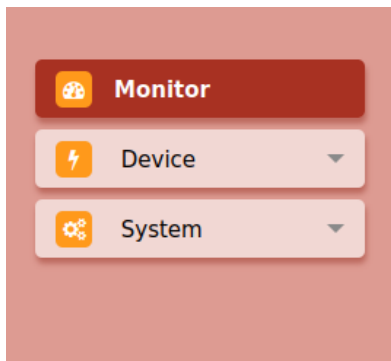



Fig. 30. Embedded panel main navigation tree.

Note that the Device and System sections are drop-downs. By clicking on them, the other options will be shown.

 It will only be displayed in this way if you have logged in as Administrator. The section 'System' will not be visible if you access the panel as Engineer or User.

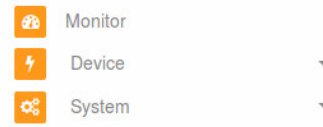



Fig. 31. Navigation tree


Note that the sections 'Device' and 'System' are drop-downs. By clicking on them, the other options will be shown.


 To avoid long navigation trees, which can lead to confusion, only one overall section at a time can be displayed. Within the section 'Device' you can continue to display the section 'Metrics'.

3.4. MONITOR.

The 'Monitor' page in Fig. 28 shows a summary of the current status of the device.

The first time you connect the card to the device, it will be configured automatically depending on the device you are working on. Keep in mind that this process usually takes a few minutes. If you cannot view the alarm block or any other part of this window correctly, exit the panel using the logout option and re-enter.

 If you are still unable to view a particular part of the panel correctly, delete the browser cache memory and press CTRL + F5.

 **Important:** if you have not acquired additional measurement modules for certain series, such as the SLC XPERT, the value corresponding to that measurement will be negative. In this consideration, the battery current, which can assume a negative value when it is discharged, is excluded.

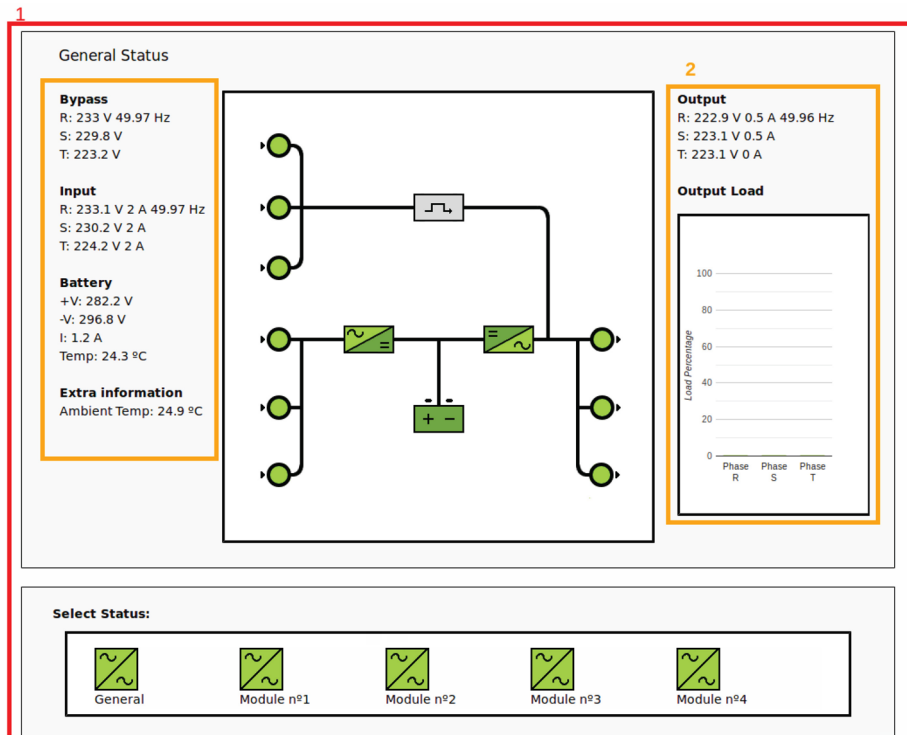


Fig. 32. UPS monitor diagram.

This page has two basic parts:

3.4.1. Diagram and measurements.

A schematic diagram of the device is shown at the top of the screen (block 1 in Fig. 32). The different states of the device are listed here with different colours:

- Red:
 - For elements other than the battery: there is a failure in this part.
 - For the battery: little charge remains.
- Green:
 - For elements other than the battery: the element is active and shows no errors.
 - For the battery: full charge.
- Yellow (only for the battery):
 - The battery is in discharge or the charge is less than 100%.
- Grey:
 - No current is flowing through that element or part of the circuit. It is therefore not active.
- White:
 - The corresponding element does not exist in the device.

Surrounding the diagram, a summary of the relevant measurements for the different parts of the device is shown in order to complete the basic information (block 2 in Fig. 32).

3.4.1.1. ADAPT-X & ADAPT2 series.

If you have modules connected to the device, you can access individual information for each of them by clicking on the corresponding bypass symbol:

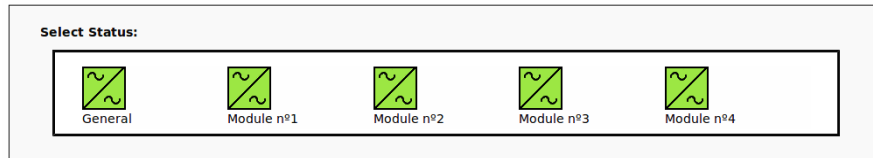
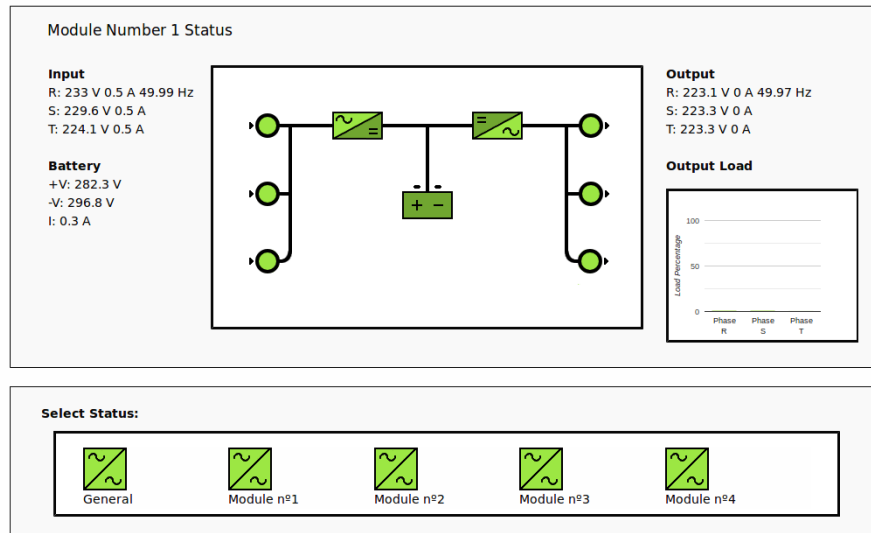


