

MANUAL DE USUARIO



MANUAL DE CONECTIVIDAD NIMBUS CLOUD



NIMBUS

salicru

ES

EN

Contents

1. INTRODUCCIÓN.

- 1.1. EQUIPOS COMPATIBLES CON CONECTIVIDAD.

2. INSTALACIÓN.

- 2.1. CON TARJETA NIMBUS.
- 2.2. SIN TARJETA NIMBUS.
 - 2.2.1. Conectividad integrada mediante Ethernet.
 - 2.2.2. Conectividad integrada mediante dispositivo WiFi.

3. PUESTA EN MARCHA.

- 3.1. REQUERIMIENTOS PREVIOS.
 - 3.1.1. Configuración del servidor NTP con tarjeta NIMBUS.
 - 3.1.2. Configuración del servidor NTP sin tarjeta NIMBUS.
 - 3.1.3. Configuración de la IP.
- 3.2. REQUERIMIENTOS DE FIREWALL.
 - 3.2.1. Requerimientos de firewall para conectividad con tarjeta NIMBUS.
 - 3.2.1.1. Opción 1 (recomendada): apertura completa de puertos 443 y 8883.
 - 3.2.1.2. Opción 2 (no recomendada): relación hostnames y puertos de google.
 - 3.2.2. Requerimientos de firewall para conectividad sin tarjeta NIMBUS.
 - 3.2.2.1. Relación hostnames y puertos de google.

4. REGISTRAR UN EQUIPO EN LA NUBE.

- 4.1. MEDIANTE LA APLICACIÓN NIMBUS CLOUD (SOLO UPS/SAI).
- 4.2. MEDIANTE PORTAL WEB (SOLO ESTABILIZADORES DE TENSIÓN Y SISTEMAS DC).

1. INTRODUCCIÓN.

Para algunas series de SAI, sistemas DC y estabilizadores de la marca SALICRU es posible monitorizar los equipos en tiempo real, de forma totalmente remota y sin necesidad de estar en la misma red donde se encuentra instalado el equipo.

Para ello, está disponible una plataforma y una aplicación móvil donde el usuario tiene la posibilidad de visualizar el estado del equipo, controlar la tarjeta de comunicaciones, visualizar la localización del equipo y personalizar notificaciones en caso de alarma.

En las series **SLC ADAPT2**, **SLC CUBE4**, **SLC TWIN PRO3**, y **SLC TWIN RT3** podrá saber si el equipo está conectado y enviando datos a la nube buscando el siguiente icono:



En caso contrario, se mostrará el siguiente icono:



Los motivos que pueden hacer que un equipo no esté conectado son:

- La tarjeta no está conectada correctamente a la red.
- La red en la que está conectada la tarjeta no tiene acceso a internet.

1.1. EQUIPOS COMPATIBLES CON CONECTIVIDAD.

Serie SAI/UPS	Nimbus - MAXI	Nimbus - MINI	IoT integrado
SLC CUBE3/3+	✓	✗	✗
SLC X-PERT	✓	✗	✗
SLC X-TRA	✓	✗	✗
SLC ADAPTX	✗	✓	✗
SLC ADAPT2	✗	✓	✗
SLC CUBE4	✗	✓	✗
SLC TWIN RT2	✗	✓	✗
SLC TWIN PRO2	✗	✓	✗
SLC TWIN/3 PRO2	✗	✓	✗
SLC TWIN PRO3	✗	✓	✓
SLC TWIN RT3	✗	✓	✓
Sistemas DC (*)			
DC POWER-S	✓	✗	✗
DC POWER-L	✓	✗	✗
Estabilizador de Tensión (*)			
EMI3	✓	✗	✗

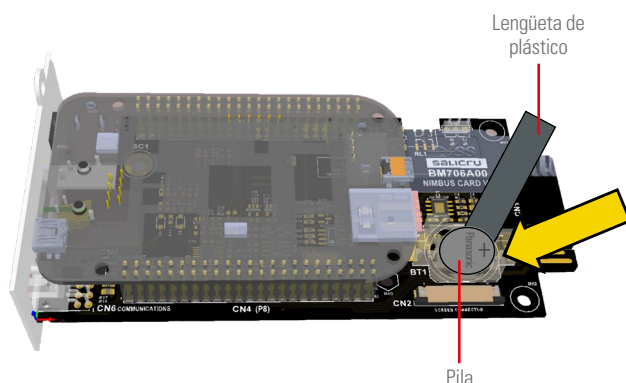
(*) La conectividad para estas series solo se ofrece mediante el panel de telemantenimiento. No están disponibles en la aplicación móvil.

2. INSTALACIÓN.

2.1. CON TARJETA NIMBUS.

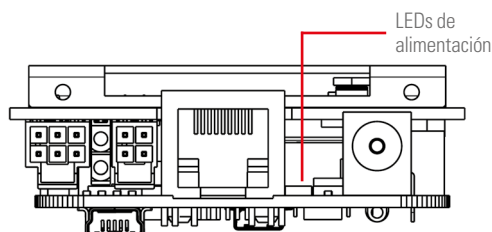
Si se dispone de una tarjeta NIMBUS proceder de la siguiente manera.

1. Retirar el plástico protector de la pila de la tarjeta NIMBUS.

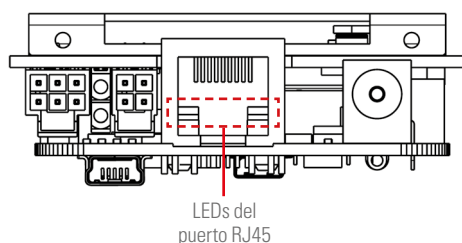


2. Conectar la tarjeta NIMBUS en la ranura correspondiente de un equipo previamente conectado. Debe quedar encajada.

La tarjeta se alimentará directamente del equipo y por lo tanto no es necesaria alimentación externa. Si se ha introducido correctamente la tarjeta, los LEDs de alimentación se encenderán en azul.

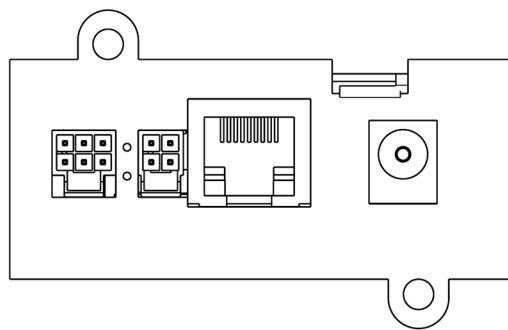


3. Conectar un cable RJ45 con un extremo en la tarjeta y el otro a la toma de ethernet. Las luces del puerto RJ45 de la tarjeta deberán encenderse.



4. Una vez alimentada correctamente la tarjeta NIMBUS en el equipo, ya estará lista para su uso. La última versión disponible para la tarjeta NIMBUS ya vendrá instalada por defecto.

Colocando la tapa de protección de la tarjeta NIMBUS, finalmente debería verse como en la imagen siguiente.



2.2. SIN TARJETA NIMBUS.

Para las series SLCTWIN PRO3/RT3, además de permitir su conectividad con una tarjeta NIMBUS, también es posible conectarse sin ella. Dispone para ello, de dos formas.

2.2.1. Conectividad integrada mediante Ethernet.

Simplemente conectar un extremo de un cable RJ45 a la entrada Ethernet del SAI y otro a la red.

