

MANUAL DE USUARIO



MANUAL DE CONECTIVIDAD NIMBUS CLOUD



NIMBUS

salicru

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	✓	✗	✗

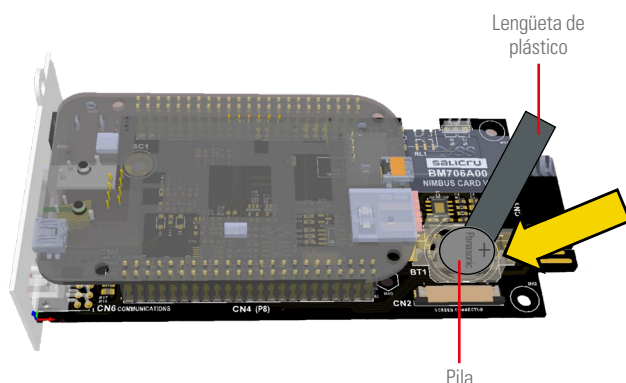
(*) La conectividad para estas series solo se ofrece mediante el panel de telemantenimiento. No están disponibles en la aplicación móvil.

2. INSTALACIÓN.

2.1. CON TARJETA NIMBUS.

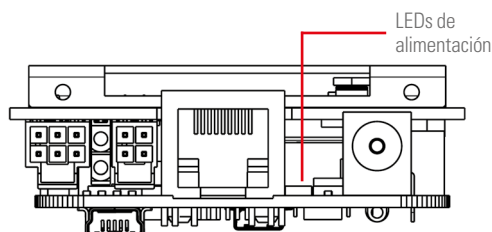
Si se dispone de una tarjeta NIMBUS proceder de la siguiente manera.

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

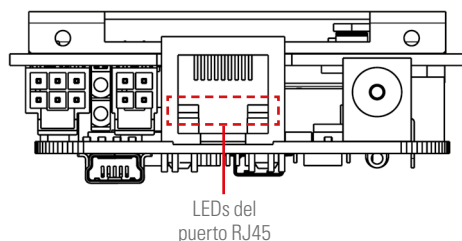


2. Conectar la tarjeta NIMBUS en la ranura correspondiente de un equipo previamente conectado. Debe quedar encajada.

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.

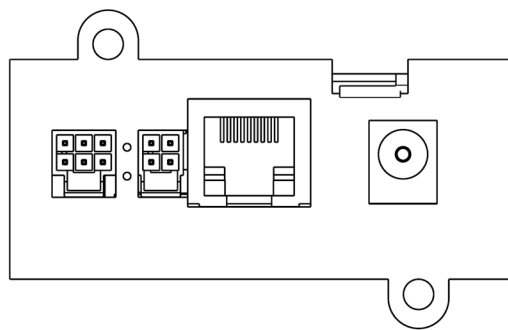


3. Conectar un cable RJ45 con un extremo en la tarjeta y el otro a la toma de ethernet. Las luces del puerto RJ45 de la tarjeta deberán encenderse.



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.

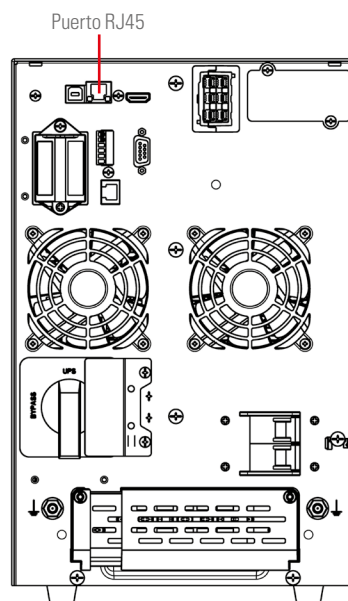


Fig. 1. Conexión Ethernet en los SAI de la serie SLCTWIN PRO3.