Fig. 33. Example of modules in the ADAPT2 and ADAPT-X series.

By clicking on any of them, an individualised monitor will appear showing its own diagram and measurements, as it can be seen in the following figure:

UPS Monitor Synoptic State adaptx



Alarms 1 - Module 1:

Rectifier Failure	✓
Inverter Failure	✓
High Rectifier Temperature	✓
Fan Failure	✓

Alarms 2 - Module 1:

Inverter Bridge Failure	✓
Outlet Temperature Error	✓
Input Current Unbalance	✓
High DC Bus Voltage	✓

Fig. 34. Diagram relating to a single module.

3.4.1.2. SLC CUBE4 7.5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2 and SLC TWIN RT2 series.

In these series, a button called "UPS status" is added to display both the system status and the alarms.

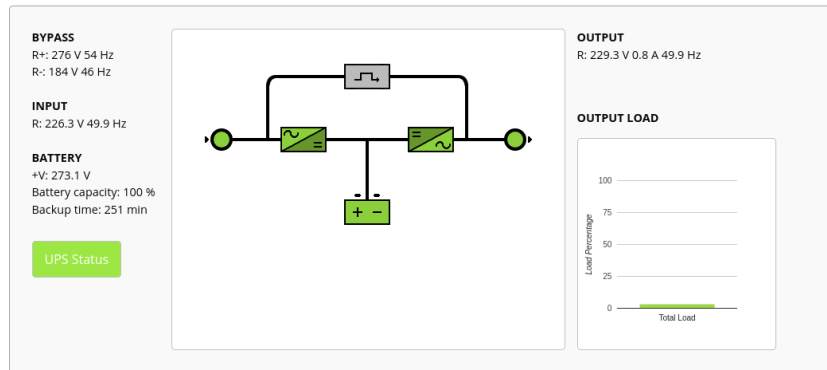


Fig. 35. Synoptic system status and alarms.

This button has 3 possible colours depending on the system status:

- Red: there is an urgent alarm on the device.
- Yellow: there is a non-urgent alarm or warning or the device status does not indicate optimal system operation (bypass or battery discharge).
- Green: there are no active alarms or warnings. Also, the device is operating perfectly.

To interact with it, click on the button. A pop-up window will open, informing you of the current status of the device.

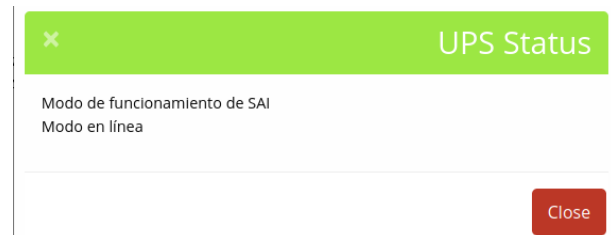


Fig. 36. Details of the "UPS status" button.

3.4.2. Alarms.

At the bottom of the screen, the different blocks of alarms that the device has and its current status are shown (**block 3**).

Non-active alarms are shown in green and active in red. An acknowledged alarm on the device (**ACK**) will also be shown in red.

System Alarms 1		System Alarms 2	
Battery Disconnected	3	Maintain Cb Open	✓
EPO	✓	Input Fail	✓
Bypass Sequence Fail	✓	Bypass Voltage Fail	✓
Bypass Fail	✓	Bypass Overload	✓
Bypass Overload Timeout	✓	Bypass Untrack	✓
Tx Time Limit	✓	Output Shorted	✓
Battery EOD	✓	Maintain Fail	✓
On UPS Inhibit Inverter On Disable	✓	Battery Volt Low	✓
Battery Reverse	✓	Input Neutral Lost	✓
Bypass Fan Fail	✓	Lost N+X Redundant	✓
EOD System Inhibited	✓	General Alarm	✓
		General Fault	✓

Fig. 37. Part of the display where the different alarms are shown.

3.5. DEVICE.

Click on 'Device' to display/hide the options described in this section.

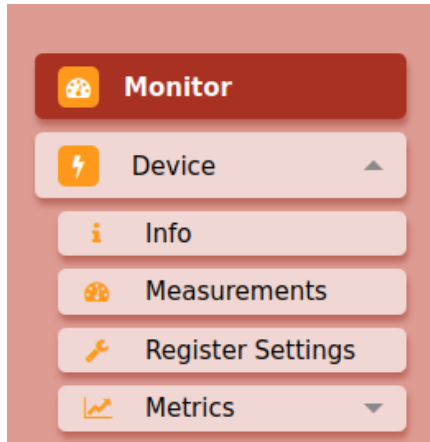


Fig. 38. Device menu

3.5.1. Info (only for Engineer user).

Page of **read-only**. This shows a summary of the technical parameters of the device and the version installed in the NIMBUS card.

3.5.2. Register Settings (only for Engineer user).

Page of **read-write**. This allows the parameters of the device to be modified.

i Only available for some specific series. Check the attached table for compatibility of the different ranges.