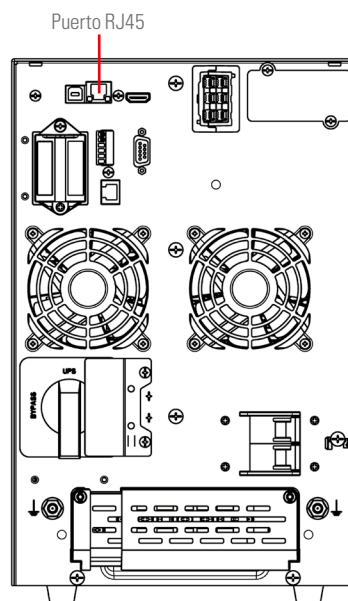


Fig. 1. Conexión Ethernet en los SAIs de la serie SLCTWIN PRO3.

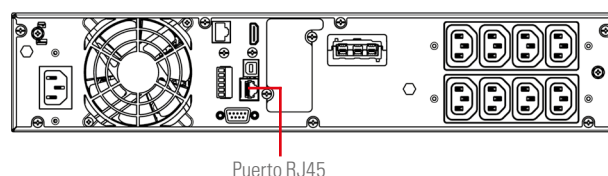


Fig. 2. Conexión Ethernet en los SAIs de la serie SLCTWIN RT3.

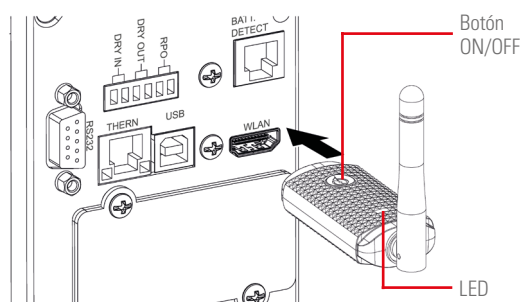


Nota: Revisar los requisitos del firewall para usar la actualización de firmware OTA. Debe habilitar el acceso en <http://firmware.salicru.com> y tomqtt.2030.ltsapis.google.

⚠ Importante: Se requiere la sincronización del servidor NTP para garantizar la correcta conexión a la nube y la transferencia de datos. Debe tener acceso a <http://pool.ntp.org>; de lo contrario, modificar su servidor NTP para que IoT obtenga la marca de tiempo correcta.

2.2.2. Conectividad integrada mediante dispositivo WiFi.

1. Conectar el dispositivo WiFi en el puerto HDMI indicado para la conexión WLAN. Esperar que el LED empiece a parpadear indicando una buena conexión.
2. Mantener pulsado el botón ON/OFF del dispositivo durante 4-5 segundos. El LED empezará a parpadear a una frecuencia más elevada, indicativo de que ha cambiado de estado a modo "Access point (AP)".



3. Utilizar un ordenador o teléfono móvil para conectarse a la red WiFi "WLANDongle" (contraseña: welcome12) proporcionada por el dispositivo WiFi.



4. Conectarse a la siguiente url <http://192.168.1.1>. Aparecerá un portal de configuración WiFi donde deberá introducir las credenciales de su red WiFi.

Wireless Setting Portal

This product supports **2.4G Wireless** only

Last status : No AP found

SSID*:

SALICRU

Password:

Obtain an IP address automatically:

Enable

Save

i Nota: Puede que tenga que hacer clic en la opción "Avanzado > Continuar en sitio no seguro" la primera vez que entra en la página web.

⚠ Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.1.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the web site, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the web site's administrator about the problem.

[Learn more...](#)

Go Back (Recommended)

Advanced...

Someone could be trying to impersonate the site and you should not continue.

Web sites prove their identity via certificates. Firefox does not trust 192.168.1.1 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

[View Certificate](#)

Go Back (Recommended)

Accept the Risk and Continue

5. Una vez haya introducido todos los datos relacionados con su red WiFi, hacer clic en "Save" y esperar unos segundos. El LED deberá cambiar de estado de parpadeo a fijo.

Wireless Setting Portal

This product supports **2.4G Wireless** only

Last status : No AP found

SSID*:

SALICRU

Password:

Obtain an IP address automatically:

Enable

Save

Please waiting...

⚠ Importante: Existen las siguientes limitaciones de red WiFi que deben considerarse para conseguir una conexión satisfactoria:

- ☐ El nombre del WiFi (SSID) debe contener exclusivamente números y letras.
- ☐ Los caracteres especiales no están soportados.
- ☐ Las redes WLAN públicas que requieren de una segunda autenticación no están soportadas.
- ☐ Los WiFi routers de 5GB no están soportados.
- ☐ Algunas redes WLAN que necesiten habilitar funciones especiales como "MAC whitelist" requerirán ese paso adicional.

6. Finalmente, asegurar habilitar el servicio IoT integrado del UPS a través de la pantalla para poder ver reflejado el cambio del icono de conectividad (nube) una vez el dispositivo quede registrado.



Importante: Si durante el proceso de conexión WiFi se produce un evento inesperado, revisar la siguiente tabla.

Estado del LED	Descripción	Acción
LED apagado	Conexión con el UPS no es buena.	Revisar la conexión entre el dispositivo y el UPS.
LED parpadea lentamente (1 flash/segundo)	El dispositivo no está conectado al router.	Revisar los requerimientos de la red WiFi. Revisar que las credenciales introducidas son correctas. Asegurar que la intensidad de la señal WiFi sea "fuerte" o al menos "media". Puede ser importante, ya que si la señal es "débil", la conexión será inestable.
LED parpadea rápidamente (4 flash/segundo)	El dispositivo está en modo Configuración.	Conectarse a http://192.168.1.1 para establecer la conexión con el router.
LED encendida	La conexión al router se ha realizado correctamente.	-

3. PUESTA EN MARCHA.

3.1. REQUERIMIENTOS PREVIOS.

Independientemente del método de conexión a la nube que se utilice (tarjeta NIMBUS / IoT integrado) se requiere la sincronización del servidor NTP para garantizar la correcta conexión a la nube y la transferencia de datos.

Debe tener acceso a <http://pool.ntp.org> ; de lo contrario, modificar su servidor NTP para que IoT obtenga la marca de tiempo correcta.

3.1.1. Configuración del servidor NTP con tarjeta NIMBUS.

Acceder al panel web de la tarjeta NIMBUS, conectándose punto a punto con un cable Ethernet. Para ello, seguir los siguientes pasos:

1. La tarjeta cuenta con una dirección IP fijada siempre en 100.0.0.1. Para conectarse a su subred, es preciso crear una nueva conexión de red con los siguientes parámetros:

- ☐ Address: 100.0.0.2
- ☐ Netmask: 255.255.255.0
- ☐ Gateway: 100.0.0.1

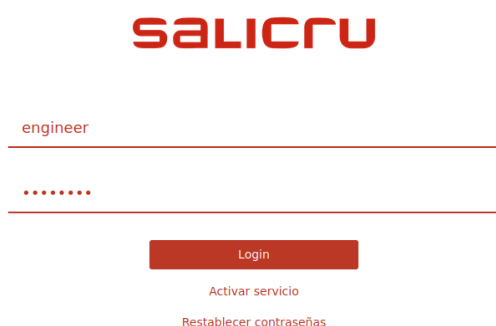
2. Conectar el cable Ethernet de la tarjeta de comunicaciones directamente al ordenador, o bien a un switch que le permita hacer de punto de acceso.

3. Configurada correctamente la red en su ordenador, y sin ninguna otra fuente de internet posible (desconectar el WiFi si fuera necesario), introducir la dirección <https://100.0.0.1/> en su navegador.

