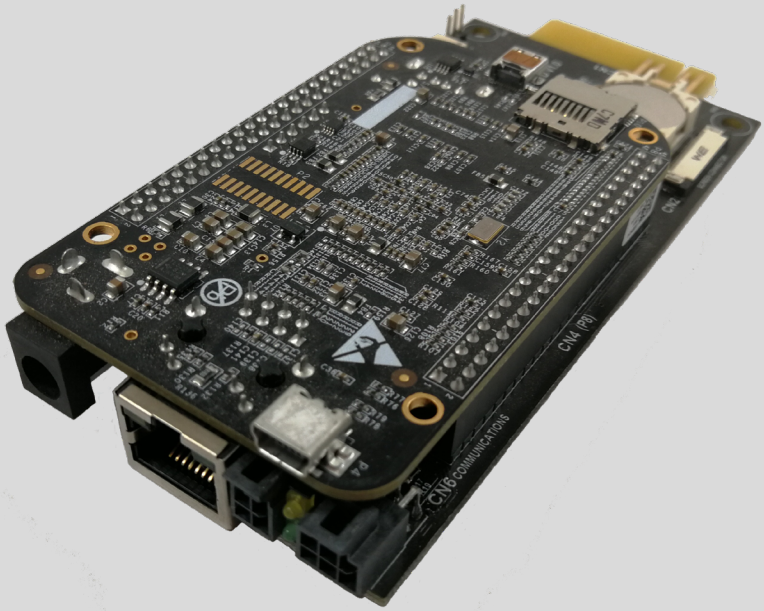
MANUAL DE USUARIO

ES

EN



Tarjeta NIMBUS

salicru

Contents

1. PRESENTACIÓN.

1.1. VISTAS.

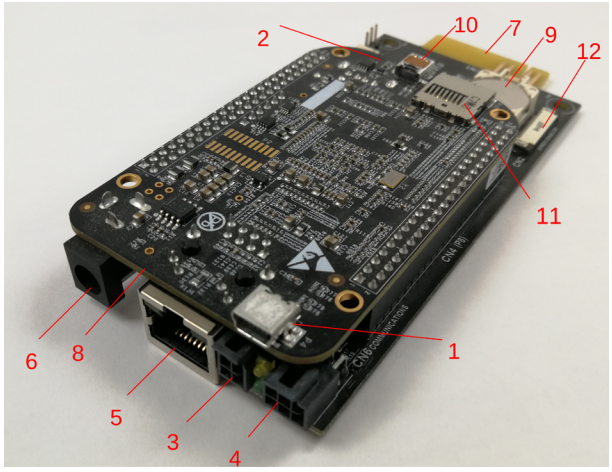


Fig. 1. Vista de la tarjeta NIMBUS MAXI.

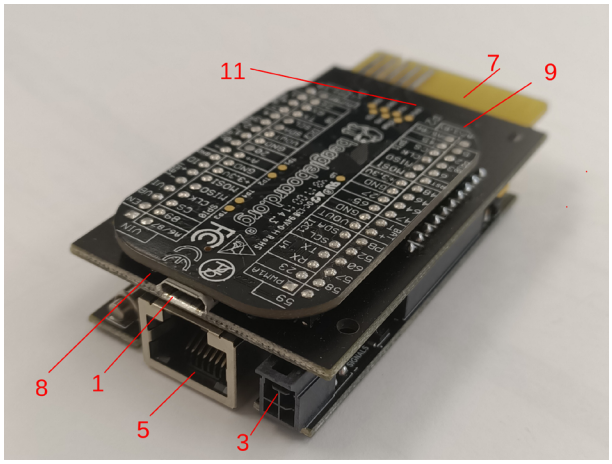


Fig. 2. Vista de la tarjeta NIMBUS MINI.

Descripción	Función
1 Puerto COM1	Interfaz serie para conectar la tarjeta a otros dispositivos mediante el cable USB mini.
2 Puerto COM2	Interfaz serie para conectar la tarjeta a otros dispositivos mediante el cable USB.
3 Puerto RS-232	Interfaz serie para conectar la tarjeta mediante el protocolo RS-232.
4 Puerto RS-485	Interfaz serie para conectar la tarjeta mediante el protocolo RS-485.
5 Puerto RJ-45	Interfaz Ethernet 10/100 Mbit
6 Entrada DC externa	Alimentado por un adaptador de 5V.
7 Puerto Modbus	Interfaz serie para la comunicación modbus con el equipo. Alimenta la tarjeta de forma interna.
8 LEDs de alimentación	Encendidos cuando se alimenta la tarjeta con la entrada DC (interna o externa).
9 RTC	Reloj en tiempo real para mantener actualizada la hora de la tarjeta en caso de fallo de red.
10 Puerto HDMI	Interfaz HDMI para conectar la tarjeta mediante el cable HDMI micro.
11 Conector microSD	Permite actualizar la versión de la tarjeta NIMBUS mediante una microSD.
12 Conector de pantalla	Conector para cable de bus plano para conectar la tarjeta a una pantalla LCD.

Tab. 1. Descripción de las partes constituyentes

1.2. DESCRIPCIÓN DEL SISTEMA.

1.2.1. Introducción.

Los equipos de SALICRU normalmente se encuentran instalados en localizaciones alejadas de la zona de producción, provocando que la información que proporciona el equipo sobre su estado pase por alto en la mayoría de casos. La tarjeta NIMBUS ofrece una solución a este problema, mediante un servicio de telemantenimiento que informa del estado actual del equipo en tiempo real.

La comunicación remota con el equipo facilita las labores de mantenimiento y reparación, al no tener que desplazarse al lugar donde se encuentra instalado para conocer su estado.

Las funcionalidades de la tarjeta NIMBUS están especialmente diseñadas para trabajar con los equipos de SALICRU, siendo actualmente compatible con las siguientes series:

- DC POWER-S
- DC POWER-L
- SLC CUBE3 / CUBE3+
- SLC CUBE4
- EMi3
- RE3
- SLC ADAPTX
- SLC ADAPT 2
- SLC X- PERT
- SLC X- TRA
- SLC TWIN PRO2 A
- SLC TWIN RT2 A
- SLC TWIN PRO2-T
- SLC TWIN R2-T
- SLC TWIN RT2
- SLC TWIN PRO2
- SLC TWIN/3 PRO2
- SLC TWIN PRO3
- SLC TWIN RT3
- SLC ADVANCE R / T
- SLC ADVANCE RT

En función del tipo de equipo, será necesario utilizar una tarjeta NIMBUS-MAXI o bien una tarjeta NIMBUS-MINI. Ambas cuentan con las mismas funcionalidades y modo de funcionamiento. Para saber las correspondencias de cada tarjeta con las distintas series compatibles, referirse a la siguiente tabla:

	Nimbus MAXI	Nimbus MINI
SLC CUBE3/3+	✓	X
SLC X-PERT	✓	X
SLC X-TRA	✓	X
SLC ADAPT-X	X	✓
SLC ADAPT2	X	✓
SLC CUBE4	X	✓
SLC TWIN PRO2 A	X	✓
SLC TWIN RT2 A	X	✓
SLC TWIN PRO2-T	X	✓
SLC TWIN R2-T	X	✓
SLC TWIN RT2	X	✓
SLC TWIN PRO2	X	✓
SLC TWIN/3 PRO2	X	✓
SLC TWIN PRO3	X	✓
SLC TWIN RT3	X	✓
SLC ADVANCE R / T	X	✓
SLC ADVANCE RT	X	✓
Sistemas DC		
DC POWER-S	✓	X
DC POWER-L	✓	X
Estabilizador de tensión		
EMi3	✓	X
RE3	✓	X

Tab. 2. Tabla de compatibilidad (X Compatible, - No compatible).

1.2.2. Características del sistema.

La tarjeta NIMBUS cuenta con distintos servicios básicos integrados que permiten una conexión básica con el equipo.

Servicio básico	Descripción
Panel embarcado	Panel web que permite monitorizar el equipo de forma remota. Al ser dependiente de la tarjeta NIMBUS, si ésta no se encuentra conectada, no se podrá acceder a dicho panel.
Comunicación por MODBUS	Lectura de datos mediante protocolo MODBUS.
RTC	Reloj en tiempo real interno de la tarjeta.
Autoconfiguración del equipo	Al instalar la tarjeta en alguno de los equipos compatibles, ésta detectará automáticamente de qué equipo se trata.
Notificación de alarmas vía panel y SMS	Alerta de notificaciones mediante el panel embarcado en tiempo real, además de ser configurables para ser reportadas también por SMS (mediante protocolo SMTP configurable).
Límites configurables	Se permiten establecer ciertos límites en algunas variables para la realización de dos acciones: o bien notificar por correo SMS o bien realizar una parada de servidores de forma remota.
Servidor DNS	Posibilidad de asignar nombres de dominio propios al equipo.
Dirección IP	A escoger entre DHCP o dirección web estática.
Conexión vía Ethernet o WiFi	Posibilidad de configurar el acceso a Internet mediante conexión cableada Ethernet o haciendo uso de una SSID para conectarse a través de una WiFi.
Servidor Proxy	Posibilidad de configurar un servidor proxy
Configuración de usuarios	Gestión de usuarios propia. Creación de usuarios con los distintos roles disponibles: "administrator"; "engineer" y "guest.
Actualización de paquetes	Actualizar a la última versión la targeta solamente si se dispone de conexión a red.

Tab. 3. Servicios básicos integrados.

1.2.3. Sistemas opcionales.

Aunque con las prestaciones básicas del sistema la tarjeta NIMBUS ya es capaz de proporcionar un telemantenimiento y el acceso a los datos del equipo, con los sistemas opcionales éste se produce de forma más efectiva.

Existen dos tipos de sistemas opcionales:

- Protocolos de comunicación: proporcionan una mayor adaptabilidad y compatibilidad de la tarjeta con distintos protocolos de comunicación industriales.
- Panel web en la nube: permite monitorizar todos los equipos desde una sola página web sin necesidad de ir uno por uno para detectar los problemas. Ofrece la posibilidad de recibir notificaciones más avanzadas: web push, e-mail o SMS.

El **telemantenimiento con el panel web** también ofrece un soporte técnico más rápido y en tiempo real, al ser una web a la que también tienen acceso los profesionales de SALICRU. De esta forma se reduce el tiempo medio de reparación del equipo en casos inesperados.

Servicio opcional	Descripción
Protocolos de comunicación	
Modbus TCP	Protocolo de comunicación secundario derivado de MODBUS (protocolo de comunicación principal).
Modbus API-REST	Habilitando la conexión externa de la tarjeta es posible efectuar llamadas a los servicios de comunicación sin necesidad de acceder al interior de la tarjeta.
RCCMD	Servicio que permite realizar una parada controlada de servidores en caso de cumplirse ciertas condiciones en el equipo.
SNMP	Protocolo de comunicación secundario. Permite recibir notificaciones a la IP del usuario cuando se activa una alarma.
Protocolo IEC 61850	Estándar internacional que define los protocolos de comunicación entre diferentes equipos ubicados en las subestaciones.
Panel web en la nube	
Panel	Panel web en la nube con acceso a todos los dispositivos contratados con tarjeta NIMBUS activa.
Notificación de alarmas	Alerta de notificaciones mediante web, correo electrónico y SMS.

Tab. 4. Servicios opcionales disponibles.

2. INSTALACIÓN Y PUESTA EN MARCHA.

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

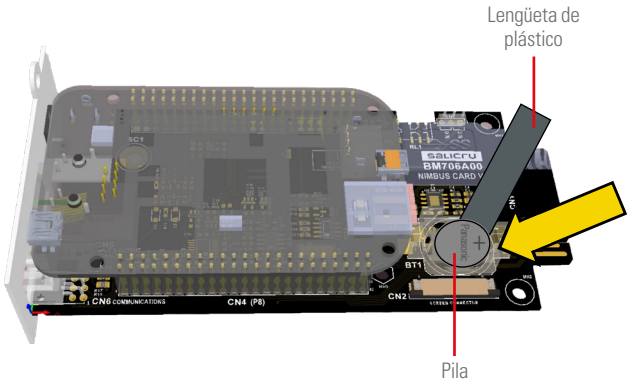


Fig. 3. Desbloqueo de la pila de la tarjeta NIMBUS.

2. Conectar la tarjeta NIMBUS en el slot correspondiente del equipo. Debe quedar encajada.

   La tarjeta se alimentará directamente del equipo y, por lo tanto, no es necesaria una alimentación externa. Si se ha introducido correctamente la tarjeta, los LEDs de alimentación se encenderán. Ver Fig. 4.

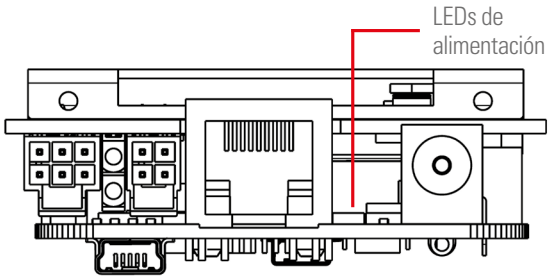


Fig. 4. Targeta NIMBUS insertada en su slot

3. Conectar un cable RJ45: un extremo en la tarjeta y el otro a la toma de Ethernet. Los LED del puerto RJ45 de la tarjeta deberán encenderse. Ver Fig. 5.

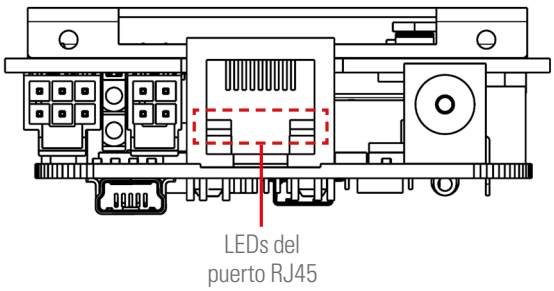


Fig. 5. Conexión del cable RJ-45

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 estará instalada por defecto.

   Una vez ubicada la tapa de protección de la tarjeta NIMBUS, ésta debería tener el aspecto mostrado en la Fig. 6.

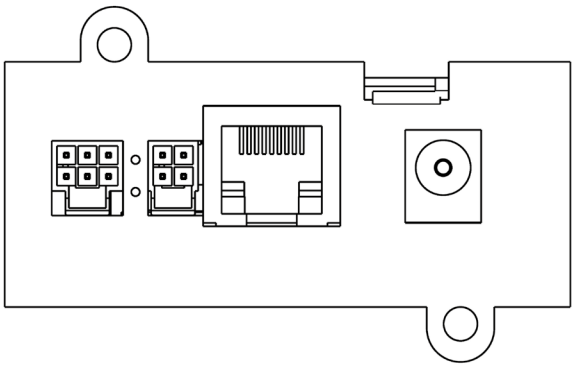


Fig. 6. Aspecto de la tarjeta NIMBUS con la tapa de protección ubicada.

2.1. PRIMERA CONEXIÓN.

Importante: La tarjeta dispone de una dirección IP prefijada para su primera conexión. Dicha IP estará siempre disponible y de forma fija, aunque será necesaria la configuración de la IP secundaria para su correcto uso.

Una vez instalada la tarjeta NIMBUS correctamente en la ranura prevista para tal fin en el equipo, configurar correctamente una IP disponible para poder acceder al panel embarcado de dicha tarjeta de forma remota. Se dispone de dos opciones para ello:

2.1.1. Conexión punto a punto (cable Ethernet).

La IP fijada se encuentra siempre disponible en la dirección 100.0.0.1.

Para acceder a ella, conectar un extremo del cable Ethernet en la ranura específica de la tarjeta NIMBUS y el otro extremo al ordenador.

Configurar la conexión punto a punto accediendo a las conexiones de red y creando una nueva conexión con los siguientes parámetros:

Address	Netmask	Gateway	Metric
100.0.0.2	255.255.255.0	100.0.0.1	

Fig. 7. Parámetros de conexión de red para conexión punto a punto.

Una vez creada correctamente la conexión punto a punto, se debería tener acceso a la tarjeta NIMBUS a través de esta IP. Acceder a través de esta dirección en el navegador web (https://100.0.0.1), y cambiar la dirección final de la tarjeta mediante el apartado "Network" (3.5.1 Network) del panel.

2.2. CONFIGURACIÓN INICIAL.

La tarjeta NIMBUS está configurada con los parámetros necesarios para utilizar de forma satisfactoria el panel embarcado y todas sus funcionalidades.

Estas son:

- Auto configuración del equipo sobre el que está instalada.
- Servidores NTP.
- Servicios de comunicación activos (modbus).
- Dirección web por DHCP (por defecto).
- RTC activo.
- Dirección modbus del esclavo por defecto a 1 y demás parámetros de comunicación adaptados a las necesidades de cada equipo.

Es posible modificar cualquiera de estos parámetros en cualquier momento. Para más información ver el apartado 3.5 System.

Tener en cuenta que modificar algunos parámetros podría causar un comportamiento erróneo del panel. No modificarlos si no se está seguro de las acciones.

3. PANEL EMBARCADO.

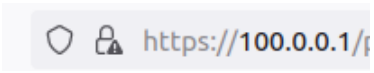
Este servicio permite monitorizar el estado del equipo de forma remota y en tiempo real, pudiendo así acceder directamente al equipo sin necesidad de estar presencialmente donde se encuentra instalado.

3.1. ACCESO AL PANEL.

Cuando la tarjeta se encuentre correctamente instalada en el equipo, seguir los pasos que se detallan a continuación. Esperar alrededor de 5 minutos desde la primera conexión de la tarjeta con el equipo hasta proceder a su acceso mediante panel.

El acceso al panel es mediante https:// y por lo tanto no olvidar escribirlo delante de la dirección IP de la tarjeta cada vez que se desee acceder al panel. En caso contrario, no se producirá una conexión correcta.

Si aún no se ha configurado correctamente la tarjeta para la red, dirigirse al apartado "2.1 Primera conexión". La IP que a emplear es la siguiente:



En caso contrario, introducir en el navegador la nueva IP asignada a la tarjeta.

El acceso al panel vía https se realiza mediante un certificado ssl autofirmado y el navegador lo identificará como no seguro. Para eliminar esta advertencia, seguir los pasos que se detallan a continuación.

3.1.1. Importar certificado.

En función del navegador con el que se acceda, aparecerá uno de los siguientes mensajes. Referirse al apartado correspondiente según las preferencias de navegación.

Solamente es necesario importar el certificado una vez con cualquiera de los navegadores. El sistema guardará el certificado para todos ellos. Si el certificado ya ha sido importado en el ordenador, al intentar reimportarlo se mostrará la opción bloqueada *(Fig. 8)*.

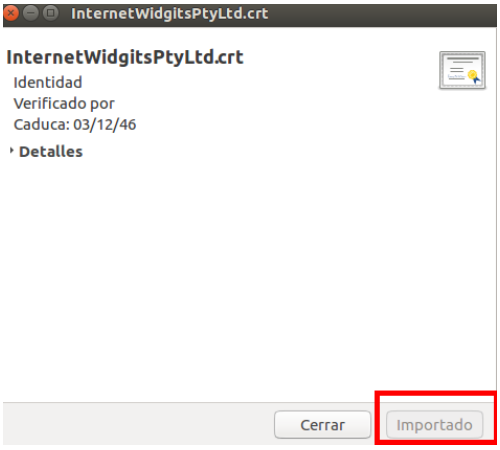


Fig. 8. Pantalla bloqueada para importar certificado.

3.1.1.1. Internet Explorer.

Ejecutar Internet Explorer como administrador. Para ello buscar "Internet Explorer" en el sistema, hacer clic derecho y seleccionar la opción "Ejecutar como administrador", tal como muestra la *Fig. 9*.

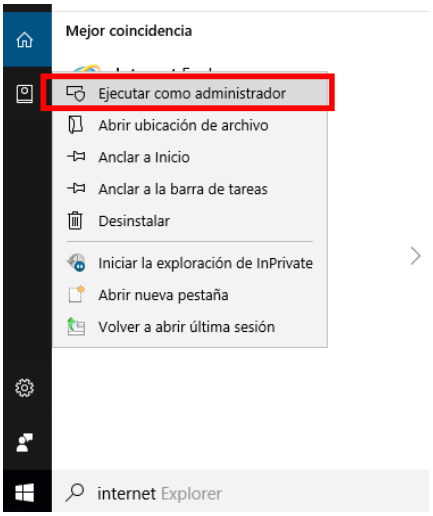


Fig. 9. Pantalla "Ejecutar como administrador"

- Acceder al panel normalmente. Se mostrará una ventana de error. Hacer clic en "Continuar al sitio web (no recomendado)".
- La página web del panel se cargará normalmente. En la barra de direcciones aparecerá un "Error de certificado"; hacer clic *(Fig. 10)*.

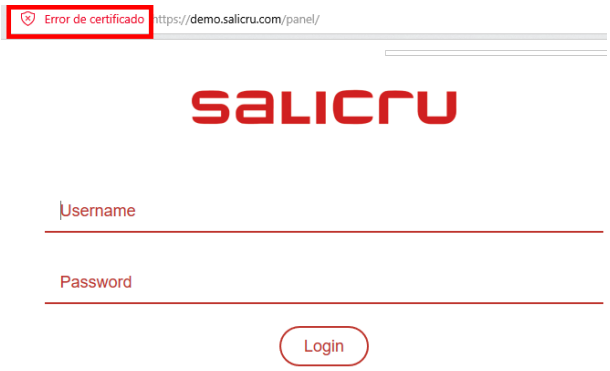


Fig. 10. Error de certificado.

- Se desplegará una ventana. Hacer clic en "Ver certificado" y luego en "Instalar certificado". Por último, hacer clic en "Si" para confirmar su instalación.
- Reiniciar el navegador y acceda al panel. Esta vez no se mostrará el mensaje de advertencia.

3.1.1.2. Mozilla Firefox.

- La primera vez que se acceda al panel aparecerá la siguiente pantalla. Hacer clic en "Avanzado..." para visualizar más opciones.

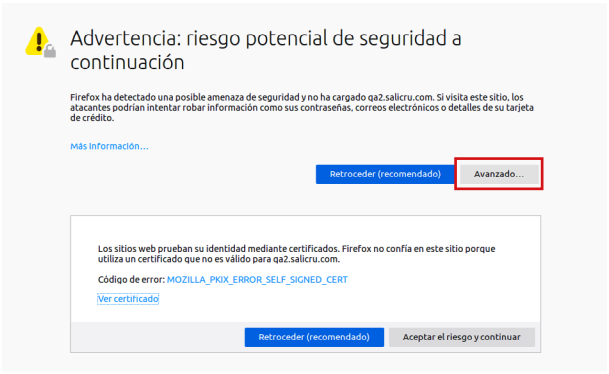


Fig. 11. Panel Mozilla Firefox

Una vez desplegadas todas las opciones, hacer clic en "Ver certificado".

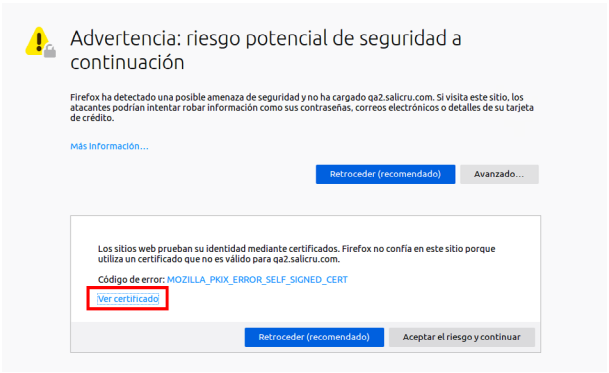


Fig. 12. Panel Mozilla Firefox

- Aparecerá una nueva pantalla con toda la información del certificado del sitio. Hacer clic en la pestaña "Detalles" y pulsar "Exportar..." al final de ésta.

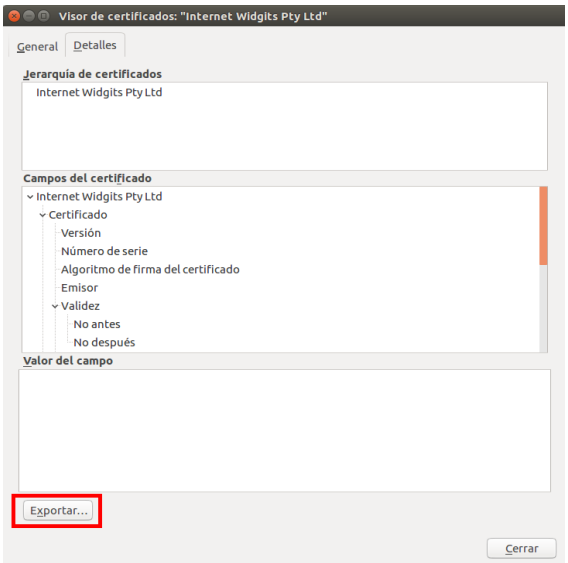


Fig. 13. Ventana "Exportar..."