Series	OPTION TO CHANGE THE PARAMETERS
UPS 3x400/230 V	
SLC CUBE3/3+	X
SLC X-PERT	-
SLC X-TRA	-
SLC ADAPT-X	X
SLC ADAPT2	X
SLC CUBE4 30-80kVA	X
SLC CUBE4 7.5-20kVA	-
SLC TWIN RT2	-
SLC TWIN PRO2	-
SLC TWIN/3 PRO2	-
DC Systems	
DC POWER-S	X
DC POWER-L	X
Voltage stabiliser	
EMi3	X

Tab. 6. Parameter change option.

! **Important:** For some devices, it is not possible to modify certain parameters if the required circumstances are not met. Refer to section 3.5.3.x for more information.

i When several parameters are modified at the same time, it is probable that the device will not be able to modify all of them. It is recommended to modify a **maximum of 4 parameters** each time.

3.5.3. Measurements.

This shows in more detail the measurements of the device that had been previously displayed on the UPS monitor screen.

The measurements are classified according to the block to which they belong.

3.5.3.1. ADAPT-X Series.

Only with this series is it possible to obtain other measurements in addition to the device's general ones, and to have control of the modules. To switch between general and module measurements, use the selector located at the top of the screen:

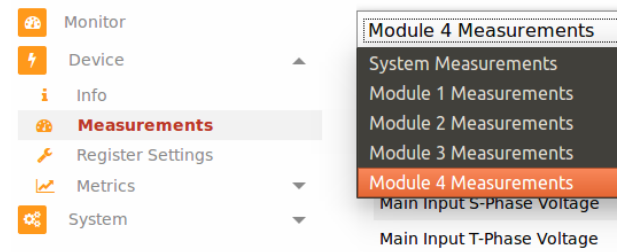


Fig. 39. Module 'Selector' screen.

3.5.4. Register Settings (only for Administrator and Engineer users).

Page of **read-write**. This allows the parameters of the device to be modified.

The Administrator user has access to all modifiable parameters, while the Engineer user has access to modify only the non-critical parameters of the device.

! **Important:** For some devices, it is not possible to modify certain parameters if the required circumstances are not met. Refer to section 3.5.3.x for more information.

i When several parameters are modified at the same time, it is probable that the device will not be able to modify all of them. We recommend that you only modify a **maximum of four parameters** at a time (see Fig. 40).

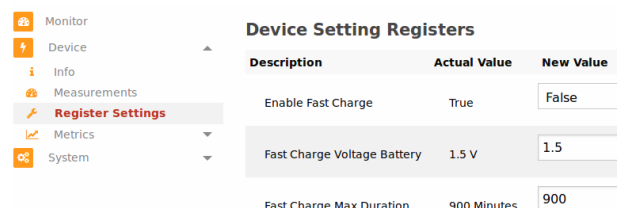


Fig. 40. Modification of parameters in Register Settings.

3.5.4.1. ADAPT-X Series.

The 'Charger Module Charging Current Limit Value' parameter can only be modified if a charger module is connected to the UPS.

3.5.4.2. CUBE3 / CUBE3+ Series.

To modify all of the parameters beforehand, it is necessary to transfer all of the load to Bypass. This can be done from the panel by changing the 'Start/Stop Inverter' parameter to Stop (see Fig. 41).

Device Setting Registers

Description	Actual Value	New Value
Start/Stop Inverter	Start	<div style="border: 1px solid black; padding: 2px;"> Start Stop Start </div>
Battery Test	Not Available	Not Available

Fig. 41. 'Start/Stop' parameter.

After you have finished modifying all of the parameters, return the UPS to its normal state.

3.5.4.3. X-PERT Series.

At the moment, it is not possible to modify any device parameter remotely.

3.5.4.4. DC-S Series.

It is not possible to modify the 'Battery Management' parameters if the corresponding functionality has not been enabled beforehand (see Fig. 42).

Battery Management: Enable Fast Charge (Y/N)	YES
Battery Management: Enable Periodic Charge (Y/N)	YES
Battery Management: Enable Exceptional Charge (Y/N)	YES

Fig. 42. 'Battery Management' parameters.

3.5.5. Metrics.

Click on 'Metrics' to display/hide the groups of graphs showing the device measurements.

Each group of graphs has one or more graphs showing the evolution over the **last three hours** of the measurement selected, see accompanying image.

If the device is connected but there is a problem with the NIMBUS card, the data sent for the most recent two-hour interval will be displayed (see Fig. 43), provided the device has been connected for at least two hours. If it has not been connected for that long, the measurements for the time it has been connected will be displayed, always up to a maximum of three hours.



Fig. 43. Evolution of the data sent every three hours.

3.5.6. Manage alarms (DC-S series only).

Remote acknowledgement of alarms is only possible for the DC-S series. When an alarm is active and can be viewed on the panel diagram, it will appear in this section as suitable for acknowledgement. To do so, click on the 'Validate' button next to the alarm you wish to acknowledge.



Fig. 44. Manage alarms.

After the alarm has been acknowledged, it will remain active and will still be shown in red on the panel. Once an alarm has been acknowledged via this page, it cannot be acknowledged again.

3.5.7. Actions (DC-S series only).

In this section it is possible to force actions on the device, although at present only the battery test is available. When it is possible to launch an action on the device internally, the corresponding button will be shown next to the action in question. Otherwise, if the action is not available (as shown in Fig. 45), a locked button will be shown and the action cannot be launched.

Device Actions

Start battery test

Back



Fig. 45. Forcing actions.

3.5.8. Logs (DC-S series only).

You can use this page to download the device's internal logs. This process requires two actions. First, generate the log by clicking on the 'Start' button. This will retrieve the device's log and display it on the screen. This may take a few minutes.



Fig. 46. Generating logs.

Once the log has been generated, it will be displayed on the screen, along with an option for downloading it in .csv format.

3.5.9. Backup (DC-S series only).

In the event of a device malfunction, you can use this page to restore the device's factory settings. First, click on the 'Start' button next to the 'Backup Device' option in order to restore the factory settings. When these settings are available, the button next to the 'Restore and Apply Backup' option will be activated and you can proceed with the operation. If you wish to restore the factory settings, click on the 'Start' button.