  <https://100.0.0.1/>

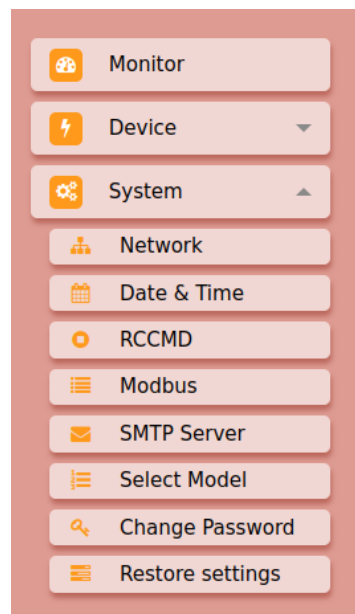
4. Conectarse al panel con las siguientes credenciales:

usuario: engineer
contraseña: SLC3ng1n

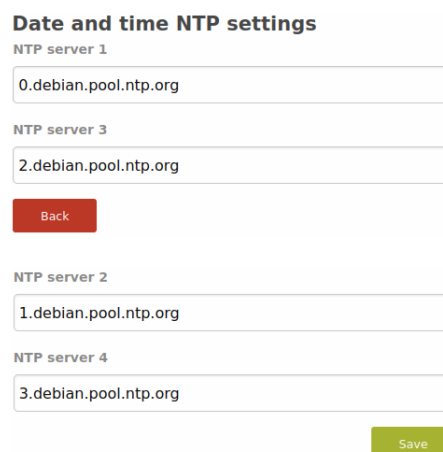


The login page features the Salicru logo at the top. Below it, there are two input fields: the first is pre-filled with 'engineer' and the second contains masked characters '.....'. A red 'Login' button is positioned below the password field. At the bottom, there are two links: 'Activar servicio' and 'Restablecer contraseñas'.

5. Ir a la sección "System > Date & Time".



6. Configurar correctamente los servidores NTP, en función de sus preferencias. Hacer clic en "Guardar".



The 'Date and time NTP settings' form contains four input fields for NTP servers. 'NTP server 1' is set to '0.debian.pool.ntp.org', 'NTP server 3' to '2.debian.pool.ntp.org', 'NTP server 2' to '1.debian.pool.ntp.org', and 'NTP server 4' to '3.debian.pool.ntp.org'. A red 'Back' button is located between the first and second server fields. A green 'Save' button is at the bottom right.

7. Ir a "System" > "Network" y hacer clic en la pestaña "Connectivity Test". Realizar el test pulsando el botón.

8. Comprobar que no hay ningún error con la conexión NTP.

3.1.2. Configuración del servidor NTP sin tarjeta NIMBUS.

Acceder al panel web y a la IP que se muestra en el display del equipo. Para ello, seguir los siguientes pasos:

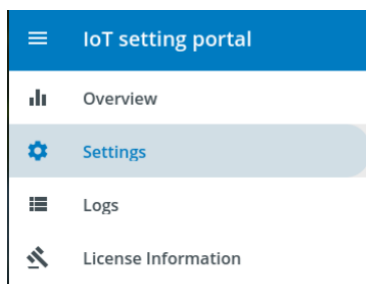
1. En el display del equipo, navegar hasta "Identification". Dentro de esta sección se encuentran las rutas "Embedded IoT IP" y "WLAN IP". En función del método utilizado para conectarse a la nube, escoger una IP u otra. La opción que no esté conectada aparecerá con "0.0.0.0".

2. Introducir en el navegador la dirección IP del display del equipo.

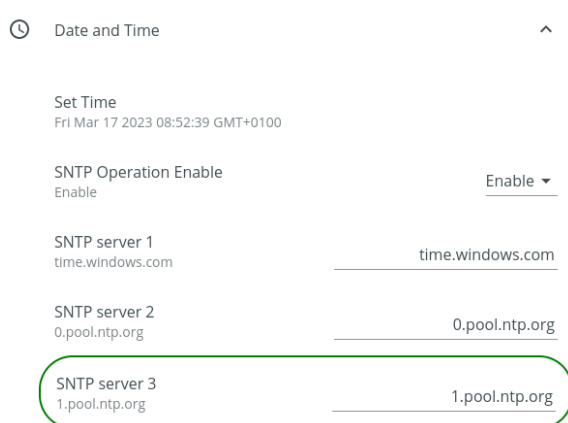
3. Conectarse al panel con las siguientes credenciales:

usuario: admin
contraseña: Admin*1

- Ir a la sección "Settings" > "Preference".



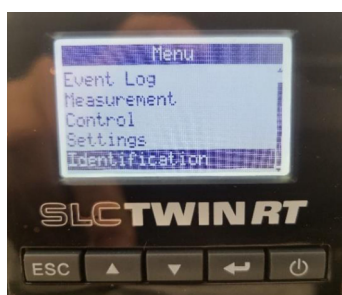
- Configurar correctamente los servidores NTP, en función de sus preferencias. Hacer clic en "Guardar".



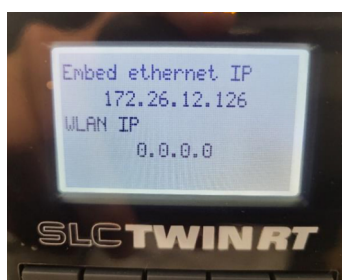
3.1.3. Configuración de la IP.

Para realizar la conexión a la interfaz del equipo es necesario conocer de antemano la IP asignada por DHCP. Para ello seguir los siguientes pasos:

- En el display del SAI, ir a la opción **Identificación** → **Embed ethernet IP**.



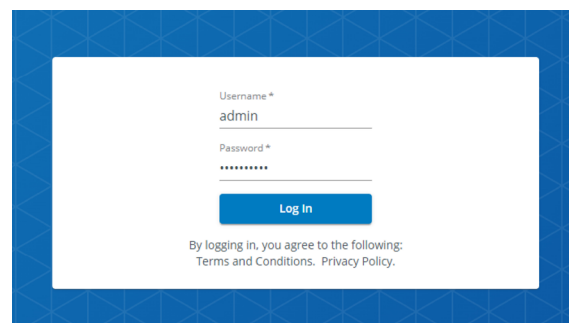
- Entrar en el navegador web con la IP proporcionada por el display.



Una vez establecida la conexión se cargará esta interfaz.

Credenciales de acceso:

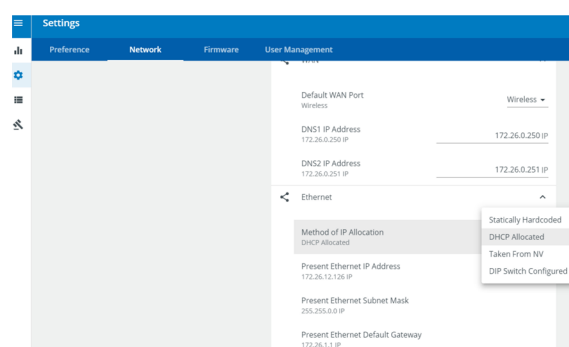
- Username: **admin**
- Password: **Admin*1**



- En el caso de no poder acceder con estas credenciales, proceder a restablecer las opciones del SAI.



- Una vez obtenido el acceso, se dispone de 4 opciones en el apartado **Settings** → **Network** para cambiar la manera en que el equipo obtiene la IP:
 - Statically Hardcoded:** se restablece la IP por defecto 192.168.1.254.
 - DHCP Allocated:** se obtiene la IP vía DHCP.
 - Taken from NV:** se establece una IP estática.