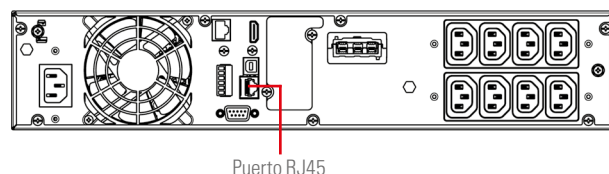


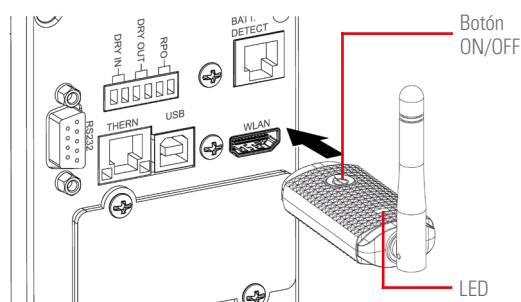
Fig. 2. Conexión Ethernet en los SAI de la serie SLCTWIN RT3.

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.itsapis.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

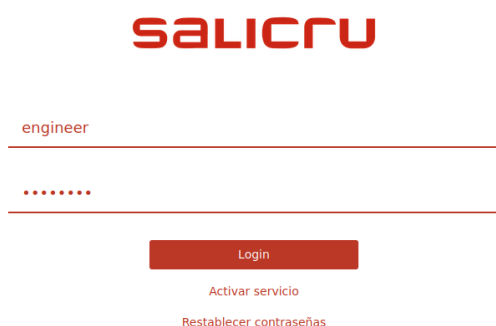
2. Conectar el cable Ethernet de la tarjeta de comunicaciones directamente al ordenador, o bien a un switch que le permita hacer de punto de acceso.

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.

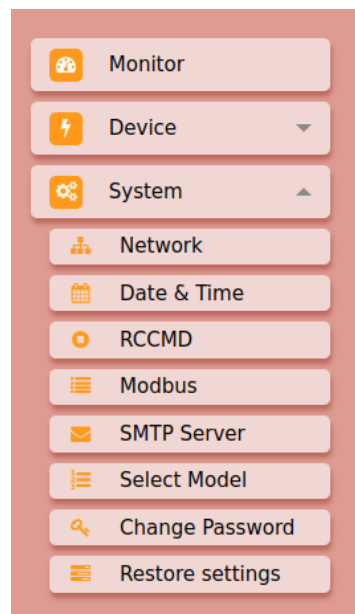


4. Conectarse al panel con las siguientes credenciales:

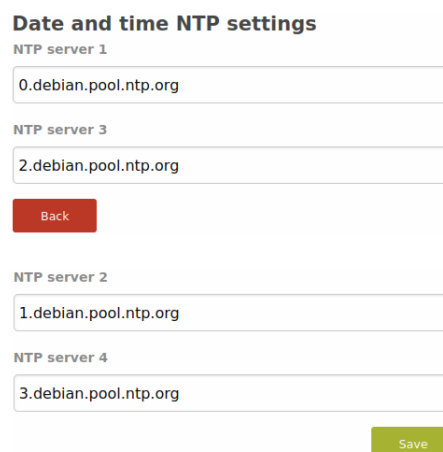
usuario: engineer
contraseña: SLC3ng1n



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



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



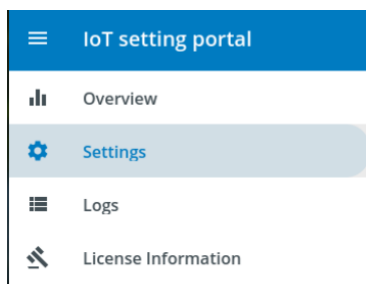
7. Ir a "System" > "Network" y hacer clic en la pestaña "Connectivity Test". Realizar el test pulsando el botón.
8. Comprobar que no hay ningún error con la conexión NTP.

3.1.2. Configuración del servidor NTP sin tarjeta NIMBUS.

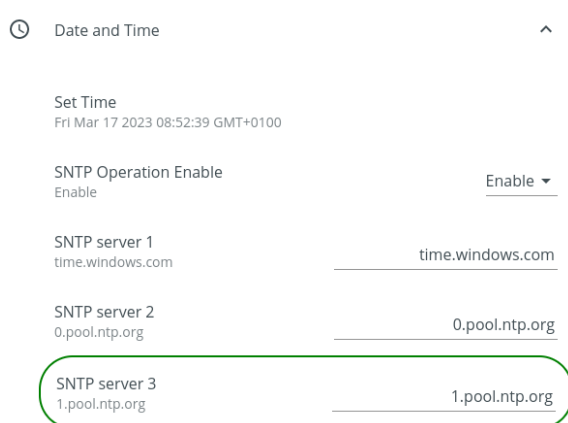
Acceder al panel web y a la IP que se muestra en el display del equipo. Para ello, seguir los siguientes pasos:

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".