- Guardar y descargar el archivo donde se desee y ejecutarlo. Se mostrará una pantalla como la que se muestra en la imagen de la *Fig. 14*. Hacer clic en "Importar...".

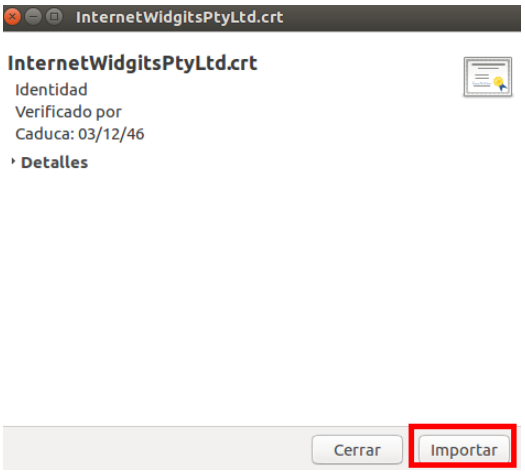


Fig. 14. Ventana "Importar..."

- El sistema requerirá la contraseña del ordenador antes de proceder. Cuando se solicite la etiqueta, introducir "Nimbus" y hacer clic en "Aceptar".

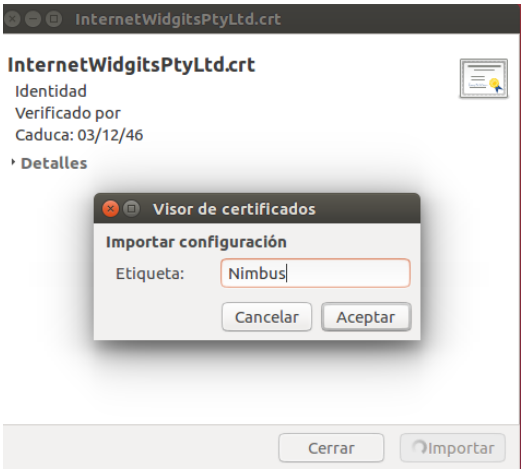


Fig. 15. Ventana "Etiqueta".

- Una vez finalizado este paso, el certificado se habrá importado correctamente. Iniciar el navegador para confirmarlo. En "Preferencias" hacer clic en el menú lateral izquierdo para navegar hasta "Privacidad & Seguridad". Navegar hasta el final de la pestaña hasta encontrar el apartado "Certificados". Hacer clic en "Ver certificados..." *(Fig. 16)*.

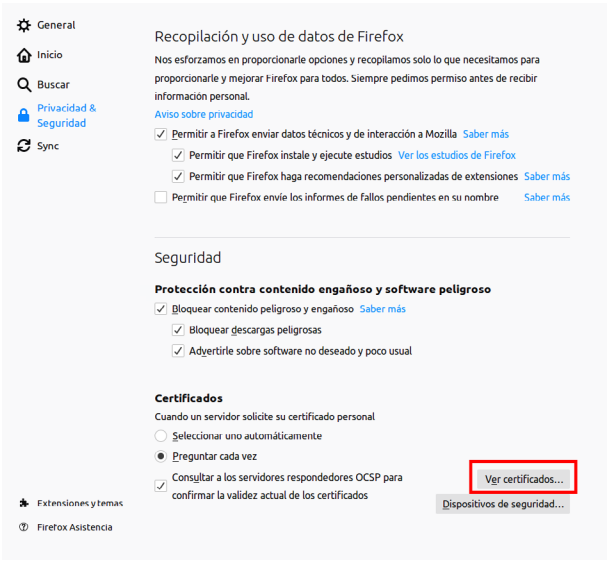


Fig. 16. Menú "Privacidad & Seguridad" de Firefox

- Buscar el nombre del certificado instalado en la lista para verificar su correcta importación:

Fig. 17. Ventana "Administrador de certificados".

- Reiniciar el navegador, acceder al panel y hacer clic en "Aceptar el riesgo y continuar". La próxima vez que se acceda al panel ya no se mostrará el mensaje de advertencia:

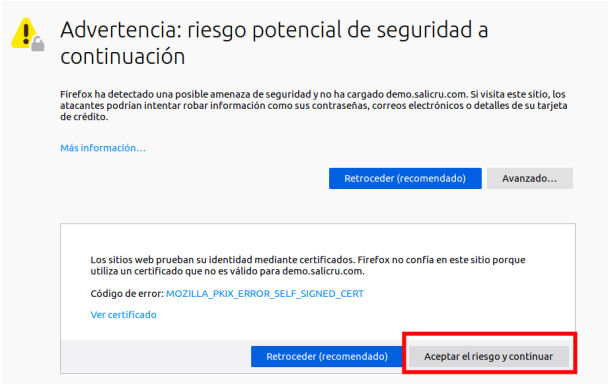


Fig. 18. Ventana "Aceptar riesgo y continuar".

3.1.1.3. Chrome / Opera.

- La primera vez que se acceda al panel se mostrará la siguiente pantalla:

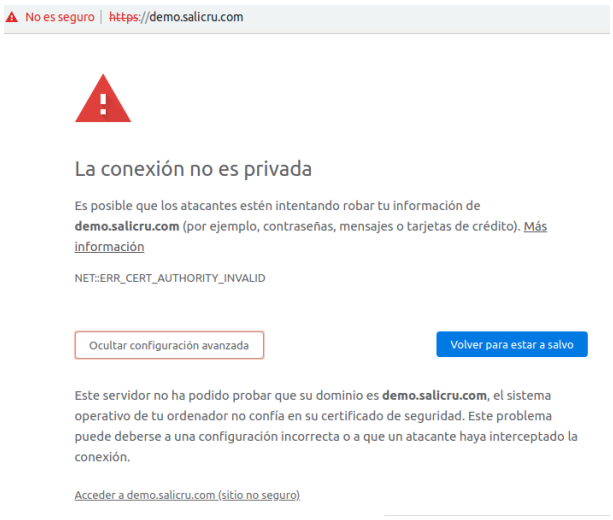


Fig. 19. Pantalla de inicio navegador Chrome / Opera.

- En la barra de dirección, hacer clic en el botón "No es seguro" para desplegar las opciones disponibles. Hacer clic en "Certificado".

Fig. 20. Ventana de Opciones disponibles.

- Aparecerá una nueva pantalla con toda la información del certificado del sitio. Hacer clic en la pestaña "Detalles" y pulsar el botón "Exportar..." al final de ésta *(Fig. 21)*.

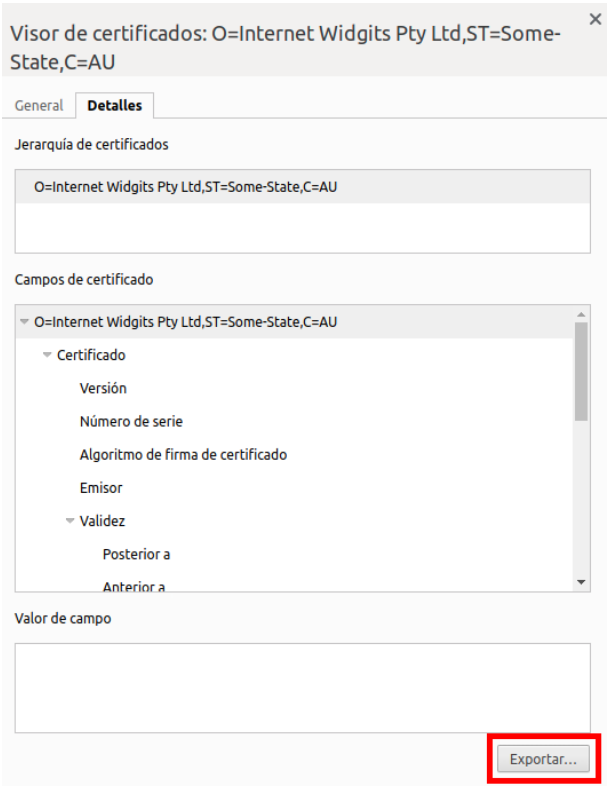


Fig. 21. Pantalla "Visor de certificados - Exportar".

- Guardar y descargar el archivo donde se desee y ejecutarlo. Se mostrará una pantalla como la que muestra la imagen de la *Fig. 22*. Hacer clic en "Importar...".

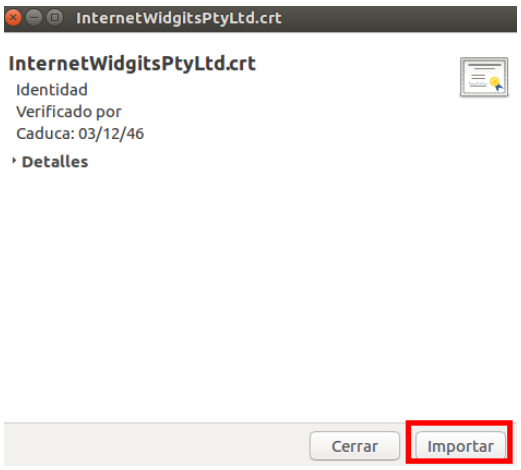


Fig. 22. Pantalla "Importar...".

El sistema requerirá la contraseña de su ordenador antes de proceder. Cuando se solicite la etiqueta, introducir "Nimbus" y hacer clic en "Aceptar", tal como muestra la *Fig. 23*.

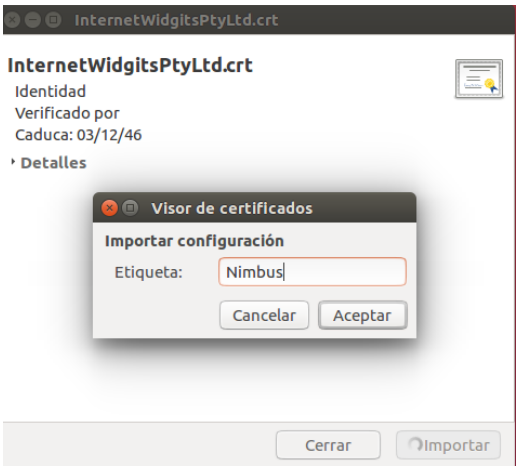


Fig. 23. Pantalla "Visor de certificados"

- Finalizado este paso, el certificado se habrá importado correctamente. Reiniciar el navegador para confirmarlo. En "Configurador" navegar hasta el final de la página y acceder a las opciones avanzadas y hacer clic en el botón "Gestionar certificados". El certificado deberá aparecer en este apartado.

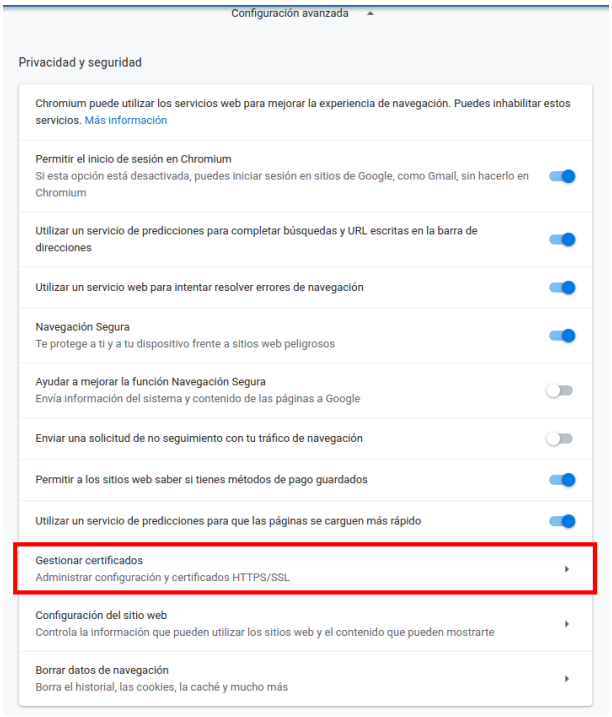


Fig. 24. Pantalla "Configuración avanzada - Gestionar certificados".

- Reiniciar el navegador, acceder al panel y hacer clic en el botón "Aceptar el riesgo y continuar". La próxima vez que se acceda al panel ya no se mostrará el mensaje de advertencia. *(Fig. 25)*.

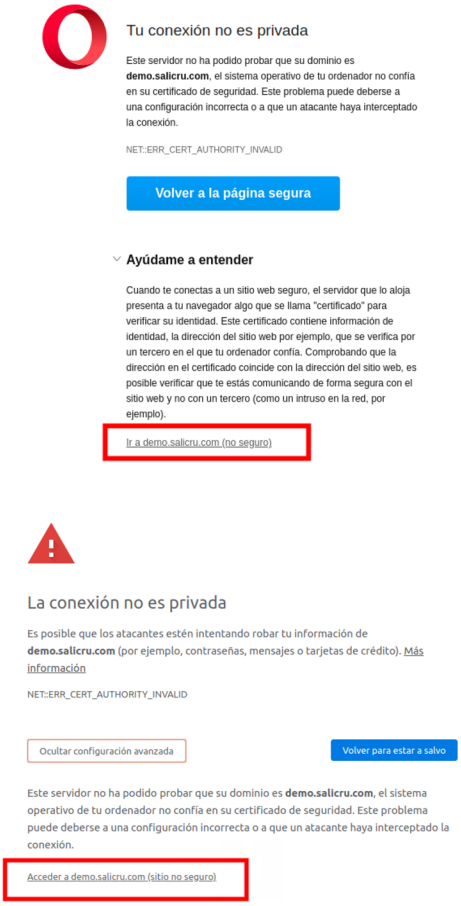


Fig. 25. Pantalla "Mensaje de advertencia".

Dispone de dos maneras para poder conectarse al panel en función de la accesibilidad al equipo:

3.1.2. Conexión local (punto a punto).

Emplear esta opción si la tarjeta no tiene acceso externo a la red.

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

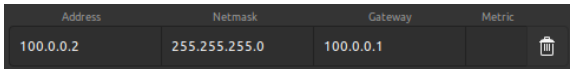


Fig. 26. Parámetros de conexión de red para conexión punto a punto.

2. Conectar el cable Ethernet de la tarjeta de comunicaciones directamente al ordenador, o bien a un switch que permita hacer de punto de acceso.
3. Configurada correctamente la red en el ordenador, y sin ninguna otra fuente de Internet posible (desconectar la WiFi si fuera necesario), introducir la dirección https://100.0.0.1 en el navegador.

3.1.3. Conexión remota.

Nota importante: Si su red se encuentra en el rango 192.168.6.0/24, o bien 192.168.7.0/24, puede provocar interferencias entre las IPs asignadas al dispositivo. Ponerse en contacto con el servicio de atención al cliente para solucionar esta incidencia.

Emplear esta opción si la conexión Ethernet se encuentra disponible o si se desea acceder al panel de forma remota.

1. Iniciar el navegador web escogido. Si se usa IE11 refiérase al apartado 3.1.3 Navegadores compatibles.
2. Introducir la dirección IP asignada a la tarjeta, previamente asignada y establecida con el método descrito en el apartado "2.1 Primera conexión".
3. Si la tarjeta dispone de una dirección dinámica y no se produce satisfactoriamente la conexión al panel, asegurar que dicha dirección es la correcta. Para ello, seguir los pasos descritos en el apartado anterior "3.1.1 Conexión local".

3.2. PANTALLA DE *LOGIN.*

Una vez introducida la dirección Web de la tarjeta en el navegador, se mostrará una página con el contenido siguiente:

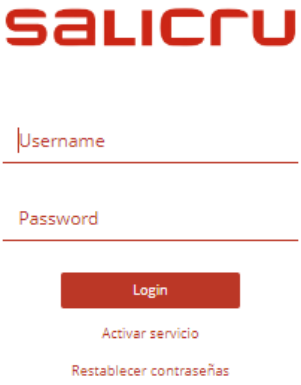


Fig. 27. Pantalla de login y password.

Para iniciar una sesión introducir las credenciales correspondientes, en función de quién desee utilizar el panel.

	Administrador	Ingeniero	Usuario
Nombre de usuario	"administrator"	"engineer"	"guest"
Password	"Nimbus4dm" [2]	"SLC3ng1n" [1] "Nimbus3ng" [2]	"SLCg13st" [1] "Nimbus6st" [2]
Permiso	- Modificar algunos parámetros del equipo. - Modificar parámetros de la tarjeta NIMBUS. - Visualización de medidas. - Gestión de usuarios. - Actualización de servicios.	- Modificar algunos parámetros del equipo. - Modificar parámetros de la tarjeta NIMBUS. - Visualización de medidas.	- Visualizar medidas del equipo.

[1] Hasta el firmware 2.8.6.

[2] Desde el firmware 3.0.0. en adelante.

Tab. 5. Credenciales y permisos.

Una vez introducida de forma válida cualquiera de las claves, se mostrará la página principal del panel descrita en el punto "3.4 Monitor".

3.2.1. Cambio de contraseña primer inicio de sesión.

Si es la primera vez que se accede al panel con un nuevo usuario por defecto (administrator, engineer o guest), se pedirá actualizar la contraseña.

La nueva contraseña no puede ser igual que la por defecto para garantizar la seguridad. Debe contener mínimo 8 caracteres, mayúsculas, minúsculas, números y caracteres especiales.

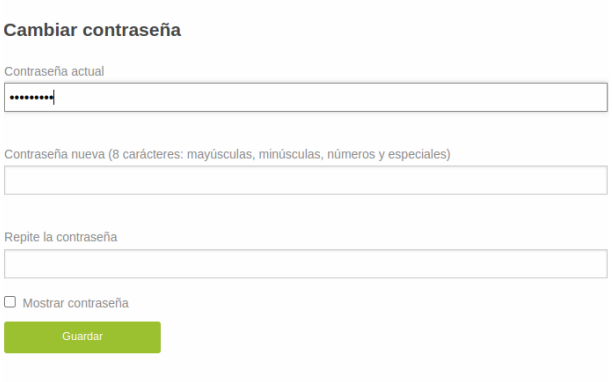


Fig. 28. Pantalla de cambio de contraseña.

Más adelante, se podrá cambiar esta contraseña desde la sección "Cambiar contraseña" una vez se haya accedido al panel embarcado.

Importante: anotar la contraseña introducida ya que no se podrá recuperar via email. Solamente se podrá restablecer la contraseña haciendo un flash completo de la tarjeta, causando una pérdida de las configuraciones en caso de no haberlas guardado.

3.3. ÁRBOL DE NAVEGACIÓN.

El árbol de navegación se encuentra en la parte izquierda de la pantalla. Se mostrará así después de un login **como ingeniero.** El apartado de System no será visible si se accede al panel como usuario.

Fig. 29. Árbol de navegación principal del panel embedded.

Observar que los apartados de "Device" y "System" son desplegables. Al hacer clic sobre ellos se mostrarán las demás opciones.

Para evitar árboles de Navegación largos que puedan llevar a confusión, solamente se permite tener desplegado un apartado global a la vez. Dentro del apartado "Device" puede seguir desplegando el apartado "Metrics".

3.4. MONITOR.

La página "Monitor" de la *Fig. 28* muestra un resumen del estado actual del equipo.

La primera vez que se conecte la tarjeta al equipo, ésta se configurará de forma automática en función del equipo en el que esté trabajando. Tener en cuenta que este proceso suele tardar unos minutos.

Si no se visualiza correctamente el bloque de alarmas o algún otro aspecto de esta ventana, salir del panel mediante la opción de logout y volver a entrar.

Si se continua sin visualizar correctamente alguna parte del panel, eliminar la memoria caché del navegador y pulsar CTRL + F5.

Importante: si no se han adquirido los módulos de medida adicionales para algunas series como la SLC X-PERT, el valor correspondiente a esa medida será negativo. En esta consideración se excluye la corriente de baterías, que puede adoptar un valor negativo cuando está en descarga.

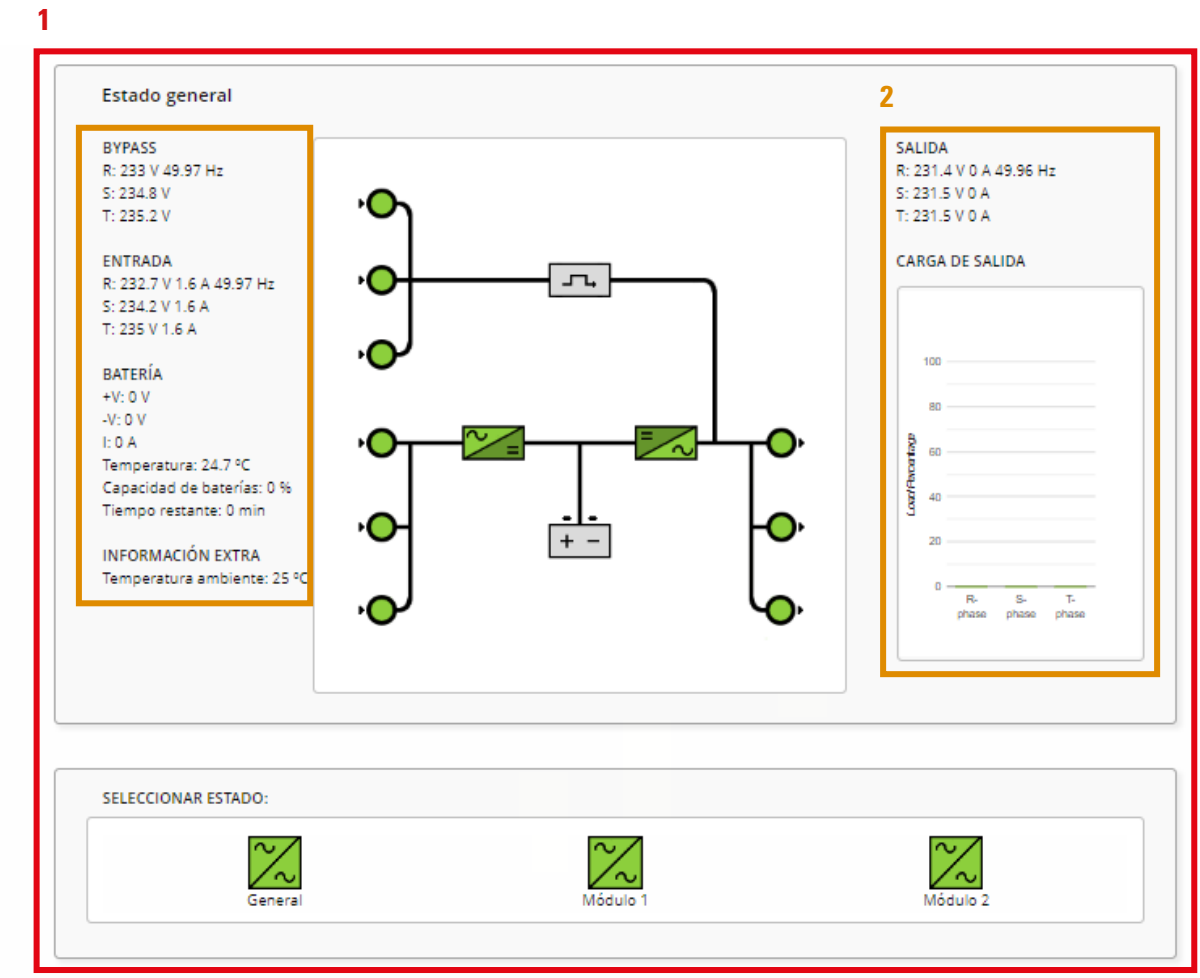


Fig. 30. Sinóptico UPS monitor.

Esta página costa de dos partes básicas:

3.4.1. Sinóptico y medidas.

Un dibujo a modo de representación esquemática del equipo se muestra en la parte superior de la pantalla (bloque 1 de la *Fig. 30*). Los distintos estados del equipo se ven reflejados aquí con distintos colores:

- Rojo:
  - Para elementos distintos a la batería: hay un fallo en esta parte.
  - Para la batería: queda poca carga.
- Verde:
  - Para elementos distintos a la batería: el elemento está activo y no presenta ningún error.
  - Para la batería: carga completa.
- Amarillo (sólo para la batería):
  - La batería se encuentra en descarga o bien la carga es inferior al 100%.
- Gris:
  - No circula corriente por ese elemento o parte del circuito. Por lo tanto, no está activo.
- Blanco:
  - El elemento correspondiente no existe en el equipo.

Rodeando al sinóptico se muestran, a modo de resumen, medidas relevantes de los distintos elementos del equipo con el fin de completar la información básica (bloque 2 de la *Fig. 30*).