3.2. REQUERIMIENTOS DE FIREWALL.

3.2.1. Requerimientos de firewall para conectividad con tarjeta NIMBUS.

Tener siempre activado el acceso a <https://archive.salicru.com> con el puerto 443. Este web se utiliza para actualizar de forma remota la tarjeta de comunicaciones NIMBUS, con lo que si no se garantiza su acceso la tarjeta no podrá ser actualizada periódicamente.

Además, se requieren puertos adicionales abiertos, que se detallan a continuación.

3.2.1.1. Opción 1 (recomendada): apertura completa de puertos 443 y 8883.

Para que la conexión y el envío de datos se produzca de manera satisfactoria contra el portal de telemantenimiento, es necesario que la tarjeta **tenga abiertos los puertos 443 (https) y 8883 (MQTT)** de modo que permitan la salida de datos y la conexión con el servidor desde cualquier IP. Esto permitirá una conexión correcta y estable de su equipo en el portal.

3.2.1.2. Opción 2 (no recomendada): relación hostnames y puertos de google.

En los casos en los que la primera opción sea excesiva, la conexión puede establecerse también mediante unas normas más restrictivas que se detallan a continuación. Es importante fijar el hostname por reglas FQDN y no por IP, ya que estas últimas son variables.

Es importante destacar que con este método la conexión es correcta, pero no es estable. Pueden producirse cortes de conexión si el firewall no resuelve correctamente el hostname fijado.

Hostname	Puerto
mqtt.googleapis.com	443 y 8883
europe-west1-mqtt.clearblade.com	443 y 8883
www.googleapis.com	443
oauth2.googleapis.com	443
accounts.google.com	443

3.2.2. Requerimientos de firewall para conectividad sin tarjeta NIMBUS.

Tener siempre activado el acceso a <https://firmware.salicru.com> con el puerto 443. Este web se utiliza para actualizar de forma remota el dispositivo IoT integrado en el dispositivo, con lo que si no se garantiza su acceso, el dispositivo no podrá ser actualizada periódicamente.

Además, se requieren puertos adicionales abiertos, que se detallan a continuación.

3.2.2.1. Relación hostnames y puertos de google.

Hostname	Puerto
tomqtt.2030.ltsapis.google	443 y 8883

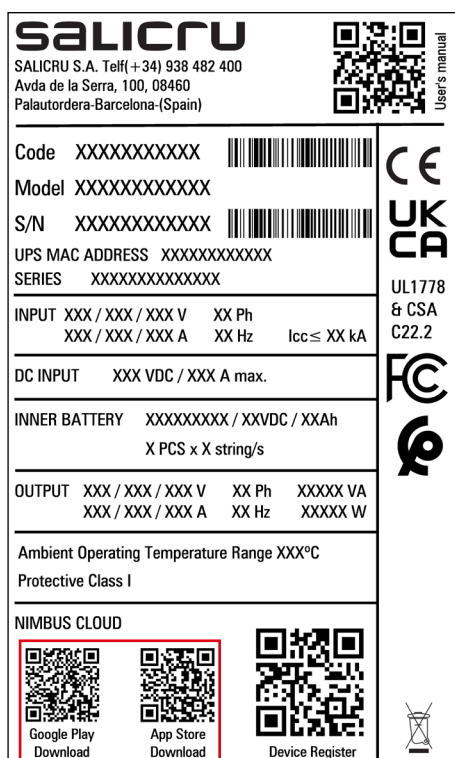
4. REGISTRAR UN EQUIPO EN LA NUBE.

4.1. MEDIANTE LA APLICACIÓN NIMBUS CLOUD (SOLO UPS/SAI).

Si se dispone de alguna serie de SAI/UPS compatible con conectividad, seguir los siguientes pasos:

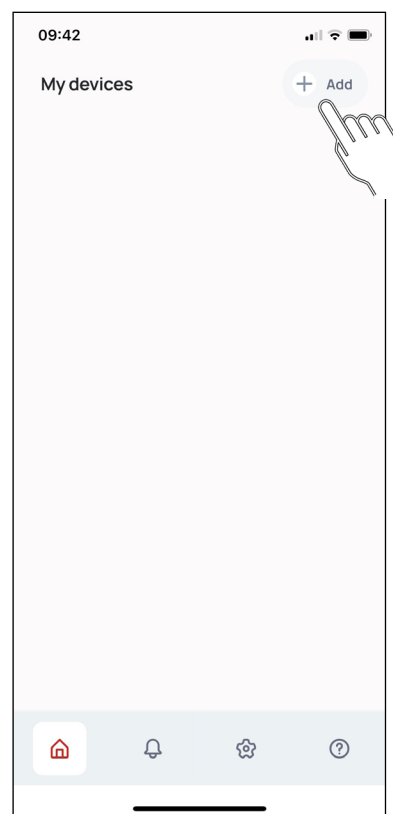
1. Descargar la aplicación NIMBUS CLOUD disponible en App Store y Play Store.

El QR con el link de descarga se encuentra en la etiqueta del dispositivo.

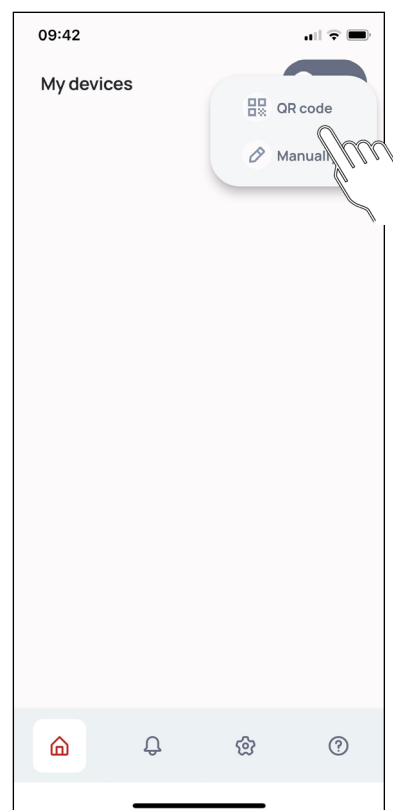


2. Iniciar sesión en la aplicación. Si no se dispone de una cuenta es preciso registrarse. Si se dispone de una cuenta creada con algún otro servicio de SALICRU, es posible utilizar la misma.

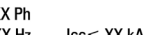
3. En la pestaña "Mis dispositivos" hacer click en el botón "Añadir".



4. Seleccionar la opción "Código QR".



5. Escanee el código QR del dispositivo que encontrará en la etiqueta del dispositivo.

SALICRU SALICRU S.A. Telf (+34) 938 482 400 Avda de la Serra, 100, 08460 Palautordera-Barcelona (Spain)		 User's manual
Code XXXXXXXXXXXX		CE UK CA UL1778 & CSA C22.2 FC 
Model XXXXXXXXXXXX		
S/N XXXXXXXXXXXX		
UPS MAC ADDRESS XXXXXXXXXXXX		
SERIES XXXXXXXXXXXX		
INPUT XXX / XXX / XXX V XX Ph XXX / XXX / XXX A XX Hz Icc ≤ XX kA		
DC INPUT XXX VDC / XXX A max.		
INNER BATTERY XXXXXXXX / XXVDC / XXAh X PCS x X string/s		
OUTPUT XXX / XXX / XXX V XX Ph XXXX VA XXX / XXX / XXX A XX Hz XXXX W		
Ambient Operating Temperature Range XXX°C Protective Class I		
NIMBUS CLOUD  Google Play Download  App Store Download  Device Register		

6. La página se redirigirá a la página de creación del dispositivo con la información del equipo correctamente cumplimentada. Termine de llenar los campos "Nombre del dispositivo" y "Localización".