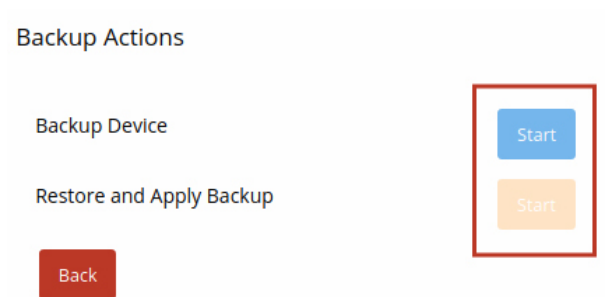


Fig. 47. Restoring factory settings.

3.6. SYSTEM (ONLY FOR THE ENGINEER USER).

Click on 'System' to display/hide the options described in this section.

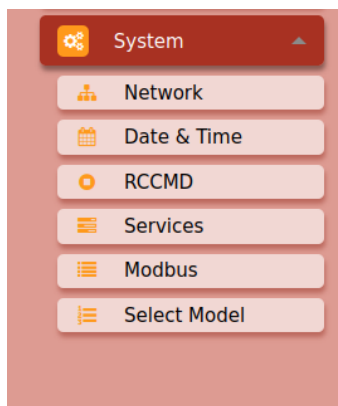


Fig. 48. System screen.

3.6.1. Network.

The NIMBUS card has two possible modes of remote connection through IP address.

3.6.1.1. Through DHCP.

In DHCP mode, the IP and other network parameters are assigned by your network's DHCP server, so no manual configuration is required for these fields.

To access the NIMBUS card you must know the IP assigned by DHCP.

3.6.1.2. Through static IP.

The IP address needs to be set manually and will remain the same until it is modified.

To modify it, you need to change the details in the IP field. The other data must be modified in accordance with the parameters of the local network where the card is being used.

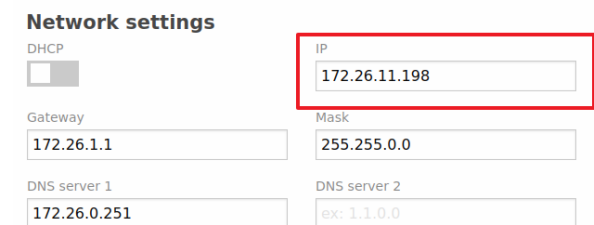


Fig. 49. Network settings.

i Do not modify the card's IP address if it is connected to the panel via that address, as the connection will automatically be lost.

You can also change or add the DNS server address. You can have up to two DNS servers.

i If DHCP configuration is enabled, these fields will be filled in automatically, but can be changed manually if necessary.

3.6.2. Date and time.

If you wish to modify the card's NTP server, you can do so in this section.

By default, it is configured with the servers of pool.ntp.org.

3.6.3. RCCMD (Optional service).

To activate this screen, first refer to section 5. Installing the RCCMD software.4. Instalación del software de RCCMD.

Specify the IP address of the destination server here. If you wish to broadcast, enter the broadcast IP. You must also add the port of the RCCMD client, in accordance with the procedure explained in section '4.2.2. Puerto del emisor.'

Set the wait time for each type of alarm before activating the server shutdown event. If the timer cannot be adjusted, the activation condition for remote server shutdown will be executed immediately.

RCCMD Settings

Receiver IP: 172.26.88.88 Port: (6003 by default) 6003

Register	Operation	Value	Timer
battery_low_level	==	1	Not Editable
inputVoltageWrong	>=	1	120000

Fig. 50. RCCMD settings.

i The value entered into the 'Timer' field must be expressed in milliseconds.

3.6.4. Services.

! This page may take longer to load than the others, so please be patient.

This section and Tab. 7 show all of the internal services of the NIMBUS card that can be modified. If you have not acquired the optional systems, the MQTT service will not appear on the list.

Service	Description
Modbus TCP	Secondary communication protocol derived from MODBUS (main communication protocol).
RCCMD	This service enables you to perform a controlled shutdown of the servers, in the event that certain conditions are detected by the device.
SNMP	Secondary communication protocol. This enables notifications to be sent to the user's IP when an alarm is activated.
MQTT	Protocol used to send data to the cloud. (Optional system)
External connection	By enabling the external connection of the card, it is possible to make calls to the communication services without having to access the inside of the card.

Tab. 7. NIMBUS card internal services

You can activate and deactivate them according to your needs. By default, all services are active except for the external connection, as shown in Fig. 51.

Services

- Modbus TCP
- RCCMD
- MQTT data
- SNMP
- External Connectivity

Fig. 51. Active services screen.

i After you enable the external connection, you will need to wait a few minutes until all of the services have started correctly. Bear in mind that the Modbus TCP service is slower to start than the others and will therefore be shown as inactive during the first minute.

! Disconnecting services means that some functionalities of the NIMBUS card will stop working. Do not modify a service if you do not know what it is used for.

3.6.5. SNMP (Optional service).

You will only be able to view this page if you have purchased the optional SNMP service.

Enter the IP address of your computer to receive alarm notifications through SNMP. To find the IP address of your computer, open the system search function, type 'cmd', then run the program. Type 'ipconfig' into the terminal and look for the address 'inet'.

The default community will always be 'salicru'. If you wish to modify this setting, use the 'SNMP Community' field to change the name of the community that is assigned by default.

SNMP Settings

Trap Server: 127.0.0.1 SNMP Community: salicru

Fig. 52. SNMP settings.

i It will be necessary to have a program installed that allows you to receive and manage the traps generated by the device.

3.6.6. MODBUS.

i In the SLC CUBE4 7,5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2 and SLC TWIN RT2 series, the communication configuration parameters cannot be changed.

You can modify the Modbus address of the slave to which the NIMBUS is connected in order to read information, as well as the parameters of the protocol for establishing a connection to the device. By default, these values already enable correct communication with the device.

If you wish to make any modifications, consult the settings of the device in order to ascertain the addresses and configuration parameters for which information is available.