3.4.1.1. Serie ADAPT-X & ADAPT2.

Si se dispone de módulos conectados al equipo, acceder a la información individual de cada uno de ellos haciendo clic en el símbolo de bypass correspondiente:

Fig. 31. Representación de módulos en las series ADAPT2 y ADAPTX.

Al hacer clic en cualquiera de ellos se mostrará un monitor individualizado, contando con su propio sinóptico y sus propias medidas, tal como se puede apreciar en la siguiente figura:

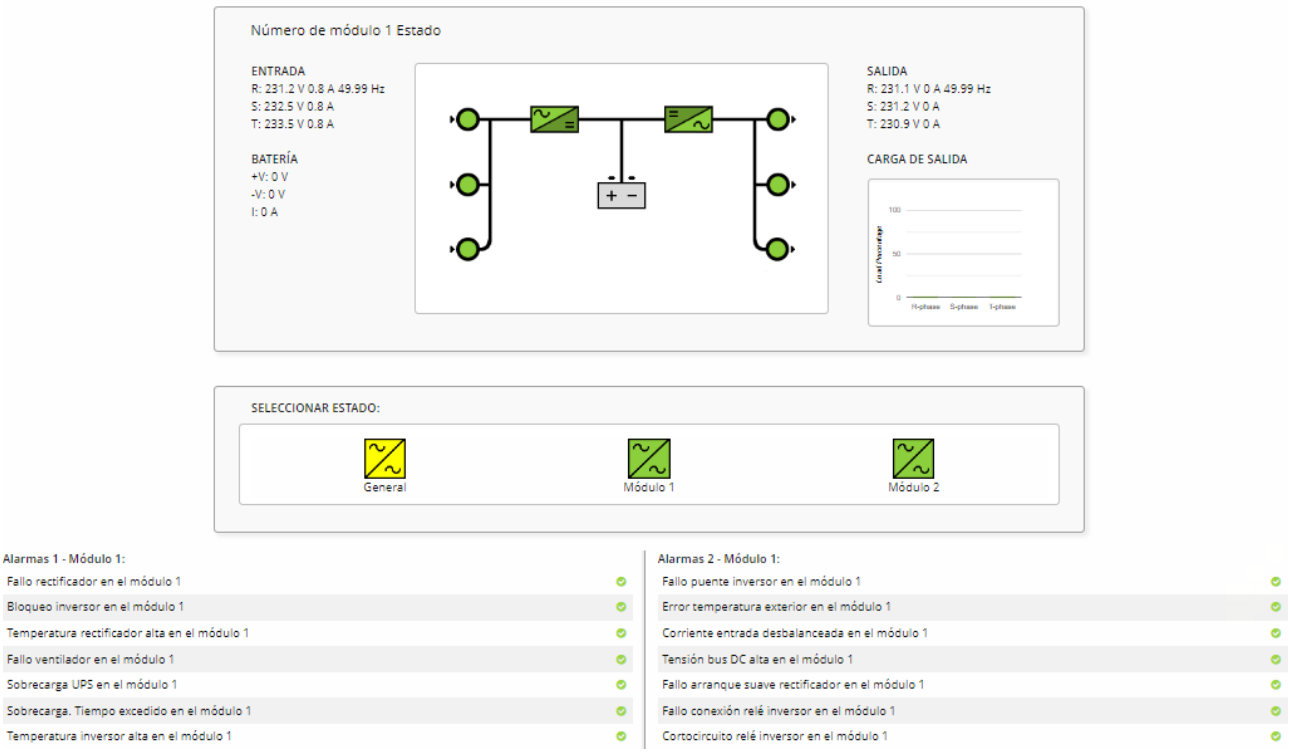


Fig. 32. Sinóptico referente a un solo módulo.

3.4.1.2. Serie SLC CUBE4 7,5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2, SLC TWIN RT2, SLC TWIN PRO3 y SLC TWIN RT3.

En estas series se añade un botón llamado "UPS status" que permite visualizar tanto el estado del sistema como las alarmas.

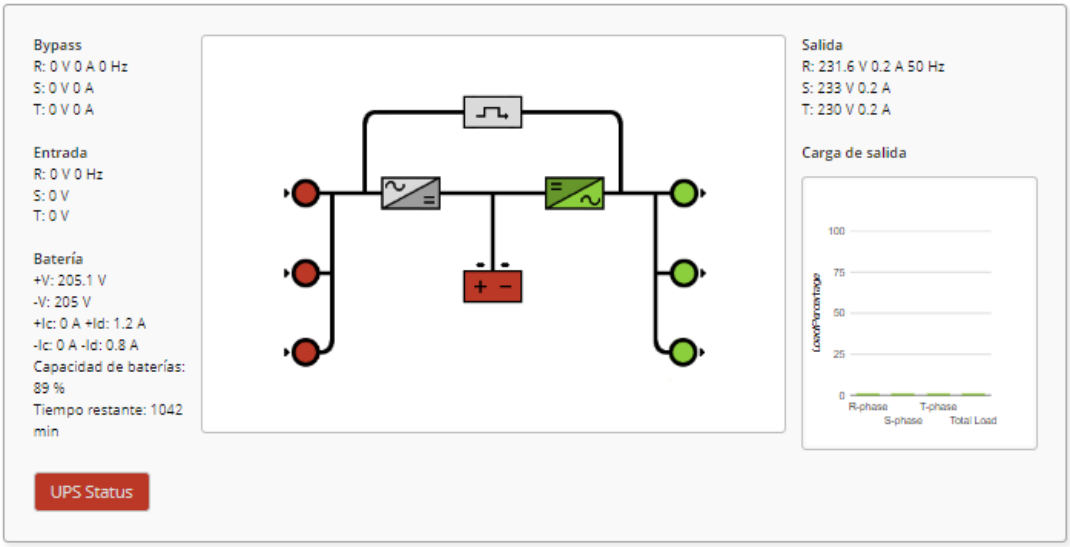


Fig. 33. Sinóptico estado del sistema y alarmas.

Este botón tiene 3 posibles colores en función del estado del sistema:

- Rojo: hay una alarma urgente en el equipo.
- Amarillo: hay una alarma no urgente, una advertencia o el estado del equipo no es el funcionamiento óptimo del sistema (bypass o descarga de batería)
- Verde: no hay alarmas ni warnings activos. Además, el funcionamiento del equipo es óptimo.

Para interaccionar con él, haga clic encima del botón. Se abrirá una ventana emergente que le informará del estado actual del equipo.

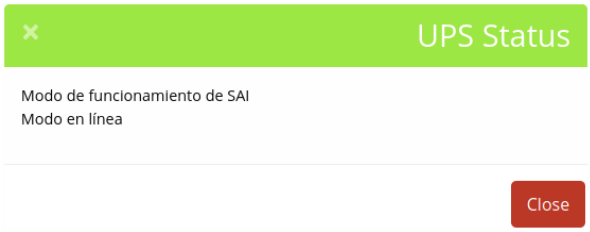


Fig. 34. Detalle del botón "UPS status".

3.4.2. Alarmas.

En la parte inferior de la pantalla se muestran los distintos bloques de alarmas con los que cuenta el equipo y su estado actual (bloque 3).

En color verde se muestran las alarmas no activas y en rojo las activas. Una alarma reconocida en el equipo (ACK) se mostrará igualmente en rojo.

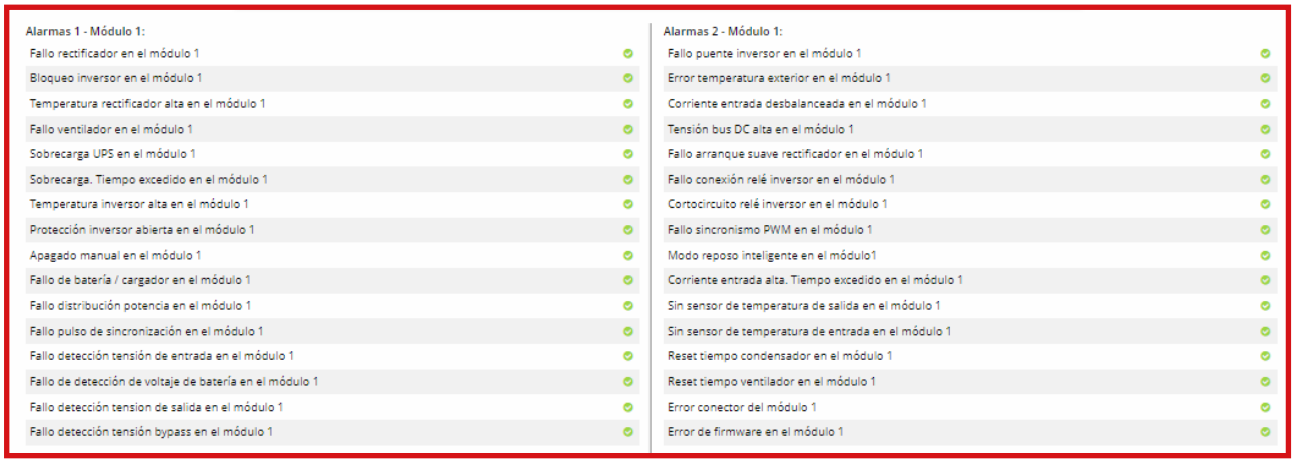


Fig. 35. Parte del sinóptico donde se reflejan las distintas alarmas.

3.5. DISPOSITIVO.

Pulsar sobre "Dispositivo" para desplegar/ocultar las opciones descritas en este punto.

Fig. 36. Menú Dispositivo.

3.5.1. Info.

Página de **solo lectura**. Muestra un resumen de parámetros técnicos del equipo, así como la versión instalada en la tarjeta NIMBUS.

3.5.2. Threshold Settings.

Página de configuración. Ajustes los valores límite sobre los cuales se desea recibir alarmas y notificaciones.

IMPORTANTE: para que la configuración de la página sea correcta, primero es preciso configurar el servidor SMTP y/o el servidor RCCMD, según cuál sea la función deseada.

Al configurar en el apartado "Advertencias" se mandará un correo al usuario cuando el umbral se salga del valor límite.

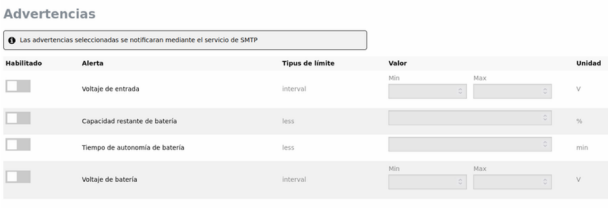


Fig. 37. Menú "Advertencias".

Al configurar en el apartado "Alarmas" se lanzará una orden de parada de servidores cuando el umbral se salga del valor límite. (ver RCCMD).

Fig. 38. Menú "Alarmas".

3.5.3. Medidas.

Muestra con más detalle las medidas del equipo que se habían presentado anteriormente en la pantalla de UPS monitor.

Se clasifican las medidas en función del bloque al que pertenecen.

3.5.3.1. Serie ADAPT-X y SLC ADAPT2.

Sólo para estas series es posible obtener medidas adicionales a las generales del equipo, disponiendo también del control de los módulos. Para cambiar entre medidas generales y de módulo, hacer uso del selector que se encuentra en la parte superior de la pantalla:

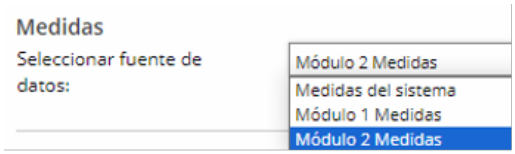


Fig. 39. Pantalla "Selector" de módulos.

3.5.4. Configuración.

Página de **lectura/escritura**. Permite modificar parámetros del equipo.

Nota: solo disponible para algunas series en específico. Revise la tabla adjunta para ver la compatibilidad de las distintas gamas.

Serie UPS	Opción de modificar parámetros
SLC CUBE3/3+	✓
SLC X-PERT	X
SLC X-TRA	X
SLC ADAPT-X	✓
SLC ADAPT2	✓
SLC CUBE4 30-80 kVA	✓
SLC CUBE4 7,5-20 kVA	X
SLC TWIN RT2	X
SLC TWIN PRO2	X
SLC TWIN PRO2	X
SLC TWIN PRO3	X
SLC TWIN RT3	X
Sistemas DC	
DC POWER-S	✓
DC POWER-L	✓
Estabilizador de tensión	
EMi3	✓

IMPORTANTE: En algunos equipos no es posible modificar determinados parámetros si no se reúnen las situaciones adecuadas. Refiérase a los apartados 3.5.3.x para más información.

Nota: Cuando se modifican varios parámetros a la vez es probable que el equipo no sea capaz de modificarlos todos. Es recomendable modificar un **máximo de 4 parámetros** en cada ocasión (ver *Fig. 40*).

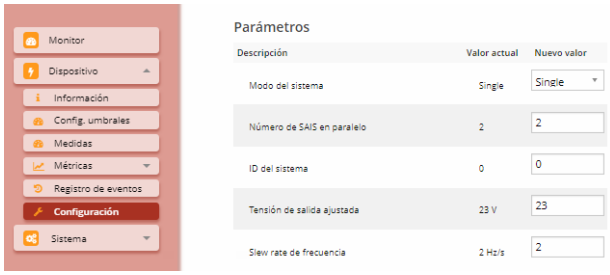


Fig. 40. Modificación de parámetros en Configuración.

3.5.4.1. Serie ADAPT-X.

El parámetro "Charger Module Charging Current Limit Value" sólo puede modificarse si se dispone de un módulo cargador conectado al SAI.

3.5.4.2. Serie CUBE3 / CUBE3+.

Para modificar todos los parámetros previamente es necesario transferir toda la carga del SAI a Bypass. Puede hacerse desde el panel, modificando el parámetro "Start/Stop Inverter" a "Stop" (ver *Fig. 41*).

Fig. 41. Parámetro Start/Stop.

Cuando se termine de modificar todos los parámetros devolver el SAI a su estado normal.

3.5.4.3. Serie DC-S.

No es posible modificar los parámetros relacionados con "Battery Management" si previamente no se ha habilitado la correspondiente funcionalidad (ver *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. Parámetros Battery Management.

3.5.5. Metrics.

Pulsar sobre "Metrics" para desplegar/ocultar los grupos de gráficas de las medidas del equipo.

Cada grupo de gráficas cuenta con una o más gráficas que permiten ver la evolución de las **últimas 24 horas** de la medida seleccionada, ver la imagen adjunta.

Si el equipo se encuentra conectado pero existe algún problema en la tarjeta NIMBUS, se mostrarán los últimos datos enviados con un intervalo de dos horas (ver *Fig. 43*), siempre que el equipo haya estado conectado, como mínimo, dicho tiempo. En caso de haber estado conectado menor tiempo se mostrarán las medidas del tiempo de conexión, siempre hasta un máximo de tres horas.

Para descargar un histórico de cada medida de forma individual en formato .csv hacer click en el botón "Exportar CSV" que se encuentra encima de cada gráfico. De esta forma, se exportarán los datos visualizados en la gráfica (últimas 24 horas).

Fig. 43. Evolución de los datos enviados cada tres horas.

3.5.6. Gestión de alarmas.

Para las series que disponen de validación de alarmas, es posible reconocerlas a distancia. Cuando una alarma esté activa y pueda visualizarse en la vista general del panel, aparecerá en esta sección como apta para ser reconocida. Para ello, haga clic en el botón "Validar" situado junto al nombre de la alarma que desea reconocer.

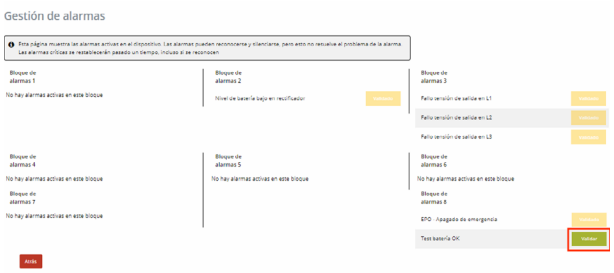


Fig. 44. Gestión de alarmas.

Una vez reconocida la alarma, esta seguirá siendo activa y por lo tanto seguirá visualizándose en el panel en color rojo. Una alarma reconocida a través de esta página no puede volverse a reconocer.

3.5.7. Actions.

Sólo para series SLC DC POWER-S es posible forzar acciones en el dispositivo, encontrándose actualmente solo disponible el test de baterías. Cuando internamente en el equipo dicha acción pueda ser lanzada, al lado de la propia acción se mostrará un botón para lanzarla. En caso contrario, como se muestra en la imagen, si la acción no se encontrara disponible aparecerá un botón bloqueado y no permitirá ser lanzada.

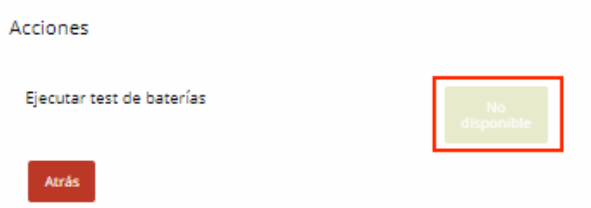


Fig. 45. Forzado de acciones.

3.5.8. Logs / Registro de eventos.

Para todas las series es posible descargar los históricos internos del equipo puede hacer uso de esta página.

3.5.8.1. Serie DC-S.

Sólo para series SLC DC POWER-S, será necesario realizar dos acciones.

Primero, generar el log haciendo clic en el botón "Start". Esta acción recuperará el histórico del equipo y lo mostrará por pantalla. Puede tardar unos minutos.

Fig. 46. Pantalla generación de Log.

Una vez generado el log, aparecerán por pantalla los históricos del equipo y una opción para descargarlos en formato .csv.

3.5.8.2. Resto de series.

Todos los eventos de alarma activados en el dispositivo se almacenarán en esta sección, hasta 500 eventos. Ir a "Dispositivo > Registro de eventos".

Fig. 47. Menú Dispositivo.

También es posible descargar el registro en formato .csv. Para hacerlo, haga clic en el botón superior derecho "Export CSV".

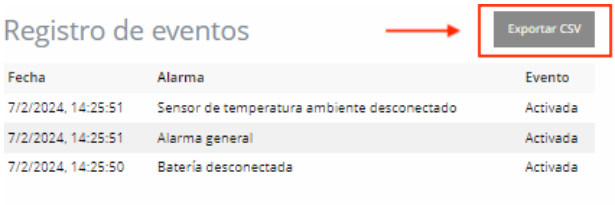


Fig. 48. Descarga en formato CSV.

3.5.9. Backup.

En caso de malfuncionamiento, sólo para las series DC power-S, es posible restaurar los valores de fábrica del equipo a través de esta página. Como primer paso, hacer clic en "Iniciar" al lado de "Ejecutar Backup" para recuperar los valores de fábrica. Cuando se disponga de dichos valores se activará el botón al lado de "Restaurar backup" para proceder a la aplicación. Si se desea restaurar los valores, hacer clic en el botón "Iniciar" en este punto.

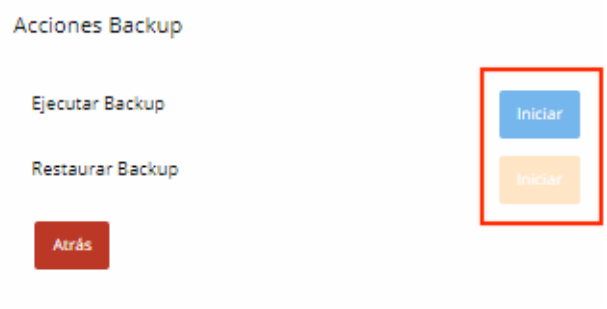


Fig. 49. Recuperación valores de fábrica..

3.5.10. Actions.

Solo para series TWIN PRO2, TWIN RT2, TWIN PRO3 y TWIN RT3 es posible ejecutar ciertas acciones sobre el dispositivo. Para ello, utilice los botones que encontrará al lado de cada acción.

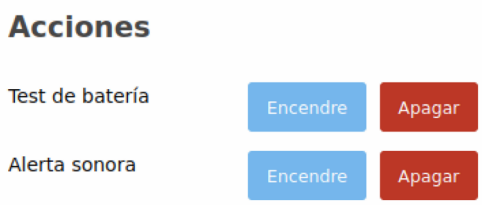


Fig. 50. Acciones sobre el dispositivo.

3.5.11. Logs de servicios.

Solamente para resolución de problemas.

Consultar y descargar los históricos de todos los servicios corriendo dentro de la tarjeta "Nimbus".

Hacer uso del desplegable para seleccionar qué servicio se quiere visualizar o recuperar los últimos registros del servicio. Después, hacer click en "Aplicar".

Fig. 51. Logs de Servicios.

Si se desea exportar el mismo registro visualizado en pantalla, hacer clic en "Exportar CSV" para obtener el mismo texto en formato .log para mandar al técnico, en caso de fallo detectado.

3.6. SYSTEM.

Disponible únicamente para usuarios Ingeniero. Pulsar sobre "System" para desplegar / ocultar las opciones descritas en este punto.

Fig. 52. Pantalla Sistema.

3.6.1. Network.

3.6.1.1. Establecer dirección IP.

La tarjeta NIMBUS cuenta con dos posibles modos de conexión remota mediante dirección IP (ir sección Ethernet).

3.6.1.1.1. Mediante DHCP.

En modo DHCP, la IP y otros parámetros de red son asignados por el servidor DHCP de su red, por lo que no se requerirá de configuracion manual para estos campos.

Para acceder a la tarjeta NIMBUS es preciso conocer la IP assignada por DHCP.

3.6.1.1.2. Mediante IP estática.

La dirección IP deberá ser establecida manualmente y se mantendrá fija hasta que se modifique.

Para modificarla, cambiar el contenido del campo IP. Los demás datos deberán ser modificados acorde a los parámetros de la red local de la instalación.

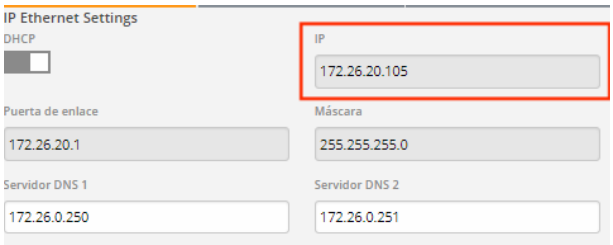


Fig. 53. Ajustes de Red.

No modificar la dirección IP de la tarjeta si se encuentra conectado al panel mediante esa dirección. Se perderá automáticamente su conexión.

También es posible modificar o añadir la dirección de servidores DNS. Se puede disponer de hasta dos servidores DNS.

Si está habilitada la configuración DHCP, estos campos se rellenaran automáticamente, aunque podrán ser manualmente modificados si es necesario.

3.6.1.2. Configuración de un servidor proxy.

Un servidor proxy actúa como un intermediario entre el dispositivo y los servidores en internet, mejorando la privacidad, el rendimiento y la seguridad de las conexiones.

Para configurarlo, activarlo desde la pestaña "proxy" (está deshabilitado por defecto) e introducir la configuración de proxy.

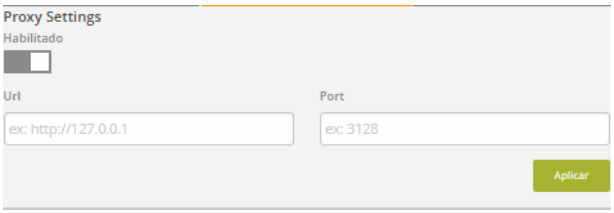


Fig. 54. Configuración de Proxy.

3.6.1.3. Test de conectividad.

Para asegurar que la conexión a los servidores básicos para el funcionamiento de la tarjeta NIMBUS están accesibles, utilizar el "Test de conectividad" que se encuentra en esta pestaña.

En él, se analizarán las principales direcciones en uso. Si todas las rutas se encuentran con color verde, significa que la NIMBUS está correctamente configurada para todos sus usos.

En caso que haya alguna ruta en rojo, podría significar que hay algún puerto no accesible o que se está vetando la entrada a la tarjeta.

Estado de la red	
Network (Internet access)	✓
DNS resolution	✓
NTP server	✗
HTTP:80 to portquiz.net	✓
HTTP:80 to archive.salicru.com	✓
SSH:22 to portquiz.net	✓
MQQT:1883 to portquiz.net	✓
MQQT:8883 to portquiz.net	✓
MQQT:8883 to mqtt.googleapis.com	✓
HTTPS:443 to portquiz.net	✓
HTTPS:443 to accounts.google.com	✓
HTTPS:443 to oauth2.googleapis.com	✓
HTTPS:443 to cloudiout.googleapis.com	✓
HTTPS:443 to www.googleapis.com	✓
HTTPS:443 to archive.salicru.com	✓

Fig. 55. Estado de la red.