Dispositivo nuevo


Información del dispositivo

NOMBRE DEL DISPOSITIVO

 Agregue una descripción memorable para recordar fácilmente su dispositivo
 SLC TWIN RT3

UUID
 cf0c6d8d1d2b

El UUID se encuentra en la etiqueta del producto.
 NÚMERO DE SERIE
 232022D70490

LOCALIZACIÓN
 Seleccione la localización

7. Hacer clic en el botón de guardar para finalizar el registro del dispositivo.
8. En la pestaña de "Mis dispositivos" aparecerá el dispositivo creado. Esperar a que establezca conexión correctamente. El dispositivo ya está listo para su uso.

4.2. MEDIANTE PORTAL WEB (SOLO ESTABILIZADORES DE TENSIÓN Y SISTEMAS DC).

Si se dispone de una serie de sistemas DC o estabilizadores de tensión compatible con conectividad, seguir los siguientes pasos:

1. Escanear el código QR del dispositivo que se encuentra en la etiqueta del dispositivo.
2. Hacer clic en el link que aparecerá en pantalla. Ello deberá redirigir a la web <https://nimbus.salicru.com>.
3. Iniciar sesión en la página web. Si no se dispone de cuenta, es preciso registrarse. Si se dispone una cuenta creada con algún otro servicio de SALICRU, es posible utilizar la misma.
4. La página se redirigirá a la página de creación del dispositivo con la información del equipo correctamente cumplimentada. Terminar de llenar los campos "Nombre del dispositivo" y "Localización".
5. Hacer clic en el botón de guardar para finalizar el registro del dispositivo.
6. En la pestaña "Dispositivos" aparecerá el dispositivo creado. Esperar a que se establezca la conexión correctamente. El dispositivo ya está listo para su uso.

Blank page with horizontal dotted lines for writing.

SALICRU

Avda. de la Serra 100

08460 Palautordera

BARCELONA

Tel. +34 93 848 24 00

sst@salicru.com

SALICRU.COM



La red de servicio y soporte técnico (S.S.T.),
la red comercial y la información sobre la
garantía está disponible en nuestro sitio web:
www.salicru.com

Gama de Productos

Sistemas de Alimentación Ininterrumpida SAI/UPS

Fuentes de Alimentación

Variadores de Frecuencia

Onduladores Estáticos

Inversores Fotovoltaicos

Estabilizadores de Tensión



@salicru_SA



www.linkedin.com/company/salicru

SALICRU



USER MANUAL



EN

NIMBUS CLOUD CONNECTIVITY MANUAL



NIMBUS

SALICRU

Contents

1. INTRODUCTION.

- 1.1. COMPATIBLE EQUIPMENT WITH CONNECTIVITY.

2. INSTALLATION.

- 2.1. WITH NIMBUS CARD.
- 2.2. WITHOUT NIMBUS CARD.
 - 2.2.1. Integrated Ethernet connectivity.
 - 2.2.2. Integrated connectivity via WiFi device.

3. COMMISSIONING.

- 3.1. PRE-REQUIREMENTS.
 - 3.1.1. NTP server configuration with NIMBUS card.
 - 3.1.2. NTP server configuration without NIMBUS card.
 - 3.1.3. IP configuration.
- 3.2. FIREWALL REQUIREMENTS.
 - 3.2.1. Firewall requirements for connectivity with NIMBUS card.
 - 3.2.1.1. Option 1 (recommended): full opening of ports 443 and 8883.
 - 3.2.1.2. Option 2 (not recommended): google hostnames and ports relationship.
 - 3.2.2. Firewall requirements for connectivity without NIMBUS card.
 - 3.2.2.1. Google hostnames and ports relationship.

4. REGISTER AN EQUIPMENT IN THE CLOUD.

- 4.1. VIA NIMBUS CLOUD APPLICATION (UPS ONLY).
- 4.2. VIA WEB PORTAL (ONLY VOLTAGE STABILISERS AND DC SYSTEMS).

1. INTRODUCTION.

For some series of UPS, DC systems and stabilisers of the SALICRU brand, it is possible to monitor the equipment in real time, completely remotely and without the need to be in the same network where the equipment is installed.

For this purpose, a platform and a mobile application are available where the user can view the status of the equipment, control the communications card, view the location of the equipment and customise notifications in the event of an alarm.

On the **SLC ADAPT2**, **SLC CUBE4**, **SLC TWIN PRO3**, and **SLC TWIN RT3** series, you can find out if the device is connected and sending data to the cloud by looking for the following icon:



Otherwise, the following icon will be displayed:



Reasons that may cause a computer not to be connected are:

- The card is not properly connected to the network.
- The network to which the card is connected does not have internet access..

1.1. COMPATIBLE EQUIPMENT WITH CONNECTIVITY.

Serie SAI/UPS	Nimbus - MAXI	Nimbus - MINI	Integrated IoT
SLC CUBE3/3+	✓	✗	✗
SLC X-PERT	✓	✗	✗
SLC X-TRA	✓	✗	✗
SLC ADAPT X	✗	✓	✗
SLC ADAPT2	✗	✓	✗
SLC CUBE4	✗	✓	✗
SLC TWIN RT2	✗	✓	✗
SLC TWIN PRO2	✗	✓	✗
SLC TWIN/3 PRO2	✗	✓	✗
SLC TWIN PRO3	✗	✓	✓
SLC TWIN RT3	✗	✓	✓
DC (*) systems			
DC POWER-S	✓	✗	✗
DC POWER-L	✓	✗	✗
Voltage Stabiliser (*)			
EMI3	✓	✗	✗

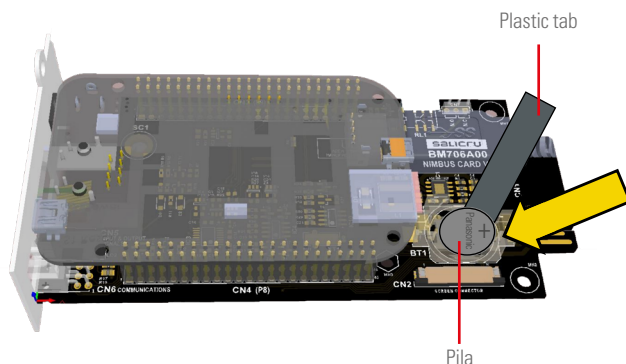
(*) Connectivity for these series is only offered via the remote maintenance panel.
Not available on the mobile App.

2. INSTALLATION.

2.1. WITH NIMBUS CARD.

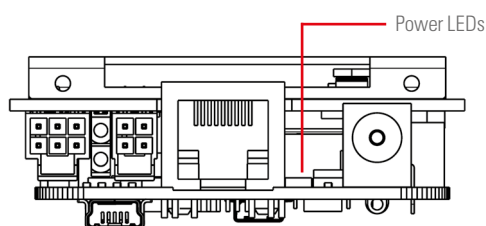
If you have a NIMBUS card, proceed as follows.