Modbus Settings

Modbus Slave: 1 Transmission rate: 19200 baud

Read time: 8 Stop time: 1

Write: None Timeout: 0.2

Fig. 53. Modbus settings.


i After changing the address, we recommend restarting the panel and waiting a few minutes. Do not restart the NIMBUS card, otherwise you will lose the new values that have been entered.


! Important: Using non-valid values will result in loss of communication with the device. Before modifying them, make sure the panel is not in the process of receiving data and that the correct values as established by the device are known. Do not modify these values if the panel is in the process of receiving data.

3.6.7. Select model.

When it is inserted for the first time, the NIMBUS card will automatically detect the device type.

However, you can change the model if you wish to connect the NIMBUS card to another device.

 Do not change the model if the NIMBUS card has not been previously inserted into a different device.

 After changing the model, we recommend exiting and re-entering the panel in order to be able to view the data correctly.

3.7. LOGOUT.



Fig. 54. Logout.

Click this button on the right of the bar when you wish to stop consulting the device panel or you wish to access it using a different password.

4. INSTALLING THE RCCMD SOFTWARE.

Remote Control Command (**RCCMD**) is an application that enables the simultaneous and secure remote shutdown of different servers, in accordance with certain conditions specified by the user. To configure these conditions, see section '3.6.4 RCCMD'.

In order for this function to work, two elements are required: a receiver and a sender. The NIMBUS card will always work as a sender, as it will have the capacity to detect the specified shutdown conditions. The receiver can be one or various servers, depending on whether you have set a single IP indicating a single server, or a broadcast IP.

The sender is configured at the factory, so you will not need to install any new software in order to use it correctly. However, for each receiver that you wish to connect to this application, you will need to install specific software, as follows.

4.1. INSTALLING THE SOFTWARE.

Open a browser window and go to <https://www.generex.de/>. From there, click on the 'Download' tab and make sure that below the 'Software' section there is a section titled 'RCCMD'. Now click on the button 'Software'.



Fig. 55. Generex main screen.

A new page will appear as shown below displaying all of the downloads that are available. Select the 'RCCMD' option.

Software

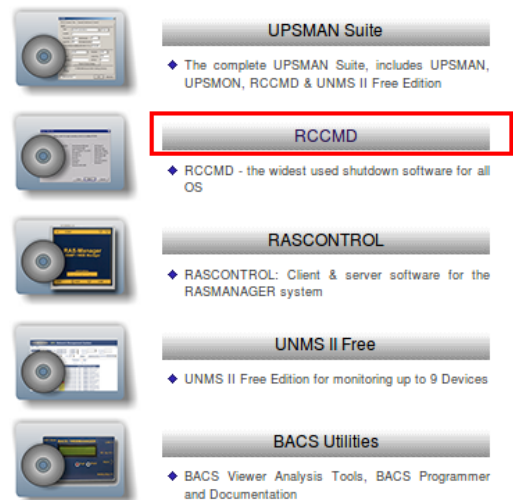


Fig. 56. Downloading the RCCMD software (detail).

In the 'RCCMD' section you will be shown a list of all of the compatible platforms. Choose the platform you require and once again select the download option by clicking on the button for the platform in question.

4.1.1. Windows.

If you have selected this operating system, you will be shown a full list of companies and their specific proprietary software. Search for the 'SALICRU' option, as shown in the image:



Fig. 57. SALICRU download option.

Click on the button shown in the image in order to begin the download.

Decompress the downloaded file, extract it to the desired location, and run the file 'installRCCMD.exe'.

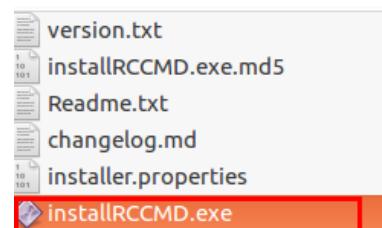


Fig. 58. Binary of execution of RCCMD

Two files will be shown, open the one named 'Windows'.

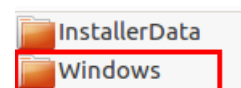


Fig. 59. Windows folder inside the unzipped folder.

Finally, run again the file 'installRCCMD.exe'.

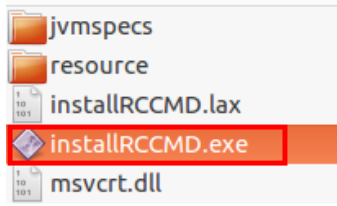


Fig. 60. Binary of execution of RCCMD in the windows folder.

Follow the steps indicated by the installer and do not modify the basic parameters that have been defined. At some stage during the installation you will be asked to enter a licence code, which will be provided by SALICRU.

4.1.2. Unix and Linux.

If you have selected either of these two operating systems, you will need a licence code, which will be provided by SALICRU.

Once you have the code and have selected the desired operating system, click on the 'Create package...' button to create the package and begin the download.

RCCMD for Linux

Version: 4.22.12 190815

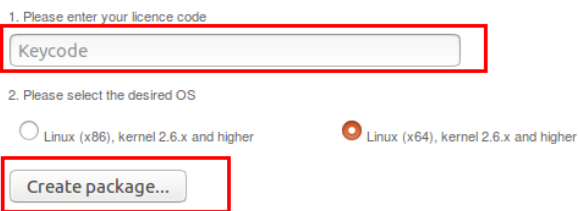


Fig. 61. RCCMD screen for Linux.

Decompress the downloaded file, extract it to the desired location, and run the file 'installRCCMD.bin'.

Follow the steps indicated by the installer and do not modify the basic parameters that have been defined. At some stage during the installation you will need to enter the same licence code you used earlier to create the package you downloaded. The licence code will be provided by SALICRU.

4.1.3. MacOS.

If you have selected this operating system, you will need a licence code, which will be provided by SALICRU.

Once you have the code and have selected the desired operating system, click on the 'Create package...' button to create the package and begin the download.

RCCMD for MacOSX

Version: 4.22.12 190815

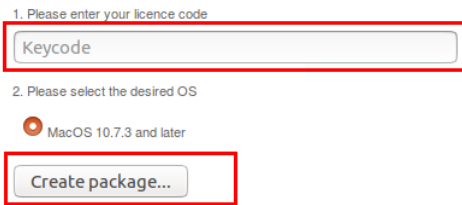


Fig. 62. RCCMD screen for MacOSX.