Para una conexión off-grid, solamente será necesario tener acceso a:

- Network (internet access).
- DNS resolution.

En caso de requerir la opción de telemantenimiento, las demás rutas deberán también estar en verde. Sin ellas, no se podrá garantizar la conectividad mediante MQTT.

3.6.2. Date & Time.

Si se desea modificar el servidor NTP con el que cuenta la tarjeta, es posible hacerlo en esta sección.

Por defecto, se encuentra configurado con los servidores de pool.ntp.org.

3.6.3. Elección de sistema y reiniciar sistema.

La primera vez que la tarjeta NIMBUS es introducida en un equipo, esta detecta automáticamente en qué tipo de equipo se encuentra. También se puede usar la opción de deshabilitar esta opción, en caso que no se vaya a cambiar la targeta de equipo.

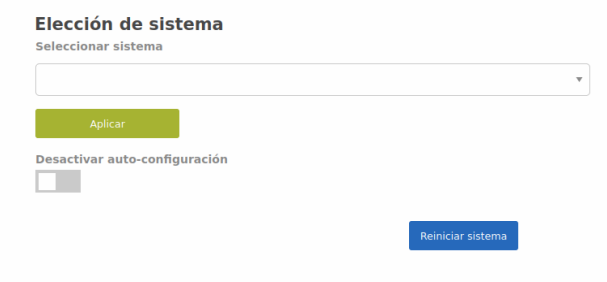


Fig. 56. Pantalla Elección de sistema.

Nota: No realizar cambios de modelo si la tarjeta NIMBUS no se ha introducido previamente en otro equipo. Después de cambiar de modelo es recomendable salir y volver a entrar al panel para visualizar correctamente los datos.

En caso que el sistema se quedara bloqueado o necesitara un reinicio de manera remota (sin necesidad de reiniciar manualmente la targeta) hacer uso del botón "Reiniciar sistema" para ejecutar esta tarea sin necesidad de desplazarse delante del equipo.

Tener en cuenta que reiniciar el sistema puede tardar de 3 a 5 minutos en volver a estar operativo.

3.6.4. Actualizar servicios.

Para actualizar la targeta de manera parcial (solamente unos paquetes) o total (todo el sistema), se cuenta con esta página solamente accesible con usuario con rol administrador.

Para empezar, hacer clic en "Comprobar actualizaciones" para que el sistema detecte si es capaz de realizar una nueva actualización o no. Este proceso puede tardar unos minutos.

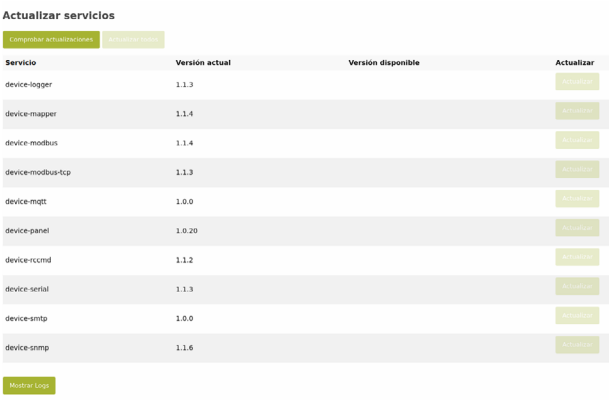


Fig. 57. Pantalla Actualizar Servicios.

Una vez ejecutado el comando, si existen actualizaciones, se mostrarán en "versión disponible". El botón "actualizar" correspondiente se activará para dar paso a la posible actualización.

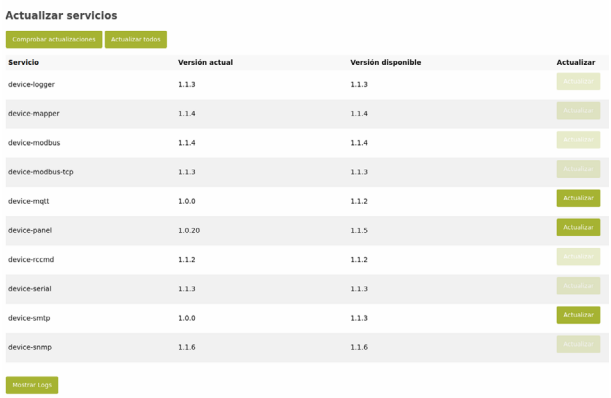


Fig. 58. Pantalla Actualizar Servicios con las versiones disponibles.

Para actualizar solamente un servicio de manera individual, hacer clic en el botón "actualizar" disponible al lado de cada servicio. Si se desea actualizar todos los servicios a la vez (recomendado) para tener la targeta a la última versión, hacer clic en el botón "actualizar todo" al inicio de la página.

Recordar que si decide actualizar los servicios de forma individual, se deberá hacer uno detrás de otro.

Para seguir el proceso de la actualización, hacer clic en "mostrar logs". Al final de la página se visualizarán los logs de la actualización en curso, de manera que se podrá ver el progreso en tiempo real.

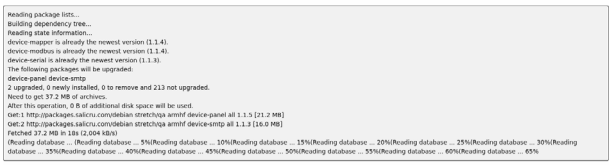


Fig. 59. Visualización de los logs.

3.6.5. Configuración de usuarios.

En caso de querer gestionar usuarios, dirigirse a esta página, donde se podrá visualizar una lista de usuarios ya creados y el rol establecido. NO se podrá ver ni recuperar contraseñas de los usuarios (ni del propio) por lo que se deben recordar las contraseñas cambiadas.

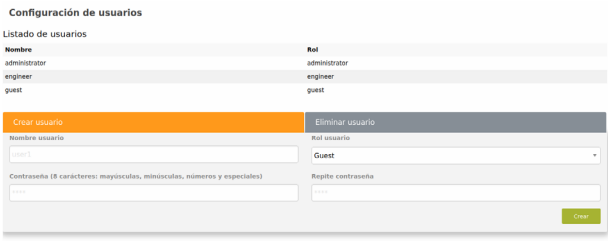


Fig. 60. Pantalla Configuración de usuarios.

Se dispone de dos secciones para modificar usuarios:

1. **Crear un usuario nuevo**: Para ello se necesitará introducir un nombre de usuario, el rol escogido para el usuario (administrador, ingeniero o usuario) y la contraseña. Recordar que la contraseña debe contener 8 caracteres entre ellos una mayúscula, una minúscula, un número y un carácter especial.

Fig. 61. Listado de usuarios.

Finalizado el proceso, hacer clic en "Crear" y le aparecerá el nuevo usuario creado en la lista.

2. **Eliminar un usuario ya existente**: Dirigirse a la segunda sección. Escoger un usuario para borrar de los disponibles en el formulario y hacer clic en "Eliminar".

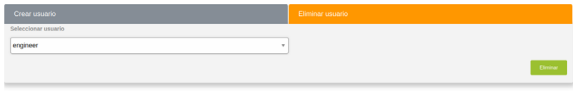


Fig. 62. Pantalla "Eliminar usuario".

Nota: No es posible borrar el propio usuario.

3.6.6. Cambiar contraseña.

Para modificar la contraseña del usuario con el que se ha iniciado sesión, introducir la contraseña actual y la nueva recordando que debe tener mínimo 8 caracteres incluyendo una mayúscula, una minúscula, un número y un carácter especial.

Fig. 63. Pantalla para el cambio de la contraseña.

3.6.7. Restablecer configuración.

En el caso de tener que actualizar el firmware del dispositivo, es muy recomendable hacer una copia de seguridad de la configuración previamente configurada en la tarjeta.

Para ello, hacer click en "Backup de configuración". Se generará un archivo que contendrá toda la configuración.

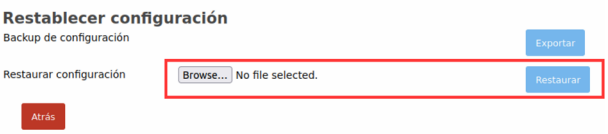


Fig. 64. Restablecer configuración.

Una vez actualizado el firmware, acceder de nuevo al panel con el usuario "ingeniero" y hacer click en "Examinar…" dentro de "Restaurar configuración". Cargar el archivo previamente generado y hacer click en "Restaurar". Esta acción puede tardar unos minutos.

3.7. SERVICIOS.

Disponible **únicamente para usuarios ingeniero/ administrador.** Pulsar sobre Servicios para desplegar/ocultar las opciones descritas en este punto.

Fig. 65. Pantalla Servicios.

3.7.1. RCCMD.

Para hacer efectiva esta pantalla, relacionada con un servicio opcional de la tarjeta, primero referirse al apartado **4. Instalación del software de RCCMD**.

Dispone de hasta 5 direcciones de IP configurables de manera individual con todas las posibilidades de alarmas disponibles. Para empezar, seleccionar un posible hueco en el que guardar la configuración haciendo uso del selector desplegable "seleccione una configuración".

Fig. 66. Pantalla Parámetros RCCMD.

Los huecos en los que ya se encuentre una IP configurada, aparecen con dicha dirección IP. Los demás, si se encuentran libres, contendrán el nombre de "Añadir nueva configuración". Se pueden configurar hasta 5 direcciones, pero no es necesario configurarlas todas.

Una vez seleccionado el hueco en el que guardar la configuración, proceder a configurar las alarmas. Existe una página como esta para cada configuración.

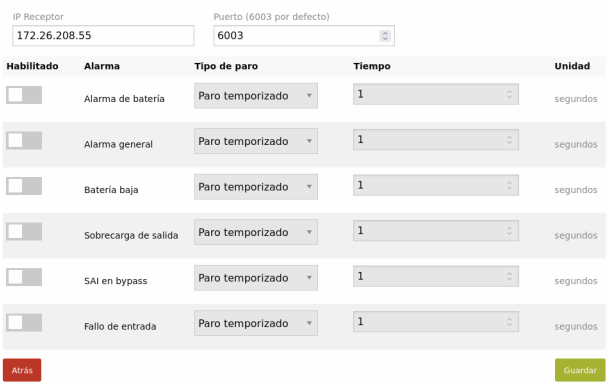


Fig. 67. Pantalla Configuración de las alarmas.

Detallar aquí la dirección IP del servidor de destino. En el caso que se desee una difusión amplia, introduzcir la IP de dicha difusión. Añadir también el puerto del cliente RCCMD, de acorde a lo establecido y explicado en el punto **4.2.2. Puerto del emisor**.

Para cada uno de los posibles grupos de alarmas, activar o desactivar la funcionalidad desplazando el botón. Solamente cuando un grupo esté activo, se podrá operar tanto sobre el tipo de apagado como con el tiempo establecido.

Cuenta con dos tipos de paro:

- **Retardado**: se asignará un rango de tiempo después del cual, si se cumple la condición, se procederá a realizar la parada remota.
- **Inmediato**: no cuenta con un temporizador, cuando se detecte la condición como activa se procederá a la parada remota.

Cuando se haya terminado de efectuar los cambios, recuerdar guardarlos mediante el botón "Guardar" abajo de la página.

Si se desea probar su configuración sin necesidad de parar ningún servidor, se puede hacer uso del botón "Test" arriba de la página. Hacer clic en este botón provocará el envío de un mensaje de LOG a su IP configurada. Asegurar que se recibe correctamente antes de dar por finalizada la instalación y puesta a punto del servicio.

3.7.2. Modbus.

Nota: en las series SLC CUBE4 7,5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2 y SLC TWIN RT2 no es posible modificar los parámetros de configuración de comunicaciones.

Modificar la dirección modbus del Slave al que se conecta la NIMBUS para leer información, así como los parámetros del protocolo para establecer conexión con el equipo. Por defecto, estos valores ya permitirán la correcta comunicación con el equipo.

Consultar la configuración del equipo para saber en qué direcciones y parámetros de configuración se encuentra disponible la información en caso de modificación.

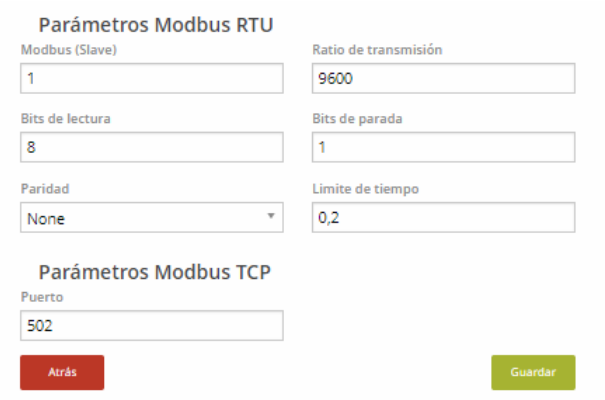


Fig. 68. Ajustes del Modbus.

Nota: Después de un cambio de dirección es recomendable reiniciar el panel y esperar unos minutos. No realizar un reinicio de la tarjeta NIMBUS ya que los nuevos valores introducidos se perderán.

Importante: Unos valores no válidos supondrán pérdida de comunicación con el equipo. Antes de modificarlos asegurar que el panel no se encuentra recibiendo datos y que conoce los valores correctos establecidos en el equipo. No modificar estos valores si el panel se encuentra recibiendo datos.

3.7.2.1. Modbus TCP.

Si se cuenta con el servidor modbus TCP activo es posible modificar el puerto en el que se encuentra disponible el servicio en esta misma sección.

Nota: el servidor TCP se encuentra disponible para todas las series, incluídas aquellas que no disponen de parámetros de configuración modbus como SLC CUBE4 7,5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2 y SLC TWIN RT2 .

3.7.3. SNMP.

Sólo si se ha contratado el **servicio opcional** SNMP se podrá visualizar esta página.

La tarjeta nimbus implementa protocolo SNMP v3 que cuenta con mejores prestaciones de seguridad en cuanto al cifrado de mensajes y acceso a ellos. Para hacer uso del servicio, es necesario establecer un nombre de usuario y contraseña con el que leer los mensajes.

Nota: SNMP v1 y SNMP v2 pueden ser activados a través de deshabilitar la versión v3 a través del selector correspondiente de la pestaña SNMP.

- Configuración V3.

  Para la configuración inicial, crear el "nombre de usuario" y la "contraseña" con la que se establecerá la conexión. Para ello, introduzcir los valores en la sección "Parámetros SNMP".

  El usuario "salicru" no está permitido.

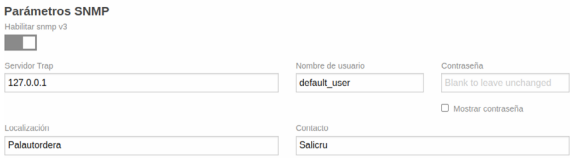


Fig. 69. Configuración inicial.

- Configuración V2.

  Deshabilitar el selector de “habilitar snmp v3”. Introducir el valor de “community” con el que comunicar el equipo. Por defecto este valor no existe, por lo que es imprescindible asignarle un valor inicial para poder prodecer a la lectura.

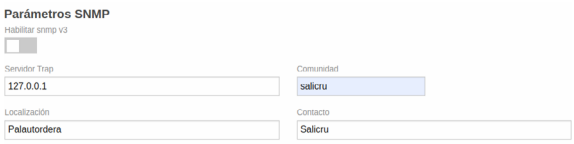


Fig. 70. Deshabilitación SNMP V3.

Si desea configurar el servidor trap en el ordenador en el que recibir las notificaciones en caso de cambio de estado, alarma y/o advertencia, introducirlo en “servidor trap”. La autenticación será la misma que para leer mensajes.

Para conocer la direcció IP del ordenador, abrir el buscador del sistema y teclear "cmd". Ejecutar el programa. Escribir ipconfig en el terminal y buscar la dirección inet.

Guardar los cambios después de realizarlos mediante el botón “guardar”.

Nota: Será necesario tener instalado algún programa que permita recibir y gestionar los "Trap" generados por el equipo.

Para comprobar que el servidor trap ha sido configurado correctamente, se puede hacer uso de la sección de abajo “test”.

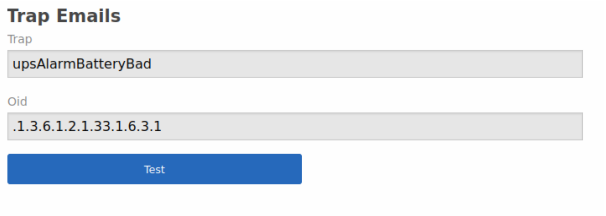


Fig. 71. Test configuración servidor trap.

3.7.4. Servidor SMTP.

Configurar el servidor SMTP con el fin de recibir correos cuando se active una alarma y/o salte un umbral predefinido (ver apartado "3.5.2. Threshold Settings." en la página 16).

Es imprescindible utilizar un servidor que permita usar nombre de usuario y contraseña. Si no se especifican, el servicio no estará correctamente configurado.

Algunas posibles configuraciones para el servidor:

- Office 365:

Host	smtp.office365.com
Puerto	587 (recomendado) o puerto 25
Correo remitente	el correo
Nombre de usuario y contraseña	las credenciales para el correo establecido arriba en “correo remitente”

- Outlook:

Host	smtp-mail.outlook.com
Puerto	587 (recomendado) o puerto 25
Correo remitente	el correo
Nombre de usuario y contraseña	las credenciales para el correo establecido arriba en “correo remitente”

Fig. 72. Configuración del servidor SMTP.

Importante: Si no se guarda la configuración explícitamente haciendo clic en el botón “Guardar” esta no se modificará. Antes de lanzar cualquier acción, asegurar de haber realizado estos cambios correctamente.

Para comprobar que la configuración es correcta y que se recibirán los correos, hacer uso del botón “Test”. Recuerdar que se deberá guardar primero la configuración.

En la segunda parte de la pantalla es posible configurar el email en función de qué desee que se notifique. Habilitar las alarmas de las que se desee recibir notificaciones. Se dispone de distintas opciones de envío, entre ellas:

- **Inmediatamente**: la alarma se notificará en el correo electrónico en el mismo momento de ser activada. No requiere tiempo.
- **Después de unos minutos**: el correo se mandará ciertos minutos (establezca un valor) después que la alarma haya sido activada. Es una función en la que se ve la notificación de alarma en diferido.
- **Frecuencia de minutos**: una vez activada la alarma, esta se notificará cada x minutos (valor establecido por el usuario). Dejará de notificarse de forma repetida cuando se desactive.
- **Después de unos minutos en batería**: una alarma activa solo se notificará siempre y cuando el equipo también se encuentre en batería y hayan pasado los minutos predefinidos por el usuario.
- **Cierto tiempo de autonomía**: una alarma activa solo se notificará cuando el equipo esté en batería y el valor límite del tiempo de autonomía esté por debajo de lo establecido por el usuario.

Nota: para recibir mensajes siempre se deberá tener mínimo 1 email de destino. Se puede configurar en la sección “Personaliza el email”.

3.7.5. IEC-61850.

Se puede exportar el archivo .icd para cargarlo en el programa de visualización a través de esta página.

Si se desea modificar cualquiera de los siguientes valores para ser distintos de la IP en la que se encuentra configurado el equipo:

- IP
- Máscara de subred
- Gateway

se pueden fijar estos valores de manera individual.

Fig. 73. Ajustes IEC-61850.

En caso contrario, activar la opción de "automático" para cargar automáticamente la configuración. Guardar los cambios antes de exportar el archivo.

3.8. LOGOUT.

Pulsar este botón de la derecha en la barra superior cuando se desee dejar de consultar el panel del equipo o bien se prefiera acceder a él con una cuenta de acceso distinta.

4. INSTALACIÓN DEL SOFTWARE DE RCCMD.

RCCMD (Remote Control Command) es una aplicación que permite realizar el apagado simultáneo y seguro de distintos servidores de forma remota, según ciertas condiciones especificadas por el usuario. Para configurar estas condiciones referirse al apartado "3.6.4 RCCMD".

Para que este servicio funcione, es indispensable contar con dos partes: un receptor y un emisor. La tarjeta NIMBUS siempre funcionará como emisor ya que será capaz de detectar las condiciones de apagado establecidas. Por otro lado, el receptor podrá ser uno o varios servidores, dependiendo de si se fija una IP única apuntando a un solo servidor o por contra se fija una IP de difusión amplia.

En cuanto al emisor, este ya vendrá configurado de fábrica para que no se deban instalar nuevos paquetes para su correcta utilización. Sin embargo para cada receptor que quiera beneficiarse de este servicio se deberá instalar un software específico que se detalla a continuación.

4.1. INSTALACIÓN DEL PAQUETE.

Abrir un navegador web y acceder a la página de https://www.generex.de/. Desde ahí, entrar a la pestaña "Download" y confirmar que bajo el apartado "Software" existe la sección referente a "RCCMD". A continuación pulsar sobre el botón "Software".

Fig. 74. Pantalla principal Generex.

Aparecerá una nueva pantalla como la que se muestra a continuación con todos los posibles descargables. Seleccionar la opción de "RCCMD".

Fig. 75. Detalle descarga software RCCMD.

Dentro de la sección "RCCMD" se mostrará una lista de posibles plataforma con los que dicho software es compatible. Escoger uno u otro en función de las necesidades y, de nuevo, seleccionar la opción a descargar a través del botón de dicha sección.

4.1.1. Windows.

Si se ha seleccionado este sistema operativo, se mostrará una lista con todas las empresas y su propio software específico. Buscar la opción de "SALICRU", tal como se muestra en la imagen:

Fig. 76. Opción descarga SALICRU.

Pulsar el botón indicado en la imagen para efectuar la descarga.

Descomprimir la carpeta descargada en el lugar que desee y ejecutar el archivo "installRCCMD.exe".

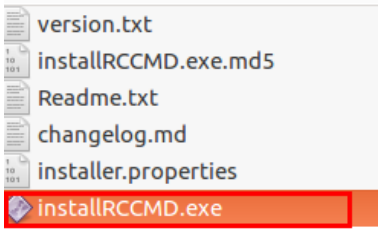


Fig. 77. Binario de ejecución de RCCMD.

Se abrirán dos carpetas, entrar en la carpeta "Windows".

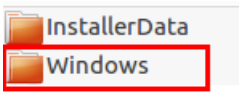


Fig. 78. Carpeta Windows dentro de la carpeta descomprimida.

Finalmente, ejecutar de nuevo el archivo "installRCCMD. exe".

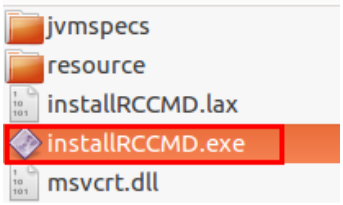


Fig. 79. Binario de execución RCCMD dentro de la carpeta Windows.

Seguir los pasos del instalador y no modificar los parámetros básicos definidos. En algún momento de la instalación se pedirá introducir un código de licencia que será facilitado por SALICRU.

4.1.2. Unix y Linux.

Si se ha seleccionado uno de estos dos sistemas operativos, se precisará un código de licencia que será facilitado por SALICRU.

Hecho esto y definido el tipo de sistema operativo usado, pulsar el botón "Create package..." para crear el paquete y efectuar la descarga.

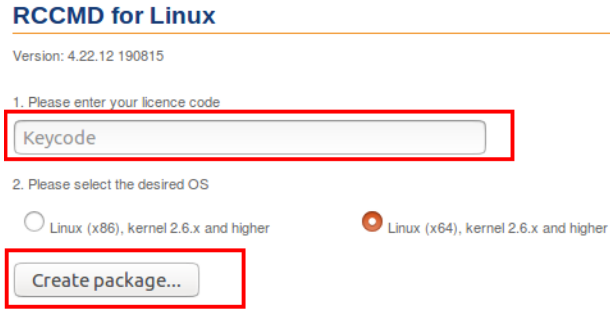


Fig. 80. Pantalla RCCMD para Linux.

Descomprimir la carpeta descargada en el lugar que se desee y ejecutar el archivo "installRCCMD.bin".

Seguir los pasos del instalador y no modificar los parámetros básicos definidos. En cierto punto de la instalación se precisará introducir el mismo código de licencia que se ha usado anteriormente para crear el paquete descargado de licencia que será facilitado por SALICRU.

4.1.3. MacOS.

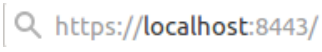
Si ha seleccionado este sistema operativo, se necesitará un código de licencia que será facilitado por SALICRU.

Hecho esto y definido el tipo de sistema operativo usado, pulsar el botón "Create package..." para crear el paquete y efectuar la descarga.

Fig. 81. Pantalla RCCMD para MacOSX.