1. Remove the protective foil from the battery of the NIMBUS card.

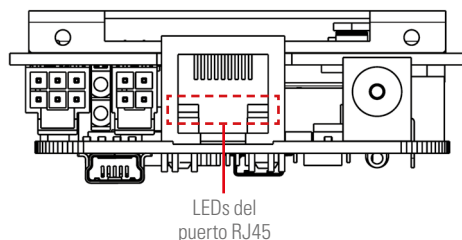


2. Plug the NIMBUS card into the corresponding slot of a previously connected device. It must be snapped into place.

The card will be powered directly from the device and therefore no external power supply is required. If the card has been inserted correctly, the power LEDs will light up blue.

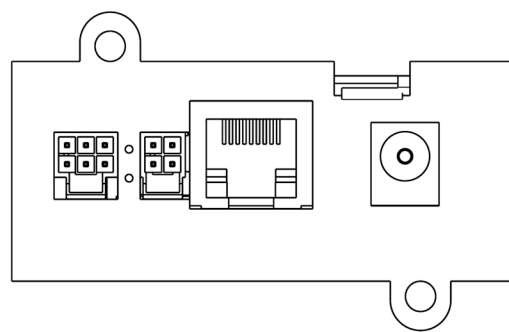


3. Connect an RJ45 cable with one end to the card and the other to the Ethernet socket. The lights on the RJ45 port of the card should come on..



4. Once the NIMBUS card has been correctly inserted in the equipment, it is ready for use. The latest available version of the NIMBUS card will be installed by default.

By placing the protective cover on the NIMBUS card, it should finally look like the following picture.



2.2. WITHOUT NIMBUS CARD.

For the SLC TWIN PRO3 / RT3 series, in addition to allowing connectivity with a NIMBUS card, it is also possible to connect without a NIMBUS card. There are two ways to do this.

2.2.1. Integrated Ethernet connectivity.

Simply connect one end of an RJ45 cable to the Ethernet input of the UPS and the other to the network.

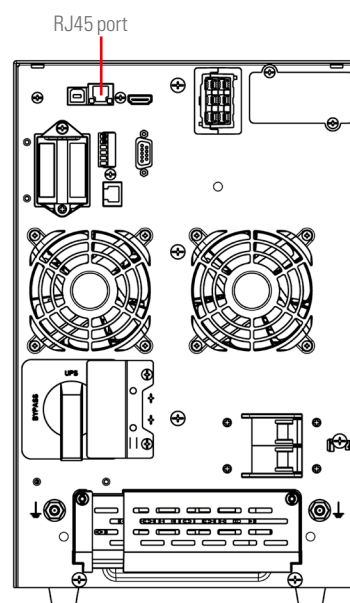


Fig. 1. Ethernet connection on the SLC TWIN PRO3 series UPSs.

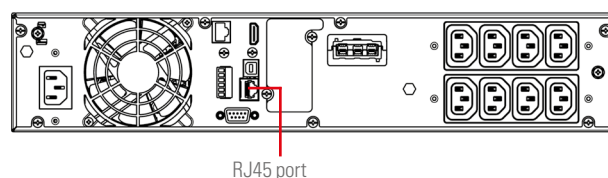


Fig. 2. Ethernet connection on SLC TWIN RT3 series UPSs.

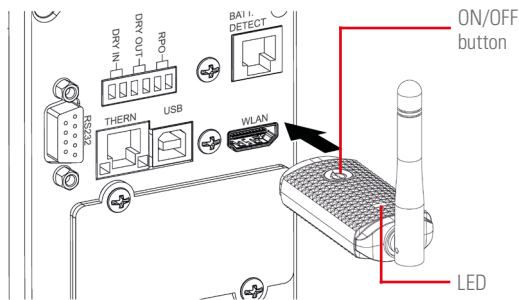
Note: Review the firewall requirements for using the OTA firmware update. You must enable access in <http://firmware.salicru.com> and tomqtt.2030.ltsapis.google.



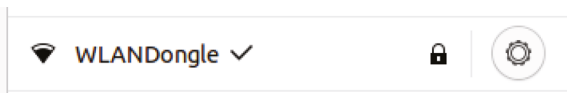
Important: NTP server synchronisation is required to ensure correct cloud connection and data transfer. You must have access to <http://pool.ntp.org>; otherwise, modify your NTP server so that IoT gets the correct timestamp.

2.2.2. Integrated connectivity via WiFi device.

1. Connect the WiFi device to the HDMI port indicated for WLAN connection. Wait for the LED to start flashing to indicate a good connection.
2. Press and hold the ON/OFF button on the device for 4-5 seconds. The LED will start flashing at a higher frequency, indicating that the status has changed to "Access point (AP)" mode.



3. Use a computer or mobile phone to connect to the WiFi network "WLANDongle" (password: welcome12) provided by the WiFi device.



4. Connect to the following url <http://192.168.1.1>. A WiFi configuration portal will appear where you will have to enter your WiFi network credentials.

Wireless Setting Portal

This product supports **2.4G Wireless** only

Last status : No AP found

SSID*:

SALICRU

Password:

Obtain an IP address automatically:

Enable

Save



Note: You may have to click on the "Advanced > Continue on unsecured site" option the first time you enter the website.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.1.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the web site, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the web site's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)

Someone could be trying to impersonate the site and you should not continue.

Web sites prove their identity via certificates. Firefox does not trust 192.168.1.1 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

[View Certificate](#)

[Go Back \(Recommended\)](#)

[Accept the Risk and Continue](#)

5. Once you have entered all the data related to your WiFi network, click on "Save" and wait a few seconds. The LED should change from flashing to steady state.

Wireless Setting Portal

This product supports **2.4G Wireless** only

Last status : No AP found

SSID*:

SALICRU

Password:

Obtain an IP address automatically:

Enable

Save

Please waiting...



Important: There are the following WiFi network limitations to consider in order to achieve a satisfactory connection:

- ☐ The WiFi name (SSID) must contain only numbers and letters.
- ☐ Special characters are not supported.
- ☐ Public WLANs that require a second authentication are not supported.
- ☐ 5GB WiFi routers are not supported.
- ☐ Some WLANs that need to enable special features such as "MAC whitelist" will require this additional step.

6. Finally, make sure to enable the integrated IoT service of the UPS through the screen to be able to see the change of the connectivity icon (cloud) reflected once the device is registered.



Important: If an unexpected event occurs during the WiFi connection process, check the following table.

LED status	Description	Action
LED off	Connection to the UPS is not good.	Check the connection between the device and the UPS.
LED flashes slowly (1 flash/second)	The device is not connected to the router.	Check the WiFi network requirements. Check that the credentials entered are correct. Ensure that the WiFi signal strength is "strong" or at least "medium". This can be important, because if the signal is "weak", the connection will be unstable.
LED flashes rapidly (4 flashes/second)	The device is in Configuration mode.	Connect to http://192.168.1.1 to establish a connection to the router.
LED on	The connection to the router was successful.	-

3. COMMISSIONING.

3.1. PRE-REQUIREMENTS.

Regardless of the cloud connection method used (NIMBUS / IoT integrated card) NTP server synchronisation is required to ensure proper cloud connection and data transfer.

You must have access to <http://pool.ntp.org> ; otherwise, modify your NTP server so that IoT gets the correct timestamp.