4.2. SOFTWARE CONFIGURATION.

After you have followed the above steps to download and install the RCCMD software, you will then be able to configure it. To do so, open any browser and enter the following address:

<https://localhost:8443/>

You will be taken to a page similar to the one shown below:

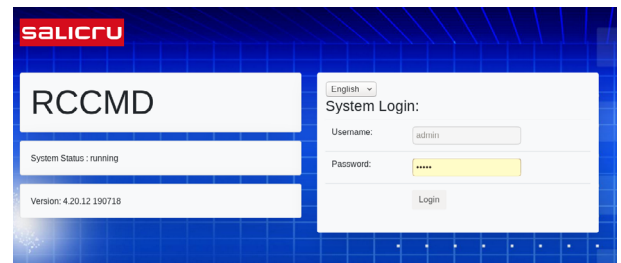


Fig. 63. RCCMD main screen.

In the section 'System Login', enter the credentials provided by SALICRU and click on the button 'Login' (Fig. 63).

By default, the page will display the status of the RCCMD ('running' or 'not running') and present you with the option to start, stop or restart, as shown in the following image Fig. 64.

i If you modify any of the parameters, we recommend selecting the 'Restart' option to make sure the modification is carried out correctly.

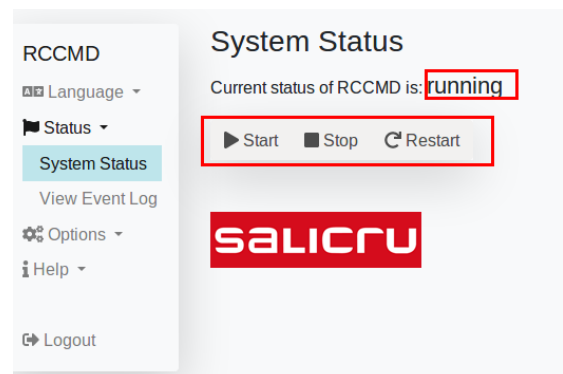


Fig. 64. RCCMD: System status.

i If the RCCMD is not running in the destination server, the NIMBUS card will not be able to send it the information it requires to function correctly.

4.2.1. Sender IP.

To pair a particular device with the NIMBUS card so that they can listen to one another, go to the 'Options' section and select the 'Connections' option in the side navigation bar on the left, as shown in Fig. 65.

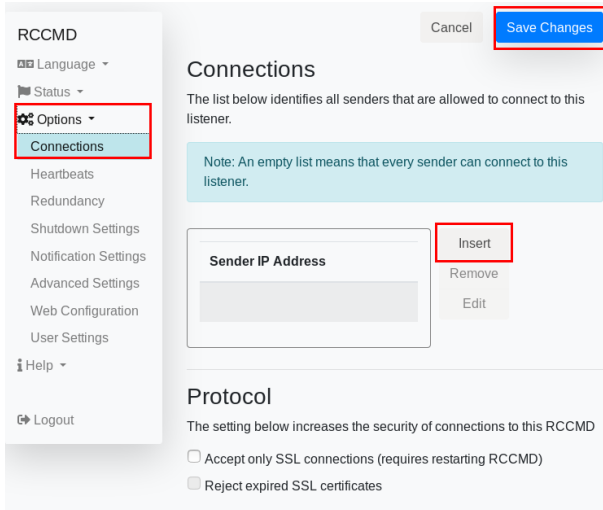


Fig. 65. Pairing screen for the NIMBUS card.

i If the 'Sender IP Address' field is left empty, the server will still be able to listen to and therefore execute any shutdown instructions it may receive from the different NIMBUS cards, if the destination IP has been correctly configured in these cards and corresponds to the server in question. In other words, even if the IP of the sender (i.e. the NIMBUS card) is not configured, the server can still receive instructions if the status of the RCCMD is 'running'. Nonetheless, for additional security we recommend pairing the device with the NIMBUS card.

To enter an IP, click on the 'Insert' button as shown in the image. A pop-up window will appear, as shown in Fig. 66.

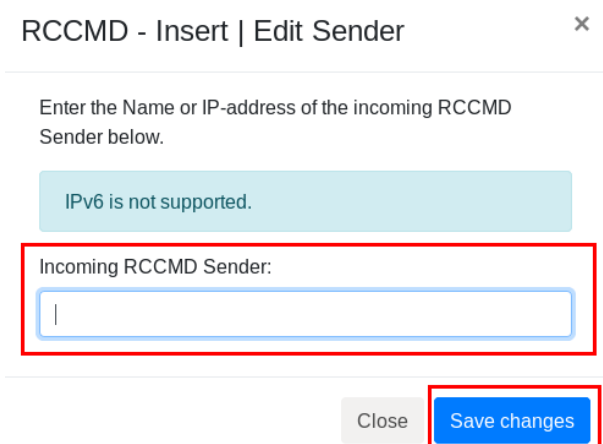


Fig. 66. Insert IP screen.

In the corresponding field, enter the IP of the NIMBUS card you wish to associate with the device. Then click on 'Save changes'.

On the main screen, save your changes again by clicking on the button 'Save changes'.

! Important: If you do not want the server to use the RCCMD service, you must deactivate it (making sure the system status is shown as 'not running'). Simply clearing the 'Sender IP Address' field is not enough, as the server may still occasionally receive an instruction.

4.2.2. Sender port.

This step is not necessary, as the RCCMD software is configured to port 6003 by default.

However, if you wish to change the port, go to 'Options' and select 'Advanced Settings' in the side navigation bar on the left, as shown in Fig. 67.