4.2. CONFIGURACIÓN DEL SOFTWARE.

Descargado e instalado el software de RCCMD siguiendo los pasos anteriores, ahora es posible configurarlo. Para ello abrir una ventana de cualquier navegador y entrar la siguiente dirección:



Se deberá mostrar una página como la siguiente:

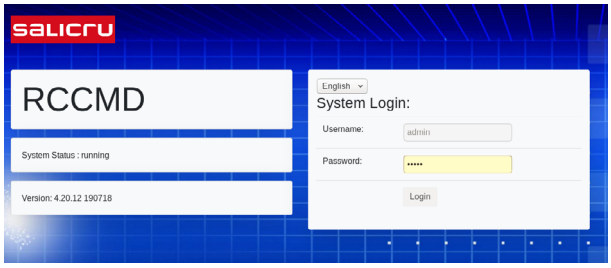


Fig. 82. Pantalla principal RCCMD.

En la sección de "System Login", introducir las credenciales facilitadas por SALICRU y pulsar el botón "Login" *(Fig. 82)*.

La página por defecto mostrará el estado de RCCMD (activo, apagado) y ofrecerá opciones para activarlo, apagarlo o reiniciarlo, tal como muestra la siguiente *Fig. 83*.

Después de modificar algún parámetro es recomendable utilizar la opción de "Restart" para que dicho cambio se ejecute correctamente.

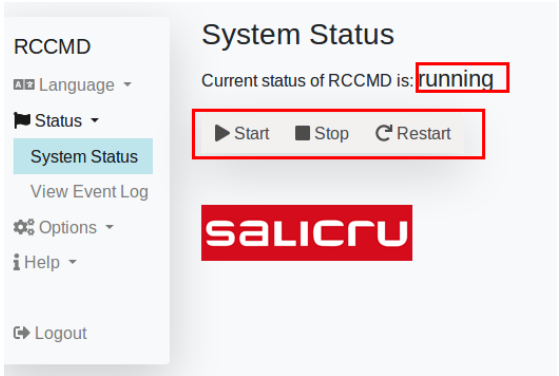


Fig. 83. RCCMD: Estado del sistema.

Si RCCMD está apagado en el servidor de destino, la tarjeta NIMBUS no será capaz de transmitirle la información necesaria para su correcto uso.

4.2.1. IP del emisor.

Para emparejar un cierto dispositivo con la tarjeta NIMBUS y que ambos se escuchen, es necesario ir al apartado "Options" y acceder al subapartado "Connections" en la barra de navegación vertical izquierda tal como se muestra en la *Fig. 84*.

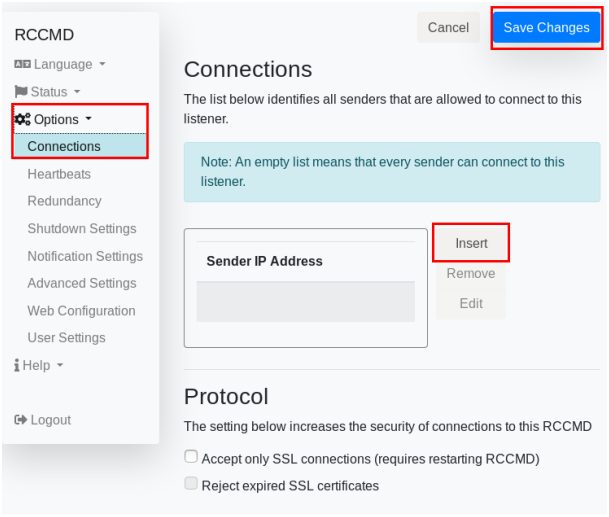


Fig. 84. Pantalla de emparejamiento con la tarjeta NIMBUS.

Si el campo "Sender IP Address" se deja vacío, el servidor aún será capaz de escuchar y, por lo tanto, acatará todas las órdenes de parada que reciba de distintas NIMBUS si en éstas se ha configurado correctamente la IP de destino hacia este servidor. Es decir, aunque no se configure la IP del emisor (tarjeta NIMBUS), el servidor puede recibir acciones si el estado de RCCMD es activado. Aún así, es recomendable emparejar el dispositivo con la tarjeta NIMBUS para mayor seguridad.

Para insertar una IP, pulsar el botón "Insert" señalado en la imagen. Se le abrirá una ventana emergente como se muestra en la *Fig. 85*.

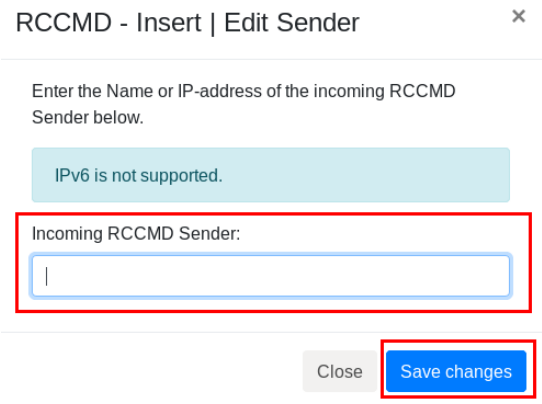


Fig. 85. Pantalla inserción IP.

Introducir la IP de la tarjeta NIMBUS a la que se quiera asociar el dispositivo en el campo habilitado para ello. Guardar los cambios a través de "Save changes".

En la pantalla principal, guardar de nuevo los cambios mediante el botón "Save changes".

Importante: Si ya no se desea que el servidor haga uso de RCCMD, desactivar el servicio (verificar que su estado se encuentre en "not running") y no únicamente limitarse a borrar el campo de "Sender IP Address", ya que ocasionalmente podría recibir alguna orden.

4.2.2. Puerto del emisor.

Este paso no es necesario ya que por defecto el software de RCCMD viene configurado en el puerto 6003.

Si se considera oportuno cambiar el puerto, dirigirse al subapartado "Advanced Settings" dentro de "Options" en la barra de navegación vertical izquierda tal como se muestra en la *Fig. 86*.

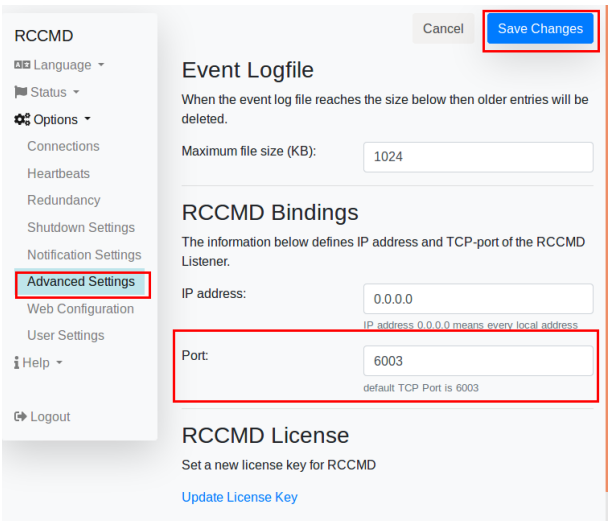


Fig. 86. Pantalla ajustes avanzados.

Modificar el puerto en el que se desea que RCCMD escuche a través de modificar el campo "Port". Para finalizar, guardar los cambios pulsando "Save Changes".

5. ACTIVACIÓN DE SERVICIOS CONTRATADOS.

Si se ha adquirido un servicio extra con la contratación de su tarjeta de comunicaciones NIMBUS, es preciso activarlo mediante el panel web embebida. Para ello, seguir los siguientes pasos:

1. Conectarse al panel web. Referirse al apartado "3.1 Acceso al panel" para más información.
2. Hacer clic en el link "Activar servicio", debajo del botón de login como se muestra en la siguiente figura.

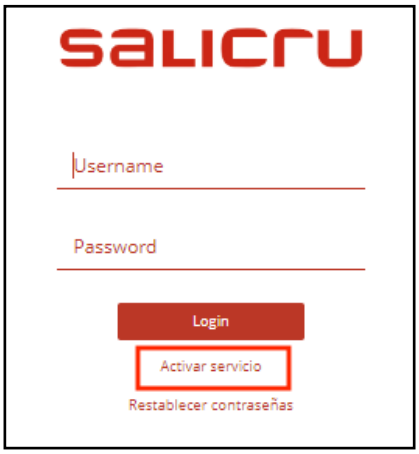


Fig. 87. Activar servicio.

3. Una vez activado el servicio, estará instalado y disponible en su tarjeta en unos 5 minutos.

   Los paquetes opcionales que pueden contratarse en la tarjeta de comunicaciones NIMBUS son los que se citan a continuación:

Servicio	Descripción
Modbus TCP	Protocolo de comunicación secundario derivado de MODBUS (protocolo de comunicación principal).
Modbus API-REST	Habilitando la conexión externa de la tarjeta es posible efectuar llamadas a los sevicios de comunicación sin necesidad de acceder al interior de la tarjeta.
RCCMD (*)	Servicio que permite realizar una parada controlada de servidores en caso de cumplirse ciertas condiciones en el equipo.
SNMP	Protocolo de comunicación secundario. Permite recibir notificaciones a la IP del usuario cuando se activa una alarma.
IEC 61850	Protocolo de comunicación secundario. Permite recibir MMS.

(*) El servicio RCCMD no debe activarse mediante código en la tarjeta de comunicaciones NIMBUS, sino que deberá activarse mediante descarga del cliente de RCCMD. Para más información, referirse al apartado "4. Instalación del software de RCCMD".

Tab. 6. Paquetes opcionales.

6. ANEXO I. CONECTIVIDAD.

En algunos equipos de SALICRU, los datos que se muestra en la web embarcada también pueden ser subidos a la plataforma web de SALICRU. En esta plataforma el usuario tiene la posibilidad de visualizar el estado del equipo sin necesidad de estar en la misma red, así como actualizar de forma remota las tarjetas, visualizar la localización del equipo y personalizar notificaciones vía SMS y correo electrónico en caso de alarma.

En las series SLC ADAPT2 y SLC CUBE4, se podrá saber si el equipo está conectado y enviando datos a la nube buscando en la parte superior derecha de la pantalla 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.

6.1. REQUERIMIENTOS DE FIREWALL PARA CONECTIVIDAD.

6.1.1. 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.

6.1.2. 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.

Hostmane	Puerto
europe-west1-g5-mqtt.clearblade.com	443 y 8883
europe-west1.clearblade.com	443

Tab. 7. Relación de IPs / puertos para la correcta conexión al panel de telemantenimiento.

6.2. SERIES SLC TWIN PRO3 Y SLC TWIN RT3.

Estas series de UPS permiten la conectividad integrada del dispositivo sin necesidad de utilizar la tarjeta Nimbus. Esta conectividad integrada puede conseguirse mediante una conexión por Ethernet o por WiFi, en cuyo último caso se necesitará un dispositivo capaz de captar la señal WiFi.

6.2.1. Conectividad integrada mediante Ethernet.

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

Revisar los requisitos del firewall para usar la actualización de firmware OTA. 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 pool.ntp.org; de lo contrario, modificar el servidor NTP para que IoT obtenga la marca de tiempo correcta.

6.2.2. 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 empieza a parpadear a una frecuencia más elevada, indicativo de que ha cambiado de estado a modo "Access point (AP)".

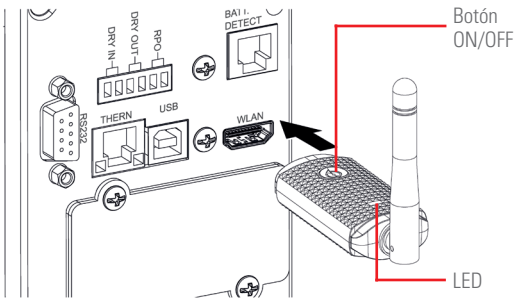
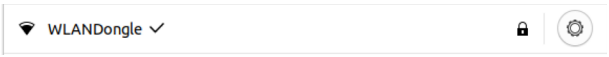


Fig. 88. Conexión del dispositivo WiFi.

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



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

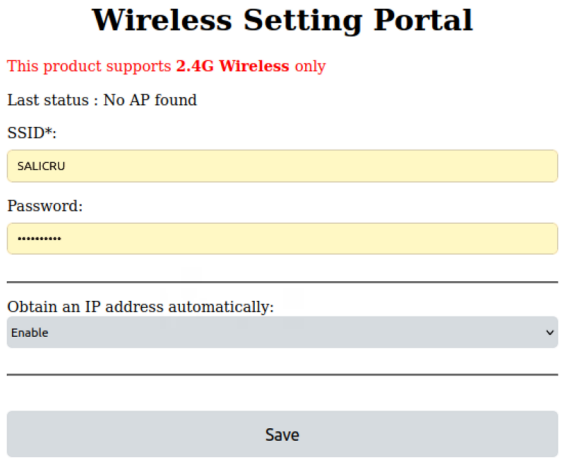


Fig. 89. Porta de configuración WiFi.

Es posible que se tenga que hacer clic en la opción "Avanzado > Continuar en sitio no seguro" la primera vez que se entra en la página web.

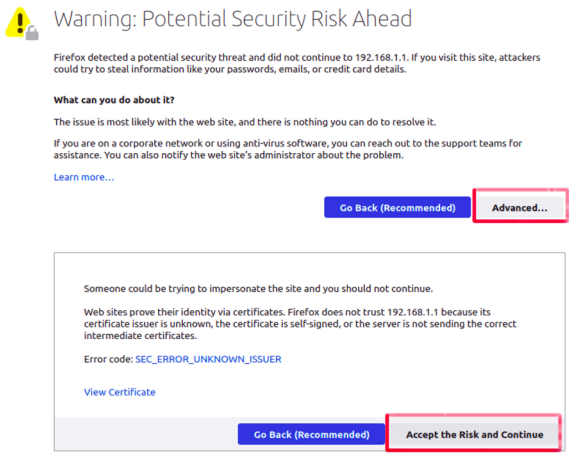


Fig. 90. Pantallas de aviso de Riesgos Potenciales.

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

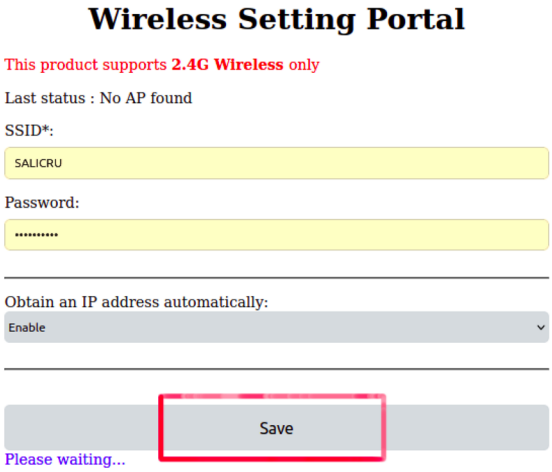


Fig. 91. Pantalla guardar cambios.

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 carácteres especiales no están soportados.
- Las redes WLAN públicas que requieran de una segunda autentificación no están soportadas.
- Los WiFi routers de 5GB no están soportados.
- Las redes WLAN que necesiten habilitar funciones especiales como "MAC whitelist" requerirán ese paso adicional.

6. Finalmente, asegurar de 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 registre su dispositivo.

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.	Revise la conexión entre el dispositivo y el UPS.
LED parpadea lentamente (1 flash/ segundo)	El dispositivo no está conectado al router.	Revisar los requermientos 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 dispositvo está en modo Configuración.	Conectar a http://192.168.1.1 para establecer la conexión con el router.
LED encendido	La conexión al router se ha realizado correctamente.	-

Tab. 8. Estados de los LED y acciones a emprender.

6.3. USO Y ACCESO AL PORTAL DE TELEMANTENIMIENTO.

6.3.1. Creación de cuenta.

Para hacer uso de este sistema opcional, siga los siguientes pasos:

1. Dirigirse al siguiente enlace: https://nimbus.salicru.com/.
2. Crear una cuenta (si no se dispone de una), mediante el enlace "Crear una cuenta" que se muestra en la imagen.

Fig. 92. Pantalla principal de login del panel de telemantenimiento.

3. Rellenar el formulario con datos correctos. Se deberán aceptar los "Términos y condiciones".

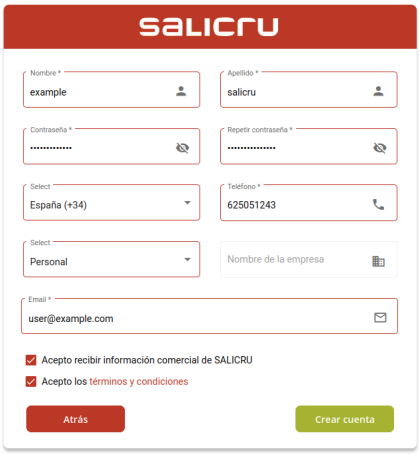


Fig. 93. Pantalla de registro de usuario.

Contraseña con mínimo 8 caracteres de los cuales debe haber: una letra en minúscula, una en mayúscula, un número y un símbolo e.g. #MiContraseñaParaNimbus2020

Para continuar, debe leer y estar de acuerdo con los términos y condiciones expuestos haciendo clic en la casilla.

4. Una vez creada la cuenta, dirigirse a la bandeja de entrada del correo introducido en el registro. En pocos minutos se recibirá un correo de confirmación de la cuenta.

Tener en cuenta que este mensaje tiene caducidad. Debe usarse en los 15 minutos posteriores a recibirse.

5. Hacer clic en el enlace enviado en el correo, de esta forma el usuario se activará y se tendrá acceso al portal de telemantenimiento.

6.3.2. Registro del equipo en la nube.

Se dispone de dos formas para registrar el equipo en la nube:

- Directamente desde el portal de telemantenimiento (no recomendable para usuarios).
- Mediante lectura del código QR que se encuentra en el frontal del equipo.

6.3.2.1. Registro manual mediante el portal de telemantenimiento.

1. Iniciar sesión en el portal con una cuenta previamente validada.
2. En la pantalla principal de la aplicación "Dispositivos" hacer click en el botón "+ añadir nuevo dispositivo", ubicado en la esquina superior derecha.
3. Cumplimentar el formulario para la creación del dispositivo con la información del equipo.

Los campos obligatorios están marcados con un asterisco (*). Los campos de NÚMERO DE SERIE, UUID y MODELO son datos básicos e identificativos del producto. Se puede encontrar esta información en la etiqueta de identificación del equipo.

Es conveniente proporcionar una descripción clara y concisa para identificar producto, ya que si se dispone de más equipos SALICRU registrados, es posible diferenciarlos fácilmente mediante este campo.

La zona horaria donde se halla el dispositivo, así como su localización son campos obligatorios. Para ubicar el equipo se puede, o bien buscar su dirección mediante la opción Search location, que abrirá un mapa interactivo, o proporcionar manualmente una dirección y coordenadas.

4. Pulsar en GUARDAR para completar el registro.

   Si hay algún error en la creación del dispositivo, se notificará en pantalla. Contactar con el servicio técnico en caso de dudas.

5. Una vez el equipo se haya creado correctamente, se mostrará en la lista de dispositivos en la página "Dispositivos".

6.3.2.2. Registro automático mediante escaneado de código QR.

1. Escanear el código QR que se encuentra situado en la parte frontal del equipo. La mayoría de dispositivos móviles disponen de serie de herramientas de escáner QR, si no es el caso, instalar uno mediante el App store.

   A continuación, se abrirá la página de registro en el navegador del dispositivo móvil.

   Iniciar sesión para registrar el dispositivo. Si no se dispone aún de una cuenta registrada en SALICRU, crear una mediante el enlace "Crear cuenta".

2. Rellenar los datos en blanco del formulario. Los datos básicos del equipo ya vendrán prefijados y no podrán modificarse.

Es conveniente proporcionar una descripción clara y concisa para identificar producto, ya que si se dispone de más equipos SALICRU registrados, se podrán diferenciar fácilmente mediante este campo.

La zona horaria donde se halla el dispositivo, así como su localización son campos obligatorios. Para ubicar el equipo, o bien buscar su dirección mediante la opción Search location, que abrirá un mapa interactivo, o proporcionar manualmente una dirección y coordenadas.

3. Pulsar GUARDAR para completar el registro.

   Si hay algún error en la creación del dispositivo, se notificará en pantalla. Contactar con el servicio técnico en caso de dudas.

4. Una vez el equipo se haya creado correctamente, se mostrará en la lista de dispositivos en la página "Dispositivos".

6.3.3. Creación de notificaciones asociadas a un dispositivo.

Después de haber registrado un dispositivo de forma satisfactoria, es posible configurar sus notificaciones de alarma. Para ello, dirigirse al apartado "Notificaciones" en la barra vertical de navegación.

Asegurarse de haber dado de alta primero un dispositivo, sino no se podrá asociar ninguna notificación al usuario.

Para crear una nueva notificación, presionar el botón "+ añadir nueva notificación". Se abrirá un formulario para la creación de la nueva notificación.

Importante: Cada usuario solamente puede configurar una notificación por cada equipo. Aún así, pueden asociarse cuentas de correo y teléfonos para que más de una persona pueda recibir la misma notificación.

Dentro del formulario de creación, seleccionar el dispositivo para el cual se desee crear una notificación mediante el desplegable de "Dispositivo". Una vez seleccionado se mostrarán los posibles grupos de alarmas disponibles. Seleccionar uno o varios, en función de los requerimientos.

Por último, seleccionar el tipo de notificación deseado en la sección de "Notificaciones habilitadas". Se dispone de tres tipos: web, correo electrónico y SMS. Si no se selecciona ninguno, no se mostrarán notificaciones de alarma de ningún tipo y se deberá ir directamente al detalle del dispositivo para controlar su estado.

6.3.3.1. Notificaciones web.

Con estas notificaciones habilitadas, se mostrará un mensaje emergente en la propia web cuando se dé una alarma. Tener en cuenta que estas notificaciones solamente se visualizarán si el usuario tiene abierta sesión y está navegando por la web de telemantenimiento.

6.3.3.2. Notificaciones e-mail.

Este tipo de notificaciones permitirán recibir un correo cada vez que se habilite una alarma. El correo por defecto de la notificación se asociará directamente al usuario creador, dicho correo se puede visualizar en la misma página (campo no editable). Para cambiar el correo por defecto, acceder al perfil de usuario.

Es posible añadir correos extra en una misma notificación. Pulsar el botón "Añadir e-mail" y escribir una dirección adicional.

Fig. 94. Añadir e-mail extra.

Tener en cuenta que la notificación ahora se mandará al correo por defecto y todos los demás correos asociados.

6.3.3.3. Notificaciones SMS.

Mediante esta notificación se recibirá un mensaje SMS en el teléfono móvil cada vez que se active una alarma. Igual que con los correos, el número de teléfono por defecto se asociará directamente al usuario creador como campo no editable. Para modificar el teléfono, acceder al perfil de usuario.

También es posible añadir números de teléfono adicionales. Pulsar el botón "Añadir teléfono" y entrar el teléfono. Tener en cuenta que la notificación ahora se mandará al teléfono por defecto y todos los demás teléfonos asociados.

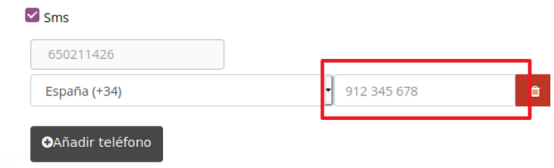


Fig. 95. Añadir número de teléfono extra.

6.3.4. Recuperación de contraseña.

Si no se recuerda la clave de acceso, es posible restablecerla haciendo clic en Restablecer contraseña en la misma pantalla de Login.

El proceso requerirá introducir el correo electrónico asociado a la cuenta. Pulsar Enviar para seguir con el proceso.

Fig. 96. Página para recuperación de contraseña perdida.

Se recibirá en el correo electrónico un mensaje para reestablecer la contraseña. Recordar comprobar la bandeja de Spam si no aparece en la bandeja de entrada.

Fig. 97. Restablecer contraseña.

Accediendo al enlace proporcionado en el correo, se podrá crear la nueva contraseña. Pulsar **Guardar** para almacenar el cambio.

Fig. 98. Guardar cambios.

7. ANEXO II. PROCEDIMIENTO DE ACTUALIZACIÓN DE TARJETAS.

7.1. MATERIAL NECESARIO.

- Tarjeta MicroSD de 8 GB o superior.
- Adaptador SD o bien MicroSD y periférico en el ordenador para leer tarjetas SD.
- Software Balena Etcher (balenaEtcher - Flash OS images to SD cards & USB drives), Win 32 disk Imager (https://sourceforge.net/projects/win32diskimager/files/latest/download) o similar.

7.2. REALIZAR UN BACKUP DE LA CONFIGURACIÓN DE LA TARJETA.

1. Conectarse al panel embedded de la tarjeta con el usuario "engineer".
2. Desplegar la sección "Sistema" y seleccionar la última pestaña "Restablecer conf."