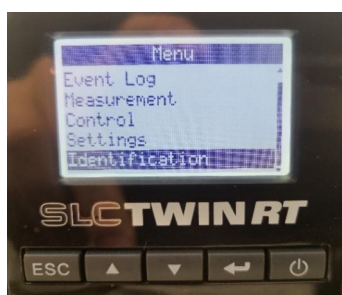
- Configurar correctamente los servidores NTP, en función de sus preferencias. Hacer clic en "Guardar".



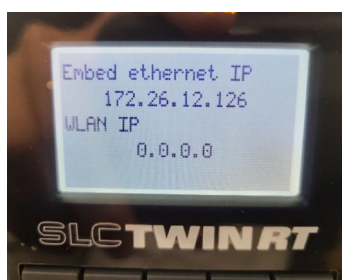
3.1.3. Configuración de la IP.

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**.



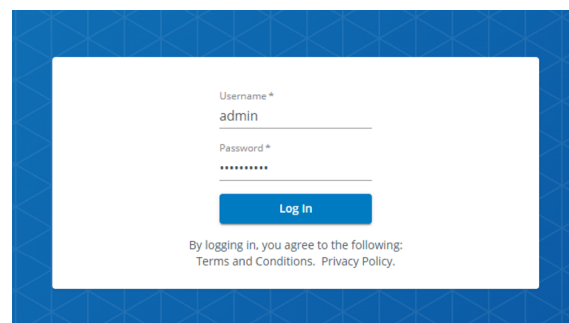
- Entrar en el navegador web con la IP proporcionada por el display.



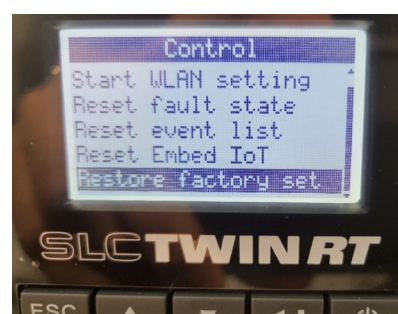
Una vez establecida la conexión se cargará esta interfaz.

Credenciales de acceso:

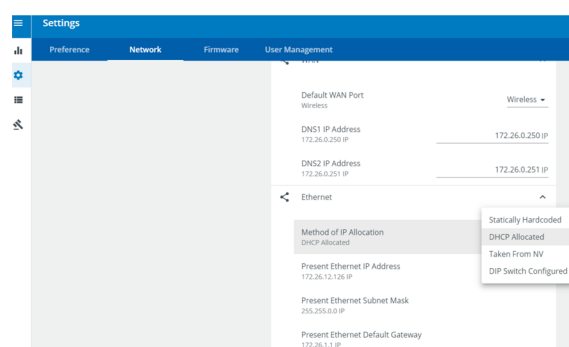
- Username: **admin**
- Password: **Admin*1**



- En el caso de no poder acceder con estas credenciales, proceder a restablecer la 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

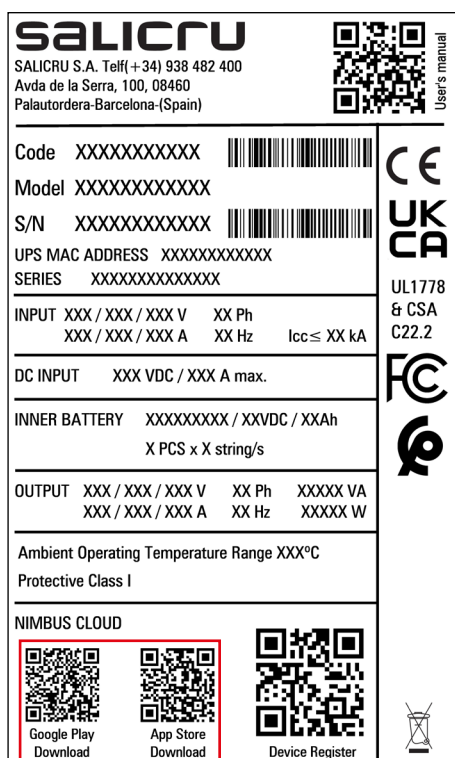
4. REGISTRAR UN EQUIPO EN LA NUBE.