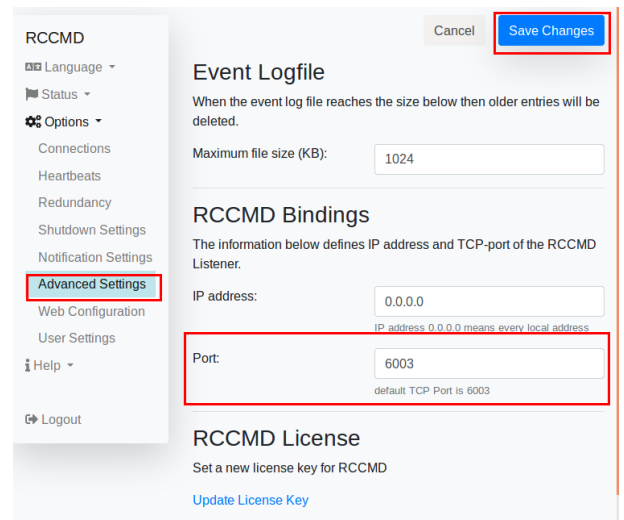


Fig. 67. Advanced Settings screen.

Choose which port you would like the RCCMD to listen to by modifying the field 'Port'. To complete the process, click on 'Save Changes'.

5. ACTIVATION OF CONTRACTED SERVICES.

If you have purchased an extra service with your NIMBUS communications card, you must activate it via the embedded web panel. To use this method, follow the steps below:

1. Connect to the web panel. Refer to section "3.1 Access to the panel" for more information.
2. Click on "Activate service", under the login button as shown in the figure below.

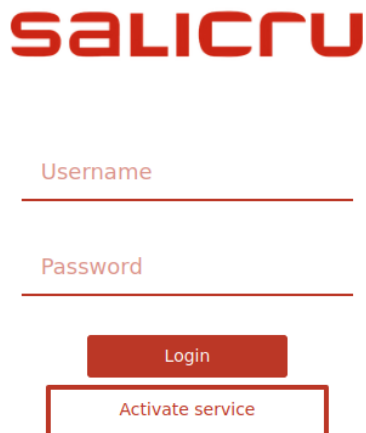


Fig. 68. Activate service.

3. Enter the activation code provided by SALICRU in the box marked "Code" and click on "Send".



Fig. 69. "Send" button.

4. If the code is correct and the service is not already installed, the following message will appear. Otherwise, installation will not occur. Contact technical support if necessary.



Fig. 70. Activation and error screens.

5. Once the service is activated, it will be installed and available on your card in about 5 minutes.

The optional packages that can be purchased on the NIMBUS communications card are listed below:

Service	Description
Modbus TCP	Secondary communication protocol derived from MODBUS (main communication protocol).
Modbus API-REST	By enabling the external connection of the card, it is possible to make calls to the communication services without having to access the inside of the card.
RCCMD (*)	This service enables you to perform a controlled shutdown of the servers, in the event that certain conditions are detected by the device.
SNMP	Secondary communication protocol. This enables notifications to be sent to the user's IP when an alarm is activated.

(*) The RCCMD service must not be activated by code on the NIMBUS communications card, but by downloading the RCCMD client. For more information, refer to section "4. Installing the RCCMD software".

Tab. 8. Optional packages.

6. APPENDIX I. CONNECTIVITY

For all SALICRU devices compatible with the NIMBUS card, the data displayed on the onboard panel can also be uploaded to SALICRU's online platform. This platform allows users to view the status of the device without needing to be on the same network. It also makes it possible to update the cards remotely, view the device's location and customise the SMS and email notifications that are received in the event of an alarm.

In the SLC ADAPT2 and SLC CUBE4 series, you can find out if the device is connected and sending data to the cloud through the following icon at the top right of the screen:



If the device is not connected, the following icon will appear:



The device may not be able to connect for the following reasons:

- The card is not correctly connected to the network.
- The card is connected to a network that does not provide access to the Internet.

6.1. NETWORK FIREWALL REQUIREMENTS.

6.1.1. Option 1 (recommended): full opening of ports 443 and 8883.

In order to successfully connect and send data towards the remote maintenance portal, the card must **have ports 443 (https) and 8883 (MQTT)** open to allow data output and connection to the server from any IP address. This will enable you to establish a correct and stable connection between your device and the portal.

6.1.2. Option 2 (not recommended): list of google hostnames and ports.

In cases where the first option is excessive, the connection can also be established by the more restrictive rules detailed below. It is important to set the hostname by FQDN rules and not by IPs, as the latter are variable.

It is important to note that with this method the connection is correct, but not stable. Connection failures may occur if the firewall does not figure out the set hostname correctly.

Hostname	Port
mqtt.googleapis.com	443 and 8883
accounts.google.com	443
oauth2.googleapis.com	443
cloudiot.googleapis.com	443
www.googleapis.com	443

Tab. 9. List of IPs / ports for correct connection to the remote maintenance panel.

6.2. USE OF AND ACCESS TO THE REMOTE MAINTENANCE PORTAL.

6.2.1. Creating an account.

In order to make use of this optional system, follow the steps below:

1. Go to <https://nimbus.salicru.com/>.
2. Create an account (if you do not already have one), using the "Create an account" link shown in the image.

Fig. 71. Main login screen on the remote maintenance panel.

3. Complete the form with the correct data. You must accept the "Terms and conditions".

Fig. 72. User registration screen.

The password must be at least 8 characters long and contain at least one lower-case letter, one upper-case letter, one number and one symbol e.g. #MiContraseñaParaNimbus2020

To continue, you must read and agree to the terms and conditions set out by clicking on the box.

4. Once you have created your account, go to the inbox of the email address you entered during registration. Within a few minutes you will receive an email confirming your account.



Remember that this message has an expiry date. To be used within 15 minutes of receipt.

5. Click on the link sent in the email for user activation and you will have access to the remote maintenance portal.

6.2.2. Registering the device in the cloud.

There are two ways of registering the device in the cloud:

- Directly from the remote maintenance portal (not recommended for users)
- Scanning the QR code located on the front of the device.

6.2.2.1. Manual registration through the remote maintenance portal.

1. Start the session on the portal with a previously validated account.
2. On the main screen of the "Devices" application, click on the "+ add new device" button in the top right corner.
3. Complete the form to create the device with the relevant information.



Obligatory fields are marked with an asterisk (*).

The SERIAL NUMBER, UUID and MODEL fields contain basic data identifying the product. You can find this information on your device's identification label.