Fig. 99. Restablecer configuración.

3. Hacer clic en el botón "Exportar" para descargar la configuración actual de la tarjeta. Esto incluye configuraciones de red (se mantendrá la IP), así como de servicios (configuraciones de thresholds, alarmas, servidor SNMP, RCCMD, Modbus, ...).

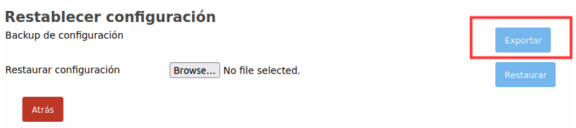


Fig. 100. Exportar en Restablecer configuración.

4. Guardar el documento para utiltizarlo después de la actualización.

7.3. PROCEDIMIENTO DE ACTUALIZACIÓN.

1. Descargar la última versión de firmware.
2. Conectar el Adaptador SD o bien directamente la tarjeta MicroSD al ordenador. Esperar a recibir la confirmación que se ha leído correctamente la tarjeta.
3. Abrir el programa descargado para flashear el firmware a la tarjeta.
4. Cargar el firmware en el programa y empezar a quemarlo en la tarjeta. El procedimiento puede tardar unos minutos.
5. Una vez finalizado, extraer con cuidado la tarjeta. Insertar la tarjeta microSD en la tarjeta NIMBUS, justo en la ranura correspondiente de "Conector microSD" (ver Tabla 1).
6. Para una nimbus MAXI :
   a. Alimentar la tarjeta introduciéndola de nuevo en el SAI o bien conectando un cable USB entre el ordenador y la tarjeta en la ranura "Puerto COM1" (ver Tabla 1). Una vez alimentada, los "LEDs de alimentación" empezarán una secuencia de flash de izquierda a derecha y viceversa. Este procedimiento puede tardar unos 10 minutos.
   b. Cuando finalice este procedimiento, los LEDs se apagarán. Retirar la alimentación de la tarjeta NIMBUS y a continuación, retirar la microSD de la ranura. La microSD ya no será necesaria.
   c. Introducir la tarjeta NIMBUS de nuevo en el SAI corresponiente y empezar de nuevo la configuración.
7. Para una nimbus MINI:
   a. Una vez insertada la tarjeta micro SD, ya se podrá conectar de nuevo la tarjeta NIMBUS en el SAI. No será necesario ningún procedimiento de grabación.
   b. Reiniciar la configuración.

7.4. PROCEDIMIENTO DE CARGA DE BACKUP.

Si previamente se ha realizado un backup de los parámetros de la tarjeta, recargarlos una vez realizada la actualización. Para ello, realizar los siguientes pasos:

1. Conectarse a la tarjeta punto a punto (ver apartado 2.1.1. Conexión punto a punto (cable Ethernet)) y acceder al panel con el usuario "engineer".
2. Desplegar la sección "Sistema" y seleccionar la última pestaña "Restablecer conf."
3. Cargar el backup, previamente descargado, mediante uso del botón "Browse". Cuando esté cargado, aplicarlo usando el botón "Restaurar".

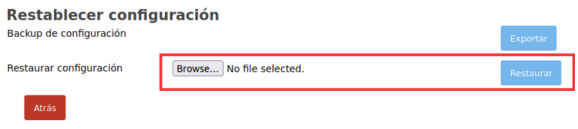


Fig. 101. Restaurar configuración.

4. Una vez aplicado, aparecerá una página como la siguiente, significando que se están aplicando los cambios. El procedimiento puede tardar unos 5 minutos.

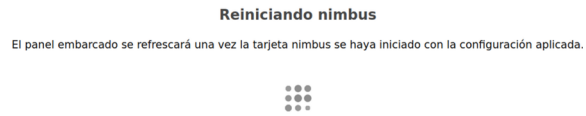


Fig. 102. Pantalla de reinicio Nimbus.

5. Una vez se haya reiniciado, la tarjeta NIMBUS se encontrará totalmente operativa y con la última versión actualizada.

8. ANEXO III. CARACTERÍSTICAS TÉCNICAS GENERALES.

En la *Tab. 9* a continuación se detallan las características técnicas de la tarjeta NIMBUS:

	Características
Procesador	Sitara AM3358BZCZ100 1GHz, 2000 MIPS
Tarjeta gráfica	SGX530 3D, 20M Polygons/S
Memoria SDRAM	512MB DDR3L 800 MHz
Memoria Flash	4GB, 8bit MMC integrada
PMIC	TPS65217C regulador PMIC y un LDO adicional.
Soporte para debug	Opcional Onboard 20-pin CTI JTAG
Conector SD/MMC	microSD , 3.3V
Audio	Interfície HDMI, Stereo

Tab. 9. Especificaciones técnicas tarjeta NIMBUS.

salicru

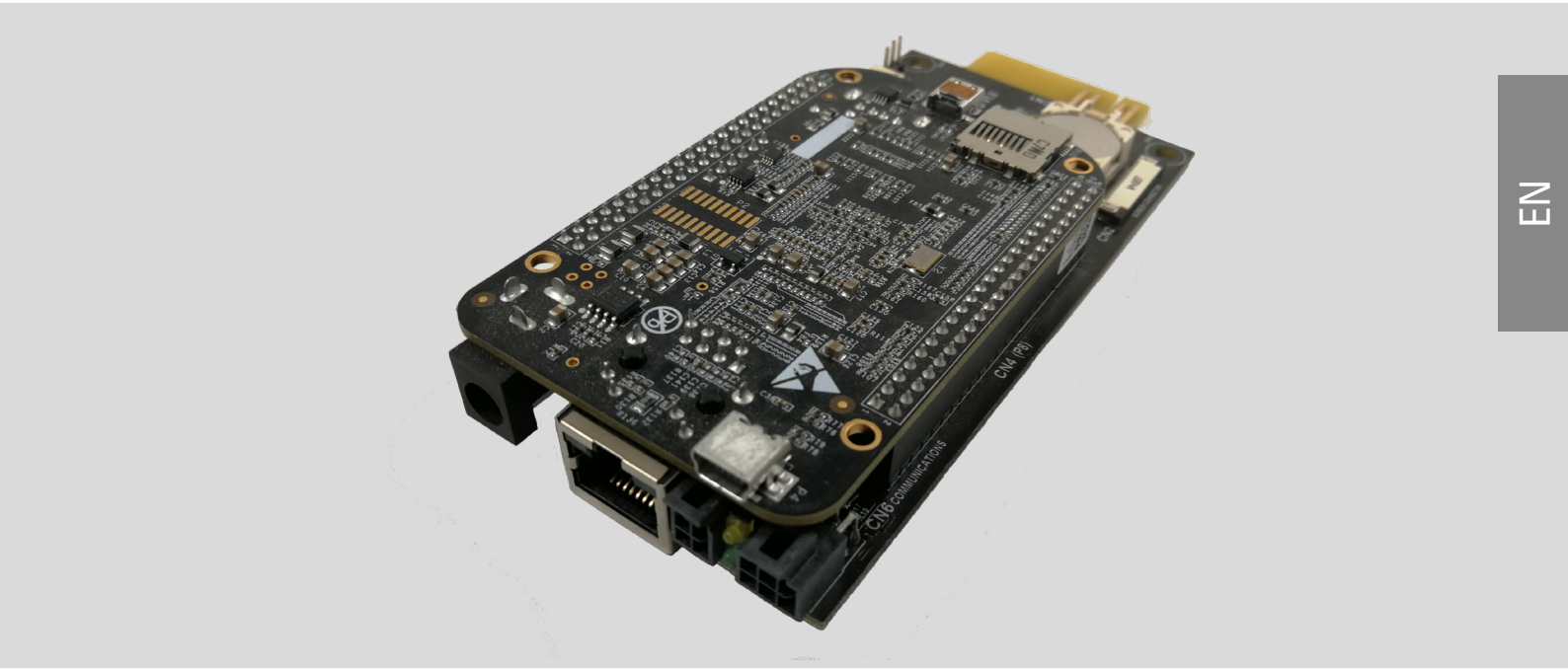
Avda. de la Serra 100
08460 Palautordera
BARCELONA
Tel. +34 93 848 24 00
sst@salicru.com
SALICRU.COM

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)
Inversores Solares
Variadores de Frecuencia
Sistemas DC
Transformadores y Autotransformadores
Estabilizadores de Tensión
Regletas protectoras
Baterías

USER MANUAL



EN

NIMBUS card

salicru

Contents

1. PRESENTATION.

1.1. VIEWS.

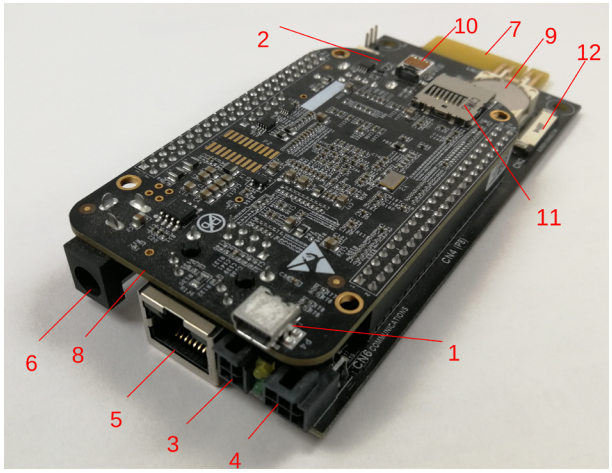


Fig. 1. View of the NIMBUS MAXI card.

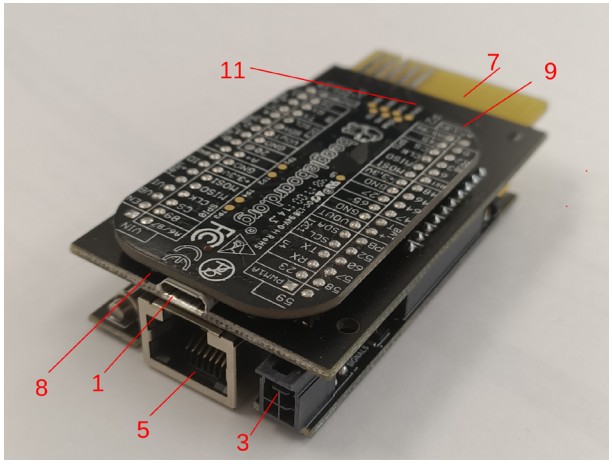


Fig. 2. View of the NIMBUS MINI card.

1.2. UKCA PRODUCT MARK AND UK AUTHORIZED REPRESENTATIVE.

UK CA product marking indicates that this UPS has been evaluated by Salicru and is deemed to comply with safety, health and environmental protection requirements.

The UK CA Declaration of Conformity is available upon request. For copies of of the UKCA Declaration of Conformity, please contact Salicru or check our website: www.salicru.com

UK Authorised Representative
Indele Limited
7 Bell Yard,
WC2A 2JR,
London

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

1.3. DESCRIPTION OF THE SYSTEM.

1.3.1. 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
- SLC CUBE3 / CUBE3+
- SLC CUBE4
- EMi3
- RE3
- SLC ADAPTX
- SLC ADAPT 2
- SLC X- PERT
- SLC X- TRA
- SLC TWIN PRO2 A
- SLC TWIN RT2 A
- SLC TWIN PRO2-T
- SLC TWIN R2-T
- SLC TWIN RT2
- SLC TWIN PRO2
- SLC TWIN/3 PRO2
- SLC TWIN PRO3

- SLC TWIN RT3
- SLC ADVANCE R / T
- SLC ADVANCE RT

Depending on the type of equipment, it will be necessary to use a NIMBUS-MAXI card or a NIMBUS-MINI card. Both have the same functionalities and mode of operation. To know the correspondence of each card with the different compatible series, refer to the following table:

	Nimbus MAXI	Nimbus MINI
SLC CUBE3/3+	✓	X
SLC X-PERT	✓	X
SLC X-TRA	✓	X
SLC ADAPT-X	X	✓
SLC ADAPT2	X	✓
SLC CUBE4	X	✓
SLC TWIN PRO2 A	X	✓
SLC TWIN RT2 A	X	✓
SLC TWIN PRO2-T	X	✓
SLC TWIN R2-T	X	✓
SLC TWIN RT2	X	✓
SLC TWIN PRO2	X	✓
SLC TWIN/3 PRO2	X	✓
SLC TWIN PRO3	X	✓
SLC TWIN RT3	X	✓
SLC ADVANCE R / T	X	✓
SLC ADVANCE RT	X	✓
DC Systems		
DC POWER-S	✓	X
DC POWER-L	✓	X
Voltage stabiliser		
EMi3	✓	X
RE3	✓	X

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

1.3.2. 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 via panel and SMS	Alert notifications through the on-board panel in real time, as well as being configurable to also be reported by SMS (using configurable SMTP protocol).
Configurable limits	It is allowed to establish certain limits in some variables to carry out two actions: either notify by SMS mail or perform a server shutdown remotely.
DNS server	Possibility of assigning domain names to the device.
IP address	Choice of DHCP or static web address.
Connection via Ethernet or WiFi	Possibility of configuring Internet access through a wired Ethernet connection or using an SSID to connect via WiFi.
Proxy server	Ability to configure a proxy server
User configuration	Own user management. Creation of users with the different roles available: "administrator"; "engineer" and "guest.
Upgrading packages	Upgrade to the latest version of the card only if you have a network connection.

Tab. 3. Basic integrated services

1.3.3. 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.
IEC 61850 protocol	International standard that defines the communication protocols between different equipment located in substations.
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.

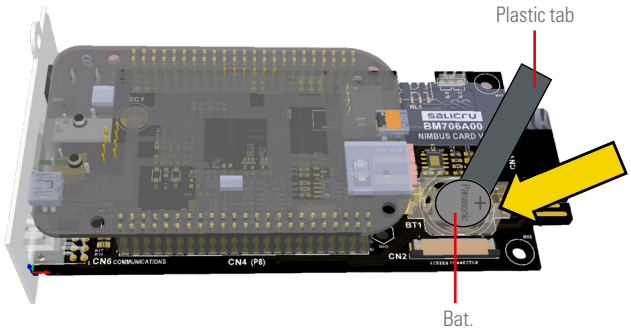


Fig. 3. Unlocking the battery of the NIMBUS card

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 Fig. 4.

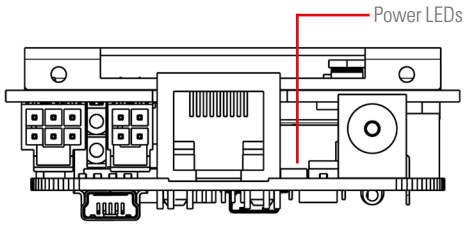


Fig. 4. NIMBUS card inserted into its slot

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 Fig. 5.

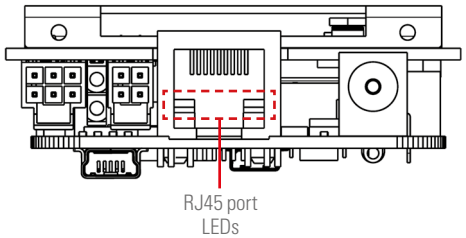


Fig. 5. Connection of the RJ-45 cable

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.

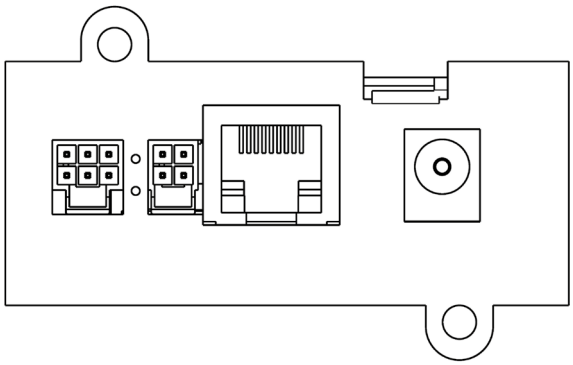


Fig. 6. The NIMBUS card with protective cover in place.

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 3.6. 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.

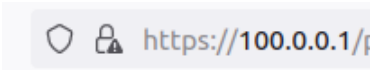
This service allows you to monitor the status of the device remotely and in real time, enabling you to directly access the device without having to be at the installation site.

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:



Otherwise, enter the new IP assigned to the card in the browser

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.

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)*.

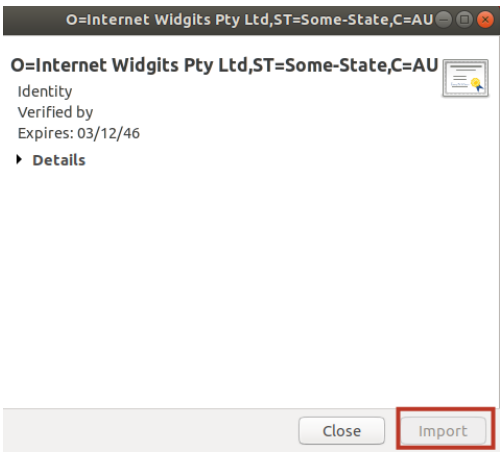


Fig. 8. Screen for importing the certificate locked.

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*.

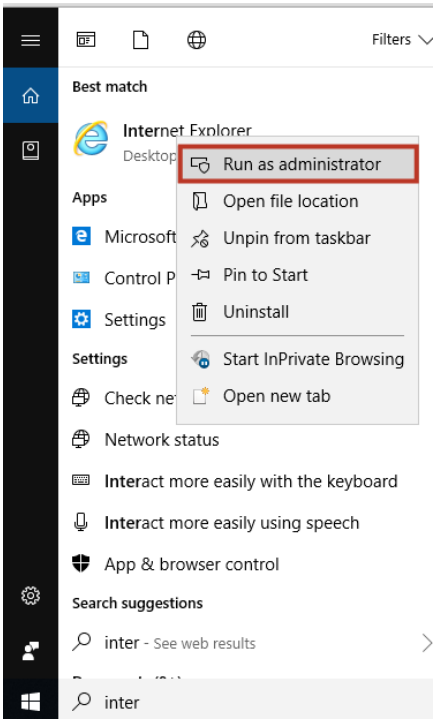


Fig. 9. 'Run as administrator' screen

- 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.

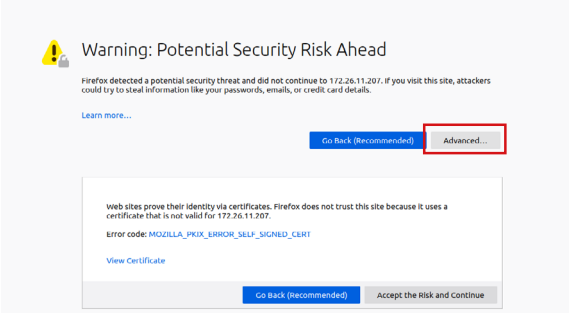


Fig. 11. Mozilla Firefox panel

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

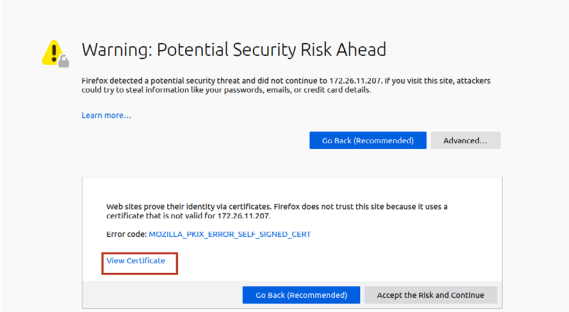


Fig. 12. Mozilla Firefox panel

- 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.

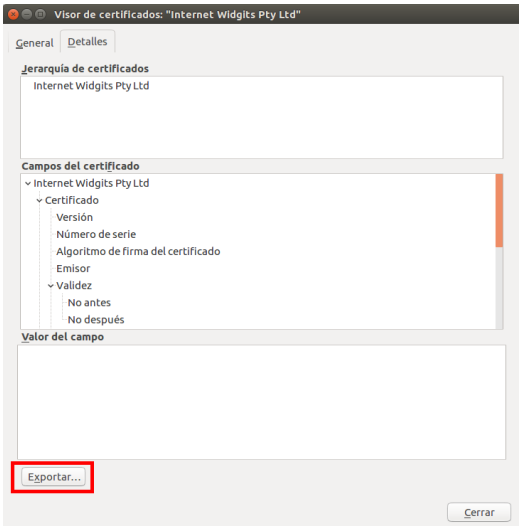


Fig. 13. 'Export ...' window.

- 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...'.

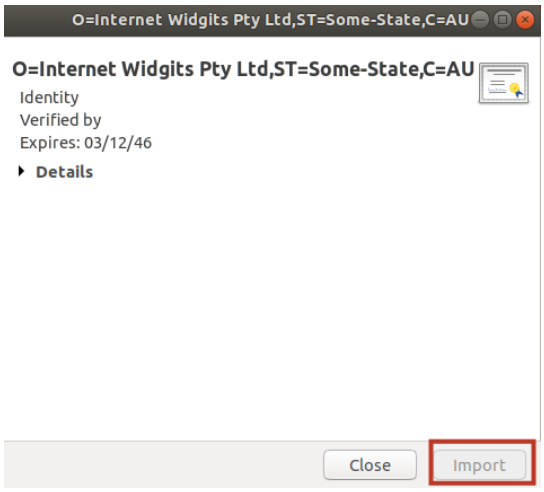


Fig. 14. 'Import...' window

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

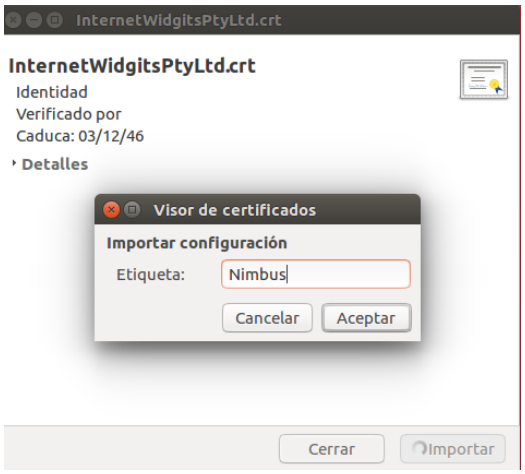


Fig. 15. "Label" window.

- 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)*.

EN

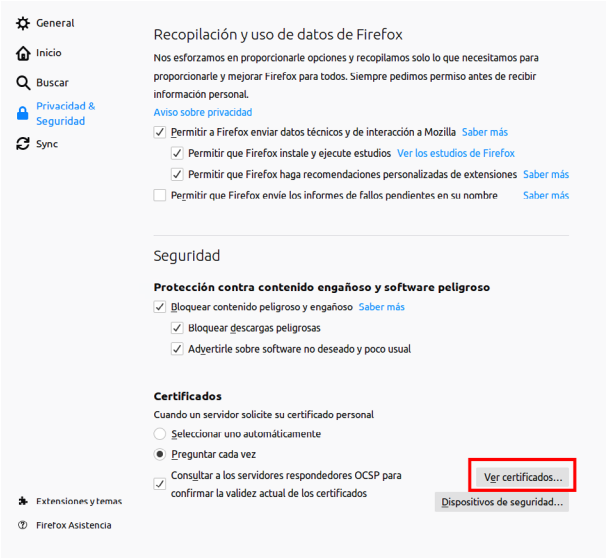


Fig. 16. Firefox 'Privacy & Security' menu

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

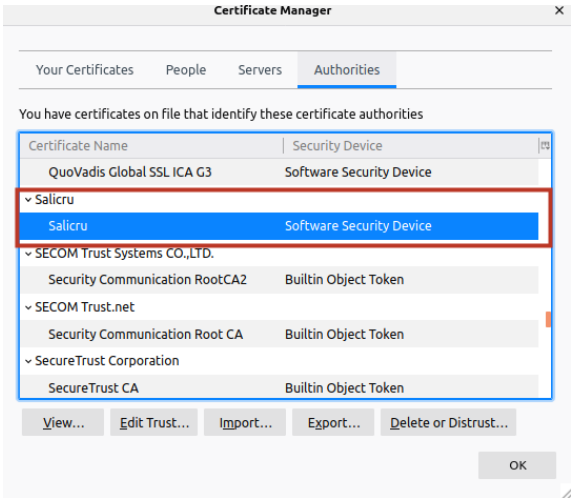


Fig. 17. 'Certificate manager' window.

- 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:

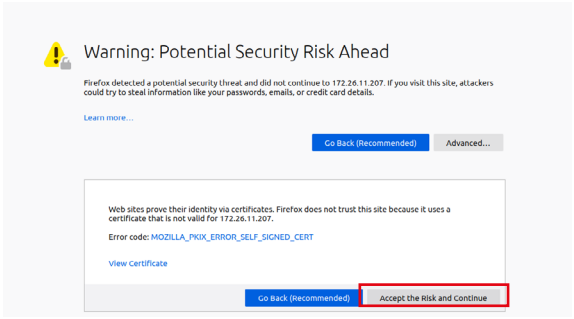


Fig. 18. 'Accept risk and continue' window.