3.1.1. NTP server configuration with NIMBUS card.

Access the web panel of the NIMBUS card, connecting point-to-point with an Ethernet cable. To do this, follow these steps:

1. The card has an IP address that is always set to 100.0.0.1. To connect to its subnet, a new network connection must be created with the following parameters:
 - ☐ Address: 100.0.0.2
 - ☐ Netmask: 255.255.255.0
 - ☐ Gateway: 100.0.0.1
2. Connect the Ethernet cable from the communications card directly to the computer, or to a switch that allows it to act 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.



4. Log in to the panel with the following credentials:
user: engineer
password: SLC3ng1n

SALICRU

engineer

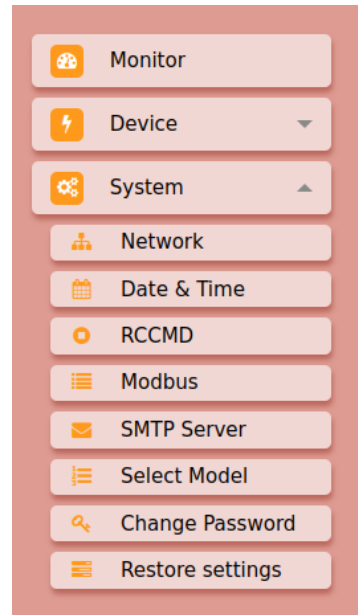
.....

Login

Activar servicio

Restablecer contraseñas

5. Go to the section "System > Date & Time".



6. Configure the NTP servers correctly, according to your preferences. Click on "Save".

Date and time NTP settings

NTP server 1

0.debian.pool.ntp.org

NTP server 3

2.debian.pool.ntp.org

Back

NTP server 2

1.debian.pool.ntp.org

NTP server 4

3.debian.pool.ntp.org

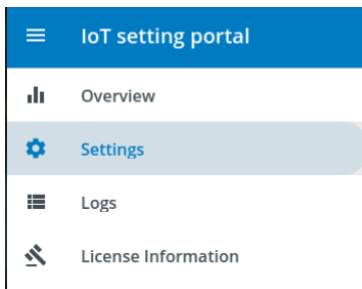
Save

7. Go to "System" > "Network" and click on the "Connectivity Test" tab. Perform the test by clicking on the button.
8. Check that there is no error with the NTP connection..

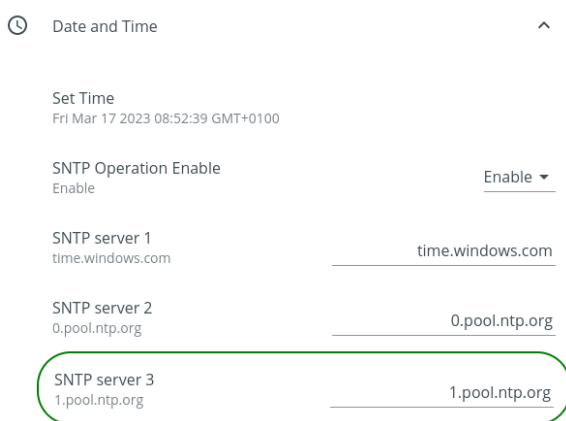
3.1.2. NTP server configuration without NIMBUS card.

Access the web panel and the IP shown on the unit's display. To do this, follow these steps:

1. On the device display, navigate to "Identification". In this section you will find the routes "Embedded IoT IP" and "WLAN IP". Depending on the method used to connect to the cloud, choose one IP or the other. The option that is not connected will appear with "0.0.0.0".
2. Enter the IP address of the device's display in the browser.
3. Log in to the panel with the following credentials:
user: admin
password: Admin*1
4. Go to the section "Settings" > "Preference"..



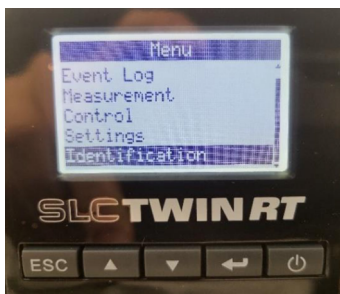
- Configure the NTP servers correctly, according to your preferences. Click on "Save".



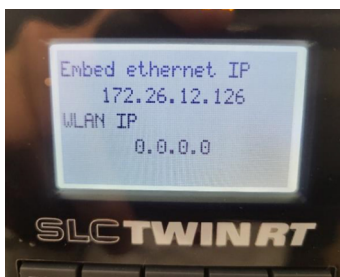
3.1.3. IP configuration.

In order to connect to the interface of the equipment, it is necessary to know beforehand the IP assigned by DHCP. To do this, follow the steps below:

- In the UPS display, go to the option **Identification** → **Embed ethernet IP**.



- Log into the web browser with the IP provided by the display.

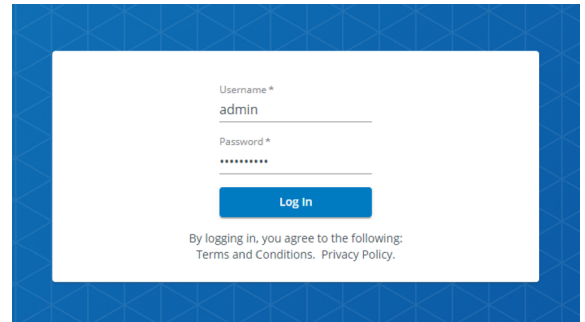


Once the connection is established, this interface will load.

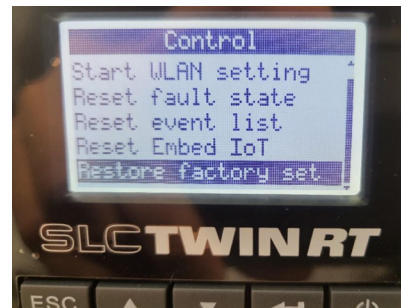
Access credentials:

- Username: **admin**

- Password: **Admin*1**

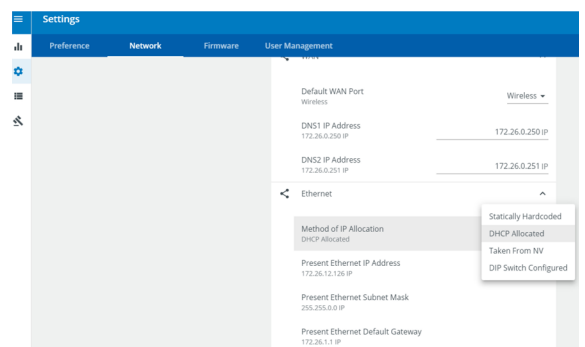


- If you cannot access with these credentials, proceed to reset the UPS options.



- Once access has been obtained, there are 4 options available in **Settings** → **Network** section to change the way in which the equipment obtains the IP address:

- Statically Hardcoded:** the default IP is restored 192.168.1.254.
- DHCP Allocated:** the IP is obtained via DHCP.
- Taken from NV:** a static IP is set.



3.2. FIREWALL REQUIREMENTS.

3.2.1. Firewall requirements for connectivity with NIMBUS card.

Always activate access to <https://archive.salicru.com> with port 443. This web is used to remotely update the NIMBUS communications card, so if access is not guaranteed, the card cannot be updated periodically.

In addition, additional open ports are required, which are detailed below.

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

In order to successfully connect and send data against the remote maintenance portal, it is necessary that the card has **open ports 443 (https) and 8883 (MQTT)** to allow data output and connection to the server from any IP. This will allow a correct and stable connection of your equipment to the portal.

3.2.1.2. Option 2 (not recommended): google hostnames and ports relationship.

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 IP, as the latter are variable.