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:

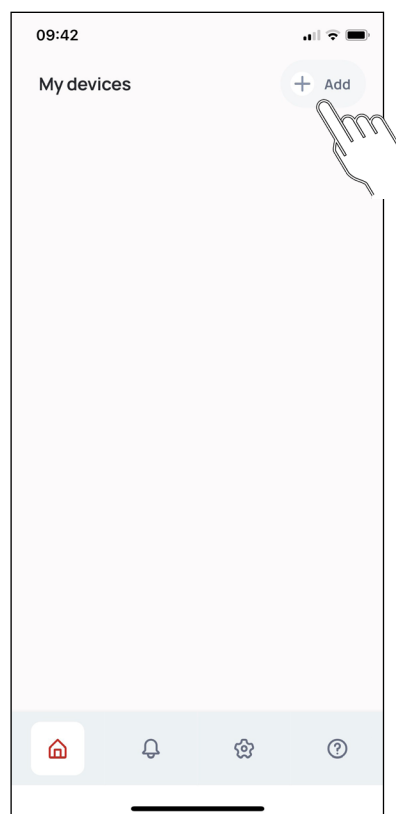
1. Descargar la aplicación NIMBUS CLOUD disponible en App Store y Play Store.

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

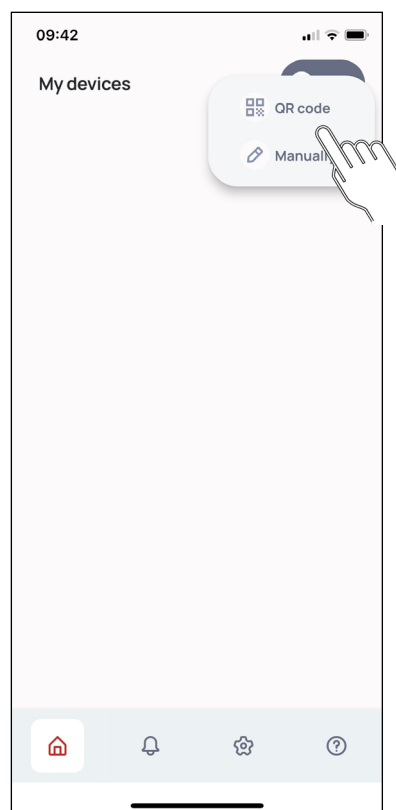


2. Iniciar sesión en la aplicación. Si no se dispone de una cuenta es preciso registrarse. Si se dispone de una cuenta creada con algún otro servicio de SALICRU, es posible utilizar la misma.

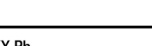
3. En la pestaña "Mis dispositivos" hacer click en el botón "Añadir".



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 XXXXXXXXXX		CE UK CA UL1778 & CSA C22.2
Model XXXXXXXXXX		
S/N XXXXXXXXXX		
UPS MAC ADDRESS XXXXXXXXXX		
SERIES XXXXXXXXXX		FC 
INPUT XXX / XXX / XXX V XX Ph XXX / XXX / XXX A XX Hz lcc ≤ 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		

- 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

- Hacer clic en el botón de guardar para finalizar el registro del dispositivo.
- 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:

- Escanear el código QR del dispositivo que se encuentra en la etiqueta del dispositivo.
- Hacer clic en el link que aparecerá en pantalla. Ello deberá redirigir a la web <https://nimbus.salicru.com>.
- 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.
- 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".
- Hacer clic en el botón de guardar para finalizar el registro del dispositivo.
- En la pestaña "Dispositivos" aparecerá el dispositivo creado. Esperar a que se establezca la conexión correctamente. El dispositivo ya está listo para su uso.

[illegible]

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

Estabilizadores - Reductores de Flujo Luminoso

Fuentes de Alimentación

Variadores de Frecuencia

Onduladores Estáticos

Inversores Fotovoltaicos

Estabilizadores de Tensión



@salicru_SA



www.linkedin.com/company/salicru

salicru