3.1.1.3. Chrome / Opera.

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

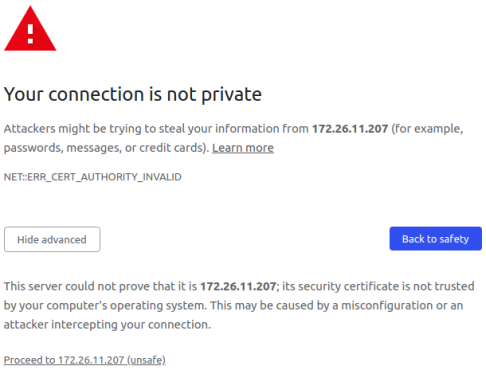


Fig. 19. Chrome / Opera browser home screen.

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

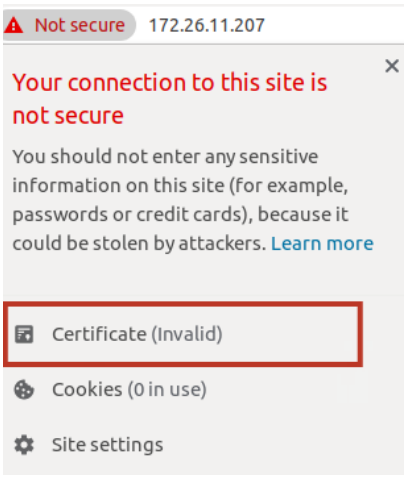


Fig. 20. Available options window

- 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)*.

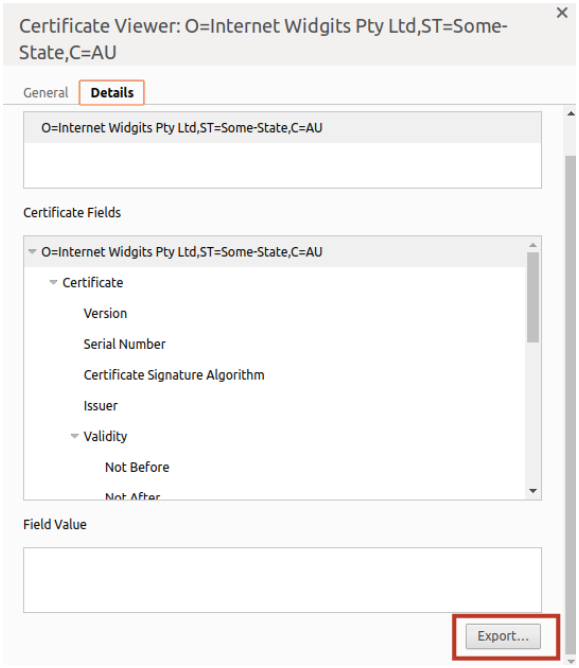


Fig. 21. 'Certificate viewer - Export' screen

- 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...'.

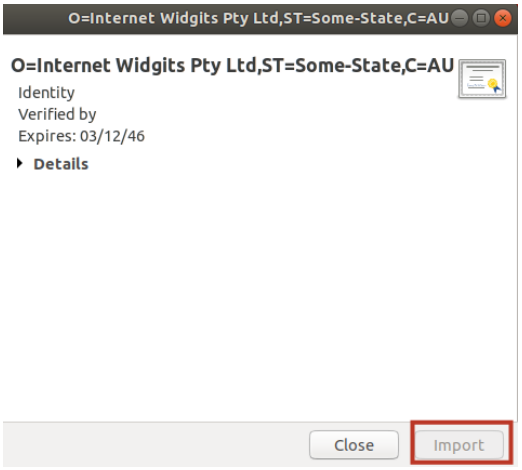


Fig. 22. 'Import ...' screen.

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

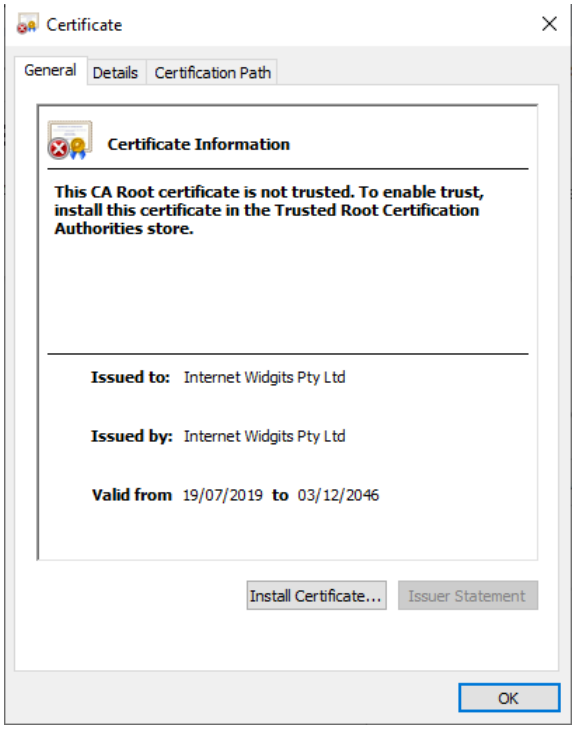


Fig. 23. "Certificate viewer" screen.

- 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.

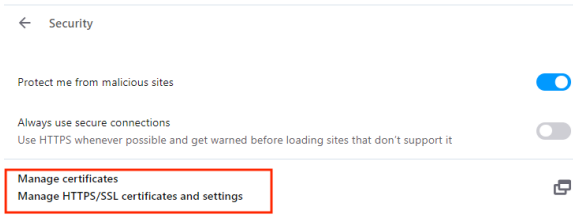


Fig. 24. 'Advanced settings - Manage certificates' screen.

- 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).*

EN

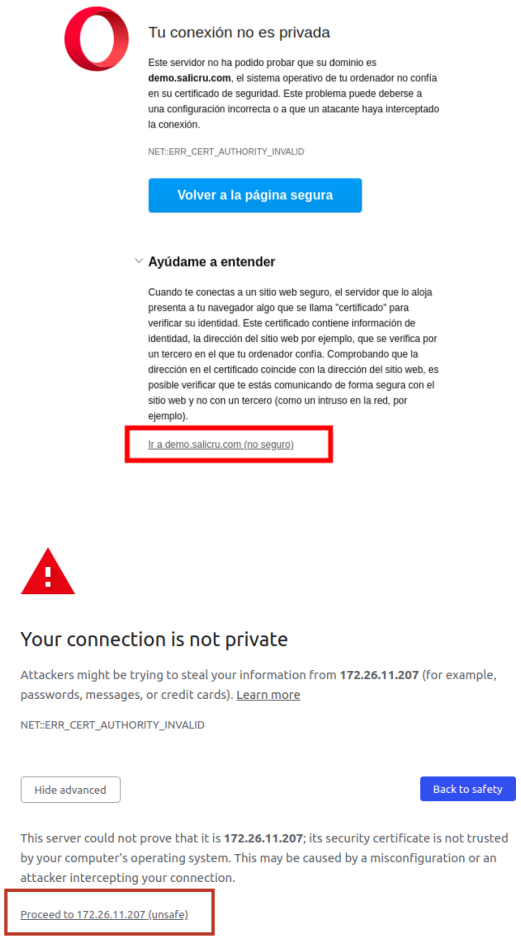


Fig. 25. 'Warning message' screen.

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.

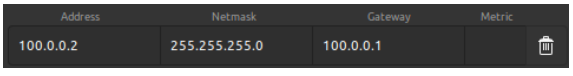


Fig. 26. Network parameters for point-to-point connection.

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.

Important note: If your network is in the 192.168.6.0/24 or 192.168.7.0/24 range, this may cause interference between the IPs assigned to the device. Please contact customer support to resolve this issue.

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.

3.2. SCREEN LOGIN.

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

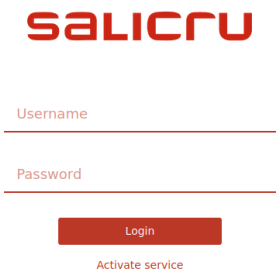


Fig. 27. Login and password screen

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

	Administrator	Engineer	User
User name	"administrator"	"engineer"	"guest"
Password	"Nimbus4dm" [2]	"SLC3ng1n" [1] "Nimbus3ng" [2]	"SLCg13st" [1] "Nimbus6st" [2]
Permission	- Modify some device parameters. - Modify NIMBUS card parameters. - Measurements display. - User management. - Updating of services.	- Modify some device parameters. - Modify NIMBUS card parameters. - Measurements display.	- Only display device measurements.

[1] Up to firmware 2.8.6.

[2] From firmware 3.0.0. onwards.

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.

3.2.1. Change password first login.

If this is the first time you access the panel with a new default user (administrator, engineer or guest), you will be prompted to update your password.

The new password cannot be the same as the default password to ensure security. It must contain at least 8 characters, uppercase, lowercase, numbers and special characters.

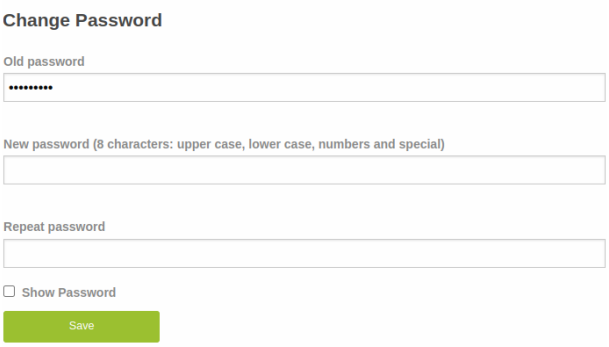


Fig. 28. Password change screen.

Later, this password can be changed from the "Change password" section once the on-board panel has been accessed.

Important: make a note of the password entered as it cannot be retrieved via email. The password can only be reset by completely flashing the card, causing a loss of the settings if they have not been saved.

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.

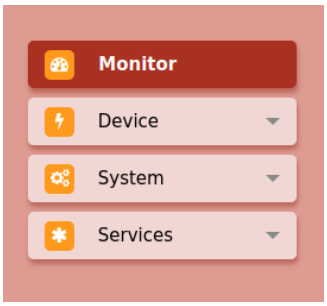


Fig. 29. Embedded panel main navigation tree.

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

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. 29* 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 X-PERT, 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.

EN

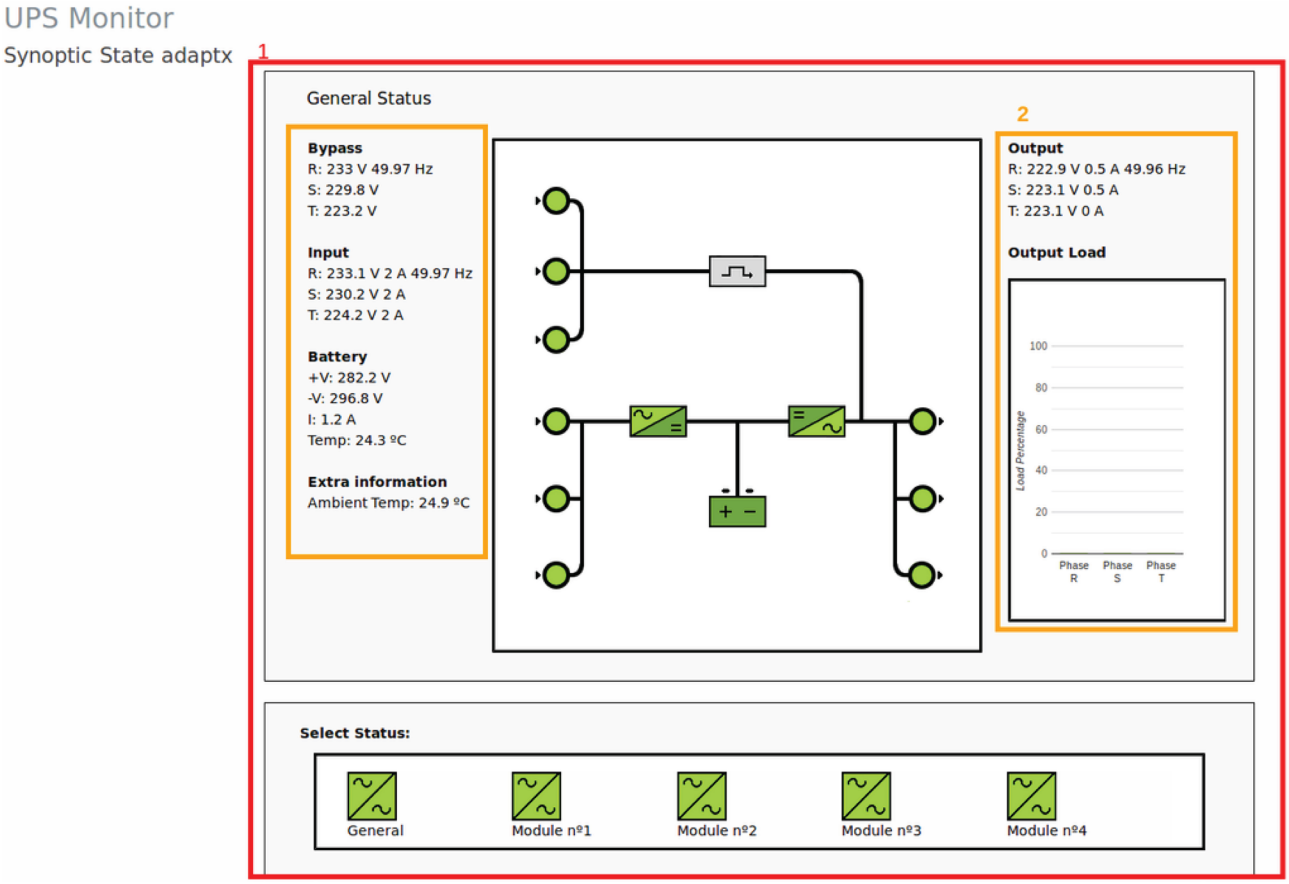


Fig. 30. UPS monitor diagram.

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. 30*). 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. 30*).

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:

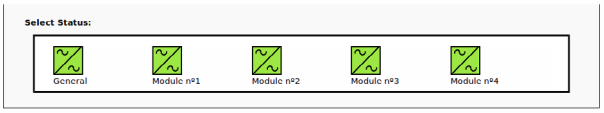


Fig. 31. Example of modules in the ADAPT2 and ADAPTX series.

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:

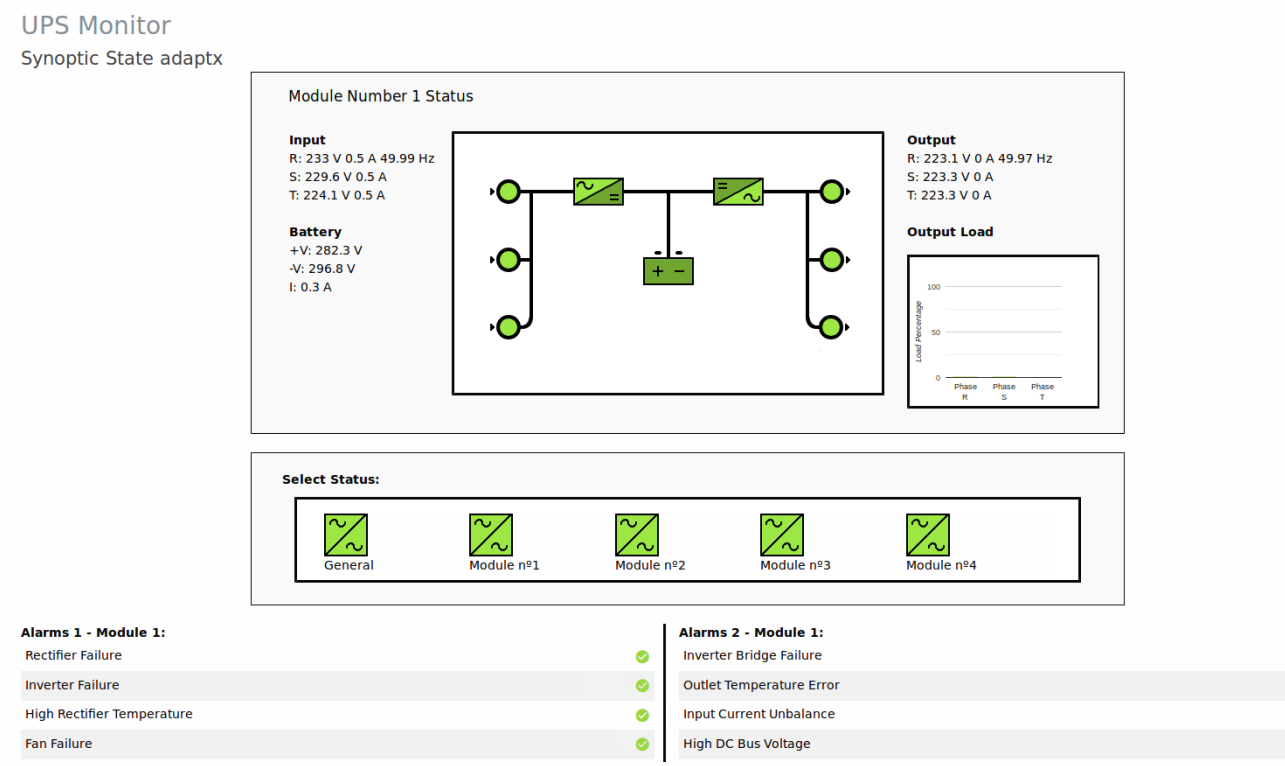


Fig. 32. Diagram relating to a single module.

3.4.1.2. SLC CUBE4 7.5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2, SLC TWIN RT2, SLC TWIN PRO2 et SLC TWIN RT3 series.

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

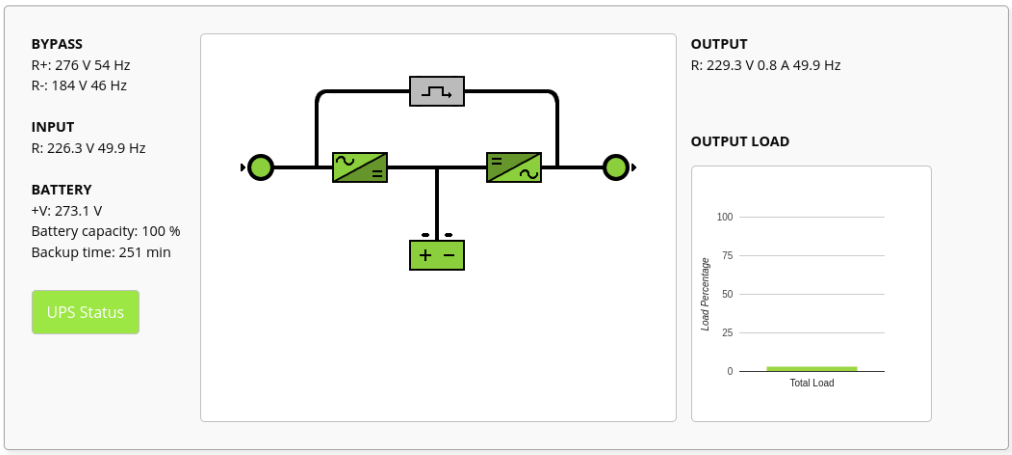


Fig. 33. Synoptic system status and alarms.

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.

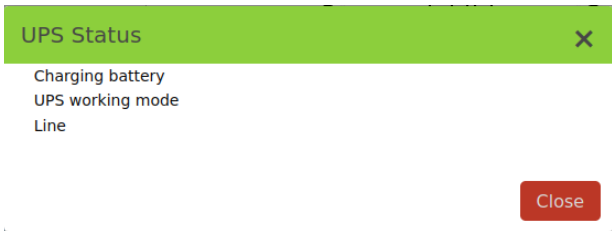


Fig. 34. Details of the "UPS status" button.

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.

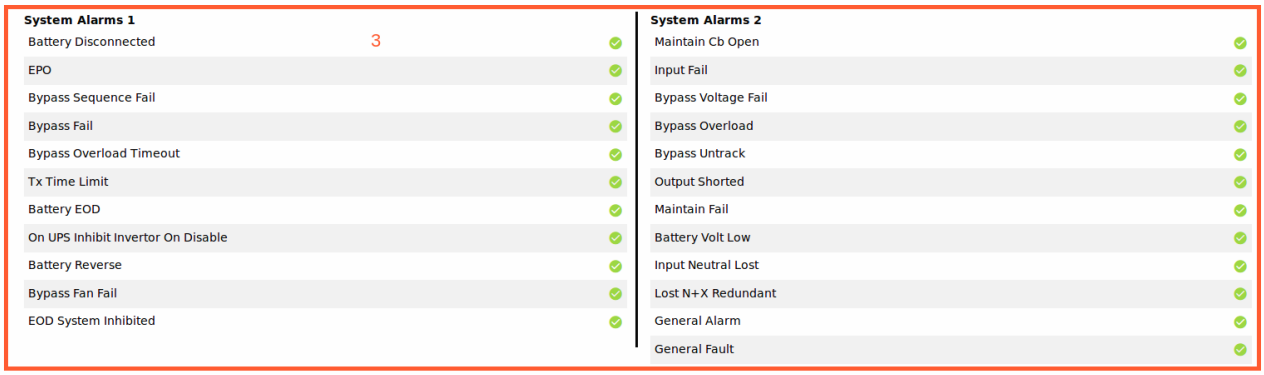


Fig. 35. Part of the display where the different alarms are shown.

3.5. DEVICE.

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

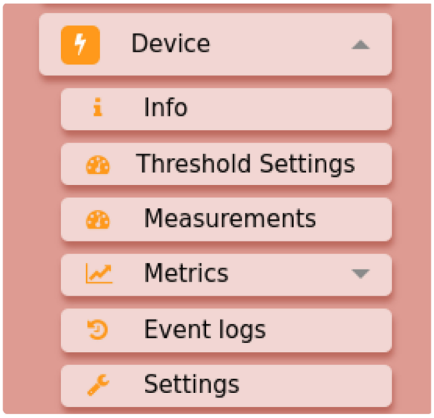


Fig. 36. Device menu.

3.5.1. Info.

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. Threshold settings.

Configuration page. Set limit values above which to receive alarms and notifications.

Important: for the page configuration to be correct, first configure the SMTP server and/or the RCCMD server, depending on the desired function.

When configuring in the "Warnings" section, an email will be sent to the user when the threshold exceeds the limit value.

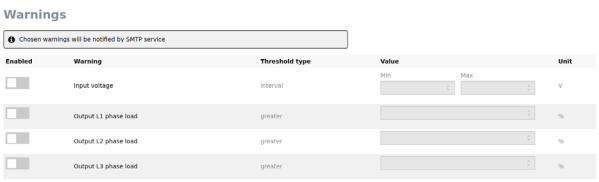


Fig. 37. Warnings menu.

When configuring in the "Alarms" section, a server stop order will be launched when the threshold exceeds the limit value. (see RCCMD).

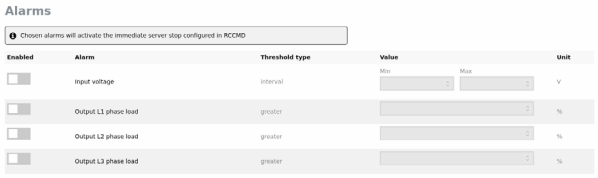


Fig. 38. Alarms menu.

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:

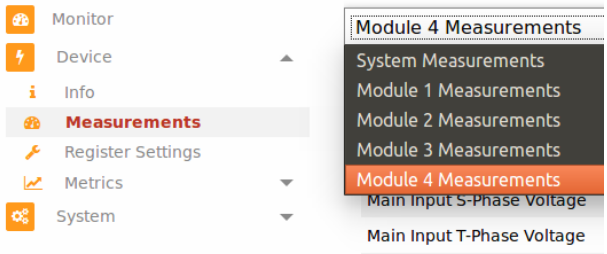


Fig. 39. Module 'Selector' screen.

3.5.4. Register Settings.

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

Note: only available for some specific series. Check the attached table to see the compatibility of the different ranges.

UPS Series	Option to modify parameters
SLC CUBE3/3+	✓
SLC X-PERT	X
SLC X-TRA	X
SLC ADAPT-X	✓
SLC ADAPT2	✓
SLC CUBE4 30-80 kVA	✓
SLC CUBE4 7,5-20 kVA	X
SLC TWIN RT2	X
SLC TWIN PRO2	X
SLC TWIN/3 PRO2	X
SLC TWIN PRO3	X
SLC TWIN RT3	X
DC systems	
DC POWER-S	✓
DC POWER-L	✓
Voltage stabiliser	
EMi3	✓

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.