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

Hostname	Port
mqtt.googleapis.com	443 and 8883
europe-west1-mqtt.clearblade.com	443 and 8883
www.googleapis.com	443
oauth2.googleapis.com	443
accounts.google.com	443

3.2.2. Firewall requirements for connectivity without NIMBUS card.

Always have access to <https://firmware.salicru.com> with port 443 enabled. This web is used to remotely update the IoT device embedded in the device, so if access is not granted, the device cannot be updated periodically..

In addition, additional open ports are required, which are detailed below.

3.2.2.1. Google hostnames and ports relationship.

Hostname	Port
tomqtt.2030.ltsapis.google	443 and 8883

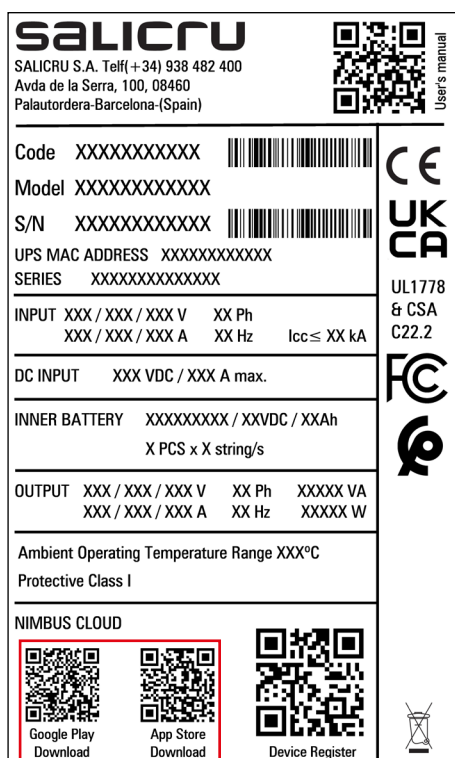
4. REGISTER AN EQUIPMENT IN THE CLOUD.

4.1. VIA NIMBUS CLOUD APPLICATION (UPS ONLY).

If you have a UPS series that supports connectivity, follow the steps below:

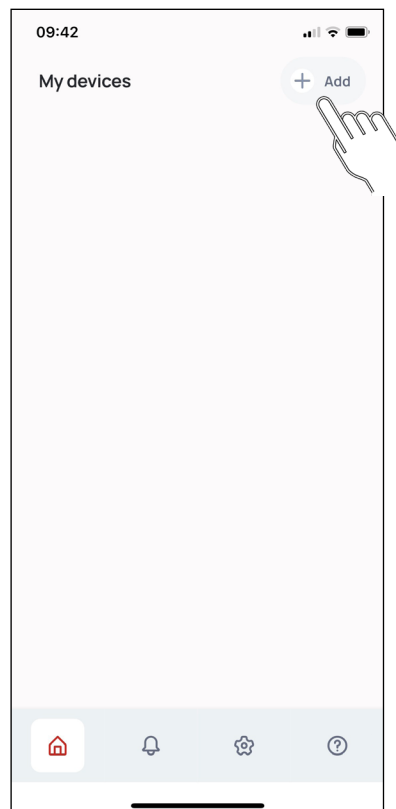
1. Download the NIMBUS CLOUD application available on the App Store and Play Store.

The QR with the download link can be found on the label of the device.

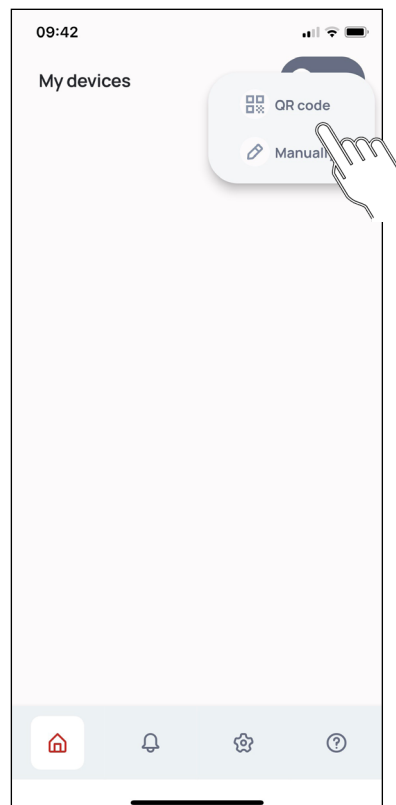


2. Log in to the application. If you do not have an account, you must register. If you have an account created with any other SALICRU service, it is possible to use the same account.

3. In the "My Devices" tab, click on the "Add" button.



4. Select the option "QR Code".



5. Scan the QR code of the device found on the label of the device.

SALICRU SALICRU S.A. Telf (+34) 938 482 400 Avda de la Serra, 100, 08460 Palautordera-Barcelona (Spain)		 User's manual
Code XXXXXXXXXXXX Model XXXXXXXXXXXX S/N XXXXXXXXXXXX UPS MAC ADDRESS XXXXXXXXXXXX SERIES XXXXXXXXXXXX	 	  UL1778 & CSA C22.2
INPUT XXX / XXX / XXX V XX Ph XXX / XXX / XXX A XX Hz Icc ≤ XX kA		
DC INPUT XXX VDC / XXX A max.		
INNER BATTERY XXXXXXXX / XXVDC / XXAh X PCS x X string/s		
OUTPUT XXX / XXX / XXX V XX Ph XXXX VA XXX / XXX / XXX A XX Hz XXXX W		
Ambient Operating Temperature Range XXX°C Protective Class I		
NIMBUS CLOUD		
 Google Play Download	 App Store Download	 Device Register

6. The page will redirect to the device creation page with the device information correctly filled in. Finish filling in the fields "Device name" and "Location".


Dispositivo nuevo


Información del dispositivo

NOMBRE DEL DISPOSITIVO


Agregue una descripción memorable para recordar fácilmente su dispositivo

SLC TWIN RT3

UUID
 cf0c6d8d1d2b


El UUID se encuentra en la etiqueta del producto.

NÚMERO DE SERIE
 232022D70490

LOCALIZACIÓN


Seleccione la localización

7. Click the save button to finalise the device registration.
8. The created device will appear in the "My devices" tab. Wait for it to establish a successful connection. The device is now ready for use.

4.2. VIA WEB PORTAL (ONLY VOLTAGE STABILISERS AND DC SYSTEMS).

If you have a series of DC systems or voltage stabilisers that are compatible with connectivity, follow the steps below.:

1. Scan the QR code of the device found on the label of the device.
2. Click on the link that will appear on the screen. This should redirect you to the website <https://nimbus.salicru.com>.
3. Log in to the website. If you do not have an account, you must register. If you have an account created with another SALICRU service, it is possible to use the same account.
4. The page will redirect to the device creation page with the device information correctly filled in. Finish filling in the fields "Device name" and "Location".
5. Click the save button to finalise the device registration.
6. The device created will appear in the "Devices" tab. Wait until the connection is successfully established. The device is now ready for use.

SALICRU

Avda. de la Serra 100
08460 Palautordera
BARCELONA
Tel. +34 93 848 24 00
sst@salicru.com
SALICRU.COM



Information about the technical support and service network (TSS), the sales network and the warranty is available on our website:

www.salicru.com

Product range

Uninterruptible Power Supplies (UPS)

Power supplies

Variable frequency drives

Static inverters

Photovoltaic inverters

Voltage stabilisers



@salicru_SA



www.linkedin.com/company/salicru

SALICRU