We recommend that you provide a clear and concise description to identify the product. That way, if you have registered other SALICRU devices, you can use this field to easily differentiate between them.

The device's location and the corresponding time zone are both obligatory fields. To add the device's location you can search for it using the option Search location, which will open an interactive map, or you can manually enter the address and coordinates.

4. Click on **SAVE** to complete the process.
If there is an error in the creation of the device, you will be notified on screen. Contact technical support if necessary.
5. Once the device has been successfully created, it will be displayed in the list of devices on the "Devices" page.

6.2.2.2. Automatic registration with QR Code.

1. Scan the QR code located on the front of the device. Most mobile phones and tablets have tools for scanning QR codes, but if yours does not, you must install one from the app store.

After scanning the code, a registration page will open in the browser of your phone or tablet.

You must log in to register the device. If you do not yet have a SALICRU account, you can create one by clicking on the 'Create account' link.

2. Fill in the blank spaces on the form. The basic data of the device will already be preset and cannot be changed.

We recommend that you provide a clear and concise description to identify the product. That way, if you have registered other SALICRU devices, you can use this field to easily differentiate between them.

The device's location and the corresponding time zone are both obligatory fields. To add the device's location you can search for it using the option Search location, which will open an interactive map, or you can manually enter the address and coordinates.

3. Click on SAVE to complete the process.

If there is an error in the creation of the device, you will be notified on screen. Contact technical support if necessary.

4. Once the device has been successfully created, it will be displayed in the list of devices on the "Devices" page.

6.2.3. Creating notifications associated with a device.

After you have successfully registered a device, you can configure its alarm notifications. To do this, go to the "Notifications" section in the vertical navigation bar.



Make sure you have registered a device first, otherwise you will not be able to associate any notifications with your user.

To create a new notification, press the "+ add new notification" button. This will open a form for the creation of the new notification.

Important: Each user can only set up one notification for each device. However, email accounts and phones can be associated so that more than one person can receive the same notification.

Within the creation form, select the device for which you wish to create a notification using the "Device" drop-down menu. Once selected, the possible alarm groups available will be displayed. Select one or more of them according to your needs.

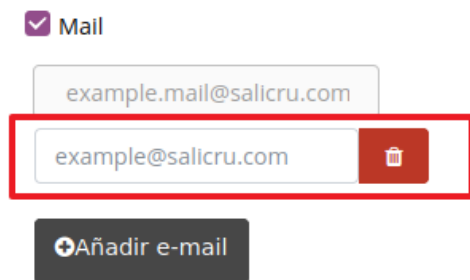
Finally, select the desired type of notification in the "Enabled notifications" section. There are three types: web page, email and SMS. If none is selected, no alarm notifications of any kind will be displayed and you must go directly to the device details to check its status.

6.2.3.1. Web notifications.

With these notifications enabled, a pop-up message will be displayed on the website itself when an alarm occurs. Note that these notifications will only be displayed if the user is logged in and browsing the remote maintenance website.

6.2.3.2. Email notifications.

This type of notification will allow you to receive an email each time an alarm is enabled. The default notification email will be directly associated with the user who created it and can be viewed on the same page (non-editable field). To change the default email address, access the user profile. Extra email addresses can be added in the same notification. Press "Add email" and enter an additional address.



Mail

example@mail@salicru.com

example@salicru.com

Añadir e-mail

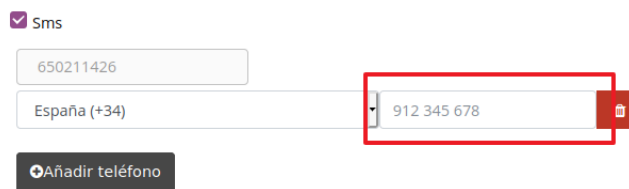
Fig. 73. Add an extra email address.

Please note that the notification will now be sent to the default email address and all others associated.

6.2.3.3. SMS notifications.

With this notification you will receive an SMS message on your mobile phone every time an alarm is triggered. As with emails, the default phone number will be associated directly with the user who created it as a non-editable field. To change the phone number, access the user profile.

You can also add more phone numbers. Press "Add phone number" and enter the number. Please note that the notification will now be sent to the default phone number and all others associated.



Sms

650211426

España (+34) 912 345 678

Añadir teléfono

Fig. 74. Add another phone number.

6.2.4. Password recovery.

If you cannot remember your password, you can reset it by clicking on the 'Reset password' option on the Login screen.

You will be asked to enter the email address that is linked to your account. Click on 'Send' to continue the process.



SALICRU

Email

user@example.com

Atrás Enviar

Fig. 75. Lost password recovery page.

You will receive an email allowing you to reset your password. Remember to check the Spam folder if you cannot find the email in your inbox.

After you click on the link contained in the email you will be able to create a new password. Click on 'Save' to set the new password.

7. APPENDIX II. GENERAL TECHNICAL SPECIFICATIONS.

In the *Tab. 10* below lists the technical specifications of the NIMBUS card:

	Specifications
Processor	Sitara AM3358BZCZ100 1GHz, 2000 MIPS
Graphics card	SGX530 3D, 20M Polygons/S
SDRAM memory	512MB DDR3L 800 MHz
Flash memory	4GB, 8bit MMC integrated
PMIC	TPS65217C PMIC regulator and an additional LDO.
Debug support	Optional Onboard 20-pin CTI JTAG
SD/MMC connector	MicroSD, 3.3V
Audio	HDMI interface, stereo

Tab. 10. Technical specifications of the NIMBUS card.

SALICRU

Avda. de la Serra 100

08460 Palautordera

BARCELONA

Tel. +34 93 848 24 00

sst@salicru.com

SALICRU.COM



Information about our technical service and support network (T.S.S.), sales network and warranty is available on our website:

www.salicru.com

Product Range

Uninterruptible Power Supplies (UPS)

Stabilisers - Step-Down Light Dimmers

Power Supplies

Static Inverters

Photovoltaic Inverters

Voltage Stabilisers



@salicru_SA



www.linkedin.com/company/salicru