Note: 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*).

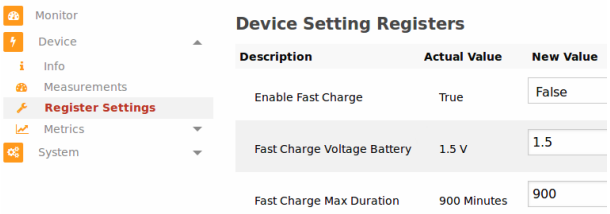


Fig. 40. Modification of parameters in Register Settings.

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*).

Fig. 41. 'Start/Stop' parameter.

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

EN

3.5.4.3. 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 24 hours** of the measurement selected, see accompanying image.

If the device is connected but there is a problem with the NIMBUS card, the last data sent will be displayed with an interval of two hours (see Fig. 44), as long as the equipment has been connected for at least that time. If you have been connected for a shorter time, the connection time measurements will be shown, always up to a maximum of three hours.

⚠ To download a history of each measurement individually in .csv format, click on the "Export CSV" button located above each graph. In this way, the data displayed in the graph (last 24 hours) will be exported.

Fig. 43. Evolution of the data sent for each three hours.

3.5.6. Manage alarms.

For series that have alarm validation, it is possible to acknowledge alarms remotely. When an alarm is active and can be viewed in the panel overview, it will appear in this section as suitable for recognition. To do this, click on the "Validate" button next to the name of the alarm you want to recognize

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.

Only for SLC DC POWER-S series it is possible to force actions on the device, currently only the battery test is available. When this action can be launched internally on the computer, a button will be displayed next to the action itself to launch it. Otherwise, as shown in the image, if the action is not available, a blocked button will appear and will not allow it to be launched.

Fig. 45. Forcing actions.

3.5.8. Logs / Event log.

For all the series it is possible to download the internal history of the team and make use of this page.

3.5.8.1. DC-S series.

Only for SLC DC POWER-S series, it will be necessary to perform 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.

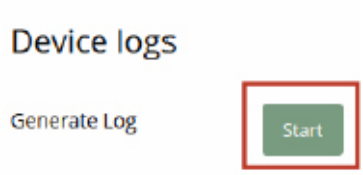


Fig. 46. Generating logs.

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

3.5.8.2. Rest of series.

All the alarm events triggered on the device will be stored in this section, up to 500 events. Go to "Device > Event logs".

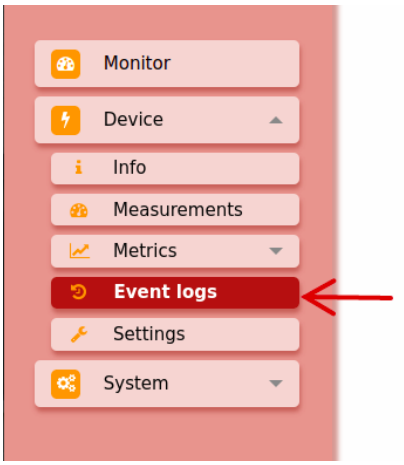


Fig. 47. Event Logs screen.

It is also possible to download the log in .csv format. To do so, click on the upper right button "Export CSV".

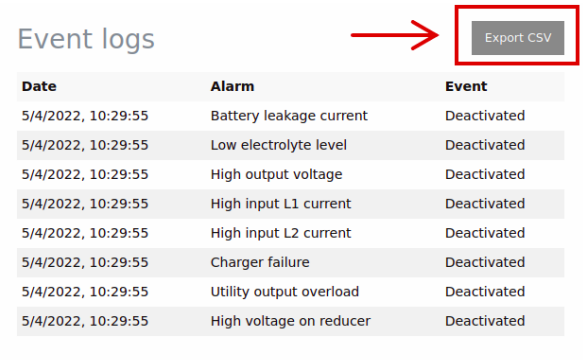


Fig. 48. Export CSV screen.

3.5.9. Backup.

In the event of a device malfunction, only for the DC power-S series, 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.

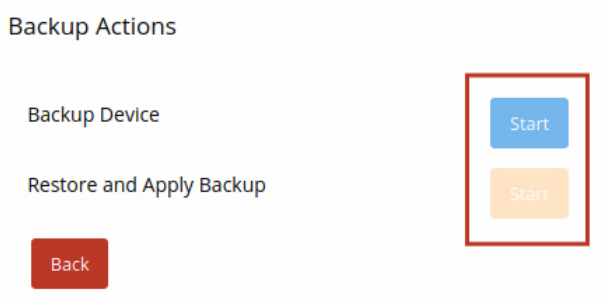


Fig. 49. Restoring factory settings.

3.5.10. Actions.

Only for TWIN PRO2, TWIN RT2, TWIN PRO3 and TWIN RT3 series it is possible to execute certain actions on the device. To do this, use the buttons that are next to each action.

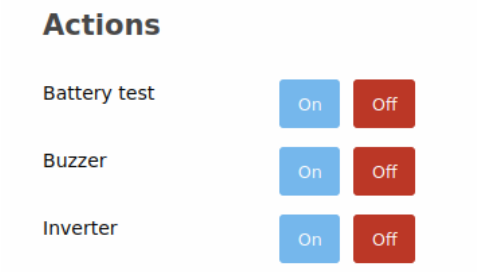


Fig. 50. Actions on the device.

3.5.11. Service logs.

For troubleshooting purposes only.

View and download the logs of all services running within the "Nimbus" card.

Use the drop-down to select which service you want to view or retrieve the latest service logs. Then click on "Apply".

Fig. 51. Service Logs.

If you wish to export the same log displayed on the screen, click on "Export CSV" to obtain the same text in .log format to send to the technician, in case of detected failure.

3.6. SYSTEM.

Available only for Engineer users. Click on 'System' to display/hide the options described in this section.

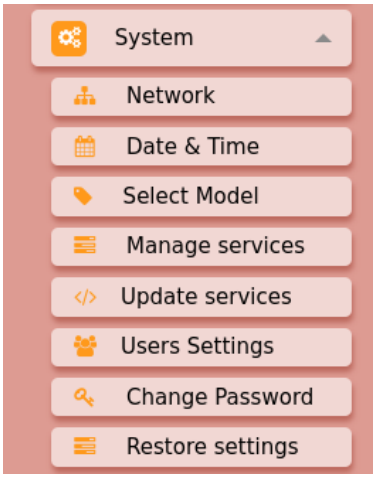


Fig. 52. System screen.

3.6.1. Network.

3.6.1.1. Set IP address

The NIMBUS card has two possible modes of remote connection through IP address (go to Ethernet section).

3.6.1.1.1. 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.

3.6.1.1.2. 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.

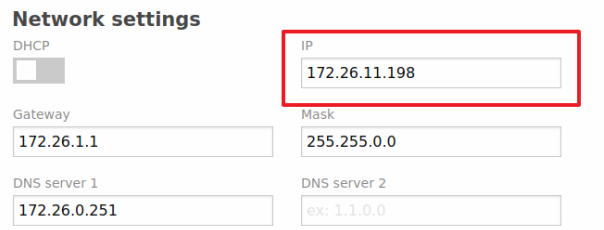


Fig. 53. Network settings.

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.

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

3.6.1.2. Configuring a proxy server.

A proxy server acts as an intermediary between your device and servers on the internet, improving the privacy, performance and security of your connections.

To configure it, activate it from the "proxy" tab (it is disabled by default) and enter your proxy settings.

Fig. 54. Proxy settings.

3.6.1.3. Connectivity test.

In order to ensure that the connection to the basic servers for the operation of the NIMBUS card are accessible, make use of the "Connectivity Test" that will be found in this tab.

In it, the main addresses in use will be analyzed. If all the routes are green, it means that the NIMBUS is correctly configured for all its uses.

In the event that there is a route in red, it could mean that there is a port that is not accessible or that the entry to the card is being banned.

Network status	
Network (Internet access)	✓
DNS resolution	✓
NTP server	✗
HTTP:80 to portquiz.net	✓
HTTP:80 to archive.salicru.com	✓
SSH:22 to portquiz.net	✓
MQQT:1883 to portquiz.net	✓
MQQT:8883 to portquiz.net	✓
MQQT:8883 to mqtt.googleapis.com	✓
HTTPS:443 to portquiz.net	✓
HTTPS:443 to accounts.google.com	✓
HTTPS:443 to oauth2.googleapis.com	✓
HTTPS:443 to cloudiout.googleapis.com	✓
HTTPS:443 to www.googleapis.com	✓
HTTPS:443 to archive.salicru.com	✓

Fig. 55. Network Status Screen.

For an off-grid connection, it will only be necessary to have access to:

- Network (internet access).
- DNS resolution.

If the remote maintenance option is required, the other routes must also be green. Without them, connectivity through MQTT cannot be guaranteed.

3.6.2. Date & 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. Choice of system and reboot system.

The first time the NIMBUS card is inserted into a device, it automatically detects which type of device it is in.

You can also use the option to disable this option, in case you are not going to change the equipment card.

Fig. 56. Choice of system screen.

Note: Do not change the model if the NIMBUS card has not been previously inserted in another unit. After changing the model, it is advisable to exit and re-enter the panel to display the data correctly.

In case the system gets stuck or needs to be rebooted remotely (without the need to manually reboot the card), use the "Reboot system" button to execute this task without having to move in front of the computer.

Please note that rebooting the system may take 3 to 5 minutes to become operational again.

3.6.4. Upgrade services.

To update the card partially (only a few packages) or completely (the whole system), this page is only accessible to users with an administrator role.

To start, click on "Check for updates" so that the system detects whether it is able to perform a new update or not. This process may take a few minutes.

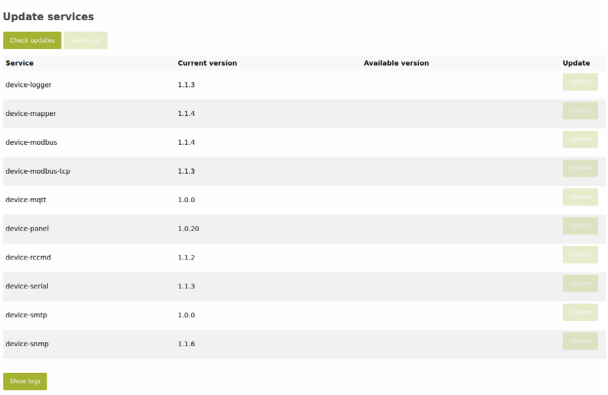


Fig. 57. Update Services screen.

Once the command is executed, if updates exist, they will be displayed under "version available". The corresponding "update" button will be activated to make way for the possible update.

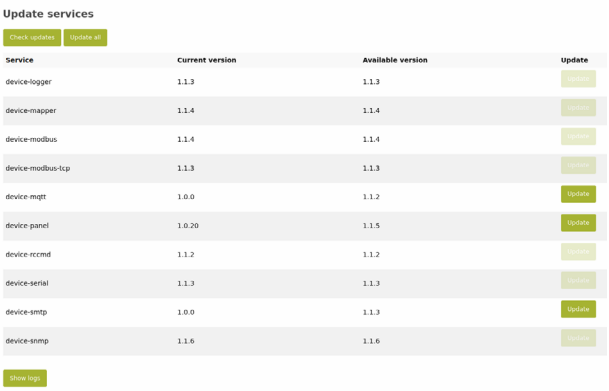


Fig. 58. Pantalla Actualizar Servicios con las versiones disponibles.

To update only an individual service, click on the "update" button available next to each service. If you wish to update all services at once (recommended) to have the card upgraded to the latest version, click on the "update all" button at the top of the page.

Remember that if you decide to update the services individually, you will have to do it one after the other.

To follow the upgrade process, click on "show logs". At the bottom of the page, the logs of the update in progress will be displayed, so that you can see the progress in real time.

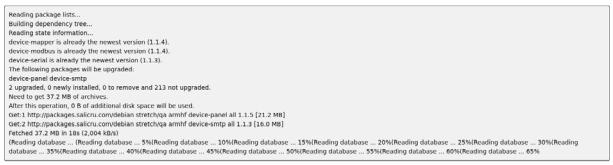


Fig. 59. Viewing logs.

3.6.5. User configuration.

If you want to manage users, go to this page, where you will be able to see a list of users already created and the role established. You will NOT be able to see or recover user passwords (or your own), so you must remember the passwords you have changed.

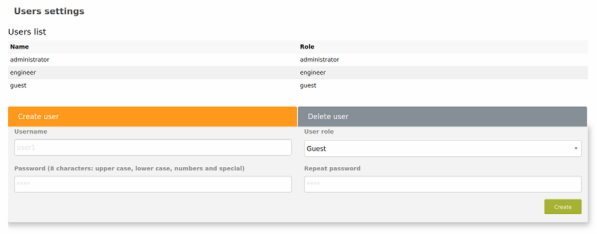


Fig. 60. User settings screen.

Two sections are available for modifying users:

1. **Create a new user**: To do this, you will need to enter a user name, the role chosen for the user (administrator, engineer or user) and the password. Remember that the password must contain 8 characters including a capital letter, a lower case letter, a number and a special character.

Fig. 61. List of users.

Once the process is finished, click on "Create" and the newly created user will appear in the list.

2. **Delete an existing user**: Go to the second section. Choose a user to delete from those available in the form and click on "Delete".

Fig. 62. Delete user" screen.

Note: It is not possible to delete one's own user.

3.6.6. Change password.

To change the password of the logged-in user, enter the current password and the new password, remembering that it must be at least 8 characters long, including an uppercase letter, a lowercase letter, a number and a special character.

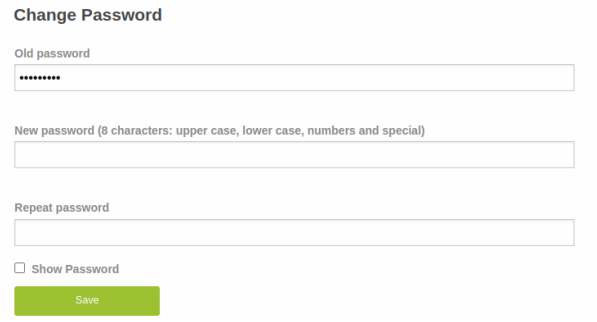


Fig. 63. Password change screen.

3.6.7. Reset configuration.

In the event of having to update the firmware of the device, it is highly recommended to make a backup copy of the configuration previously configured on the card.

To do so, click on "Backup configuration". A file containing all the configuration will be generated..

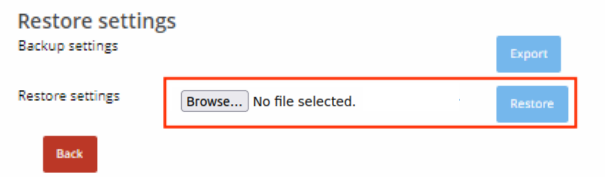


Fig. 64. Restore settings.

Once the firmware has been updated, access the panel again with the user "engineer" and click on "Browse..." under "Restore configuration". Load the previously generated file and click on "Restore".

This action may take a few minutes.

3.7. SERVICES.

Available **only for engineer/administrator users**. Click on **Services** to display/hide the options described in this point.

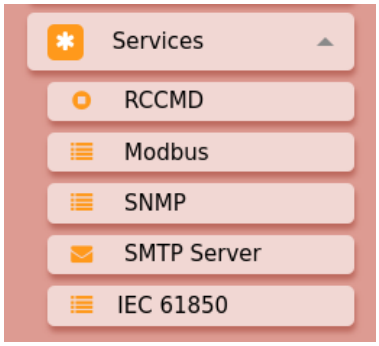


Fig. 65. Services screen.

3.7.1. RCCMD.

To make this screen, related to an optional service of the card, effective, first refer to section **4. Installing the RCCMD software**.

Up to 5 individually configurable IP addresses with all available alarm possibilities are available. To start, select a possible slot in which to save the configuration by using the drop-down selector "select a configuration".

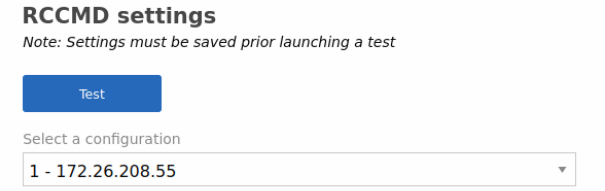


Fig. 66. RCCMD Parameters Screen.

The slots in which an IP address is already configured appear with this IP address. The others, if they are free, will contain the name "Add new configuration". Up to 5 addresses can be configured, but it is not necessary to configure all of them..

Once you have selected the slot in which to save the configuration, proceed to configure the alarms. There is a page like this for each configuration.

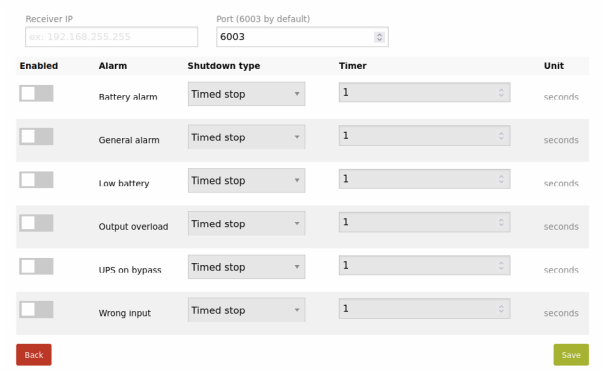


Fig. 67. Alarm configuration screen.

Enter the IP address of the destination server here. If a wide broadcast is desired, enter the IP of this broadcast. Also add the port of the RCCMD client, as described in the following point **4.2.2. Sender port**.

For each of the possible alarm groups, activate or deactivate the functionality by moving the button. Only when a group is active, it will be possible to operate both on the type of shutdown and on the set time..

It has two types of stoppages:

- **Delayed**: a time range will be assigned after which, if the condition is met, the remote shutdown will be carried out.
- **Immediate**: does not have a timer, when the condition is detected as active it will proceed to remote shutdown.

When you have finished making your changes, remember to save them using the "Save" button at the bottom of the page.

If you wish to test your configuration without having to stop any server, you can use the "Test" button at the top of the page. Clicking this button will cause a LOG message to be sent to your configured IP. Make sure that it is received correctly before finalizing the installation and setup of the service.

3.7.2. Modbus.

Note: in the SLC CUBE4 7.5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2 and SLC TWIN RT2 series, it is not possible to modify the communication configuration parameters.

Modify the modbus address of the Slave to which the NIMBUS is connected to read information, as well as the protocol parameters to establish connection with the unit. By default, these values will already allow correct communication with the equipment.

Consult the equipment configuration to know in which addresses and configuration parameters the information is available in case of modification.

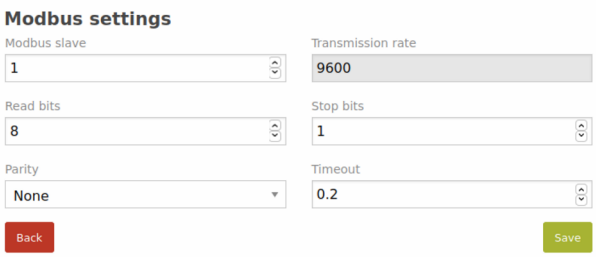


Fig. 68. Modbus settings.

Note: After a change of address it is advisable to restart the panel and wait a few minutes. Do not perform a restart of the NIMBUS card as the new values entered will be lost.

Important: Invalid values will result in loss of communication with the equipment. Before modifying them, make sure that the panel is not receiving data and that you know the correct values set in the equipment. Do not modify these values if the panel is receiving data.

3.7.2.1. Modbus TCP.

If the modbus TCP server is active, it is possible to modify the port on which the service is available in this section.

Note: TCP server is available for all series, including those without modbus configuration parameters such as SLC CUBE4 7,5-20 kVA, SLC TWIN PRO2, SLC TWIN/3 PRO2 and SLC TWIN RT2.

3.7.3. SNMP.

Only if the **optional SNMP service** has been contracted, this page can be displayed.

The nimbus card implements SNMP v3 protocol which has better security features in terms of message encryption and access to messages. To make use of the service, it is necessary to establish a user name and password to read the messages.

Note: SNMP v1 and SNMP v2 can be enabled by disabling the v3 version via the corresponding selector in the SNMP tab.

- V3 configuration.

  For the initial configuration, create the "user name" and "password" with which the connection will be established. To do this, enter the values in the "SNMP parameters" section.

  The user "salicru" is not allowed.

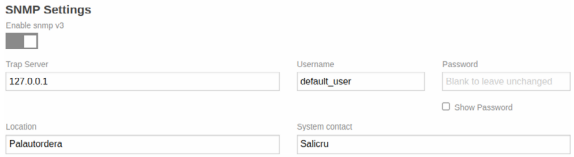


Fig. 69. Initial configuration.

- V2 configuration.

  Disable the "enable snmp v3" selector. Enter the value of "community" with which to communicate with the equipment. By default, this value does not exist, so it is essential to assign it an initial value in order to be able to proceed with the reading.

EN

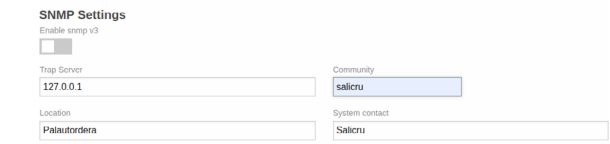


Fig. 70. Disabling SNMP V3.

If you wish to configure the trap server on the computer on which to receive notifications in the event of a change of status, alarm and/or warning, enter it in "trap server". The authentication will be the same as for reading messages.

To find out the IP address of the computer, open the system browser and type "cmd". Run the program. Type ipconfig in the terminal and search for the internet address.

Save the changes after you have made them by clicking on the "save" button.

Note: It will be necessary to have installed a programme that allows to receive and manage the "Trap" generated by the equipment.

To check that the trap server has been configured correctly, you can make use of the "test" section below.

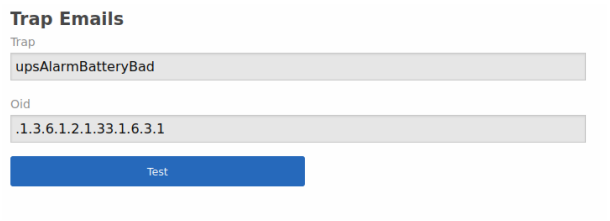


Fig. 71. Trap server configuration test.

3.7.4. SMTP server.

Configure the SMTP server in order to receive mails when an alarm is triggered and/or a predefined threshold is exceeded (see section 3.5.2. Threshold settings.).

It is essential to use a server that allows the use of a username and password. If they are not specified, the service will not be correctly configured.

Some possible server configurations:

- Office 365:

Host	smtp.office365.com
Port	587 (recommended) or puert 25
Sender mail	the mail
Username and password	the credentials for the mail set above under "sender mail".

- Outlook:

Host	smtp-mail.outlook.com
Port	587 (recommended) or puert 25
Sender mail	the mail
Username and password	the credentials for the mail set above under "sender mail".

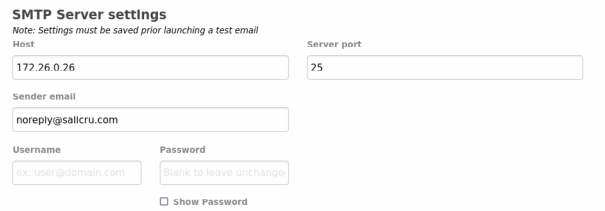


Fig. 72. SMTP server configuration.

Important: If you do not explicitly save the configuration by clicking on the "Save" button, it will not be modified. Before launching any action, make sure you have made these changes correctly.

To check that the configuration is correct and that the mails will be received, use the "Test" button. Remember to save the configuration first.

In the second part of the screen it is possible to configure the email depending on what you want to be notified. Enable the alarms for which you wish to receive notifications. Different sending options are available, among them:

- **Immediately**: the alarm will be notified by e-mail at the same time as it is triggered. No time required.
- **After a few minutes**: the mail will be sent certain minutes (set a value) after the alarm has been triggered. This is a function in which you see the alarm notification in delay.
- **Frequency of minutes**: Once the alarm is activated, the alarm shall be notified every x minutes (user set value). Repeated reporting shall cease when the alarm is deactivated.
- **After a few minutes on battery**: an active alarm will only be notified as long as the equipment is also on battery and the user predefined minutes have elapsed.
- **Some time of autonomy**: an active alarm shall only be notified when the equipment is on battery and the battery life limit value is below that set by the user.

Note: to receive messages you must always have at least 1 destination email. It can be configured in the section "Customise your email".

3.7.5. IEC-61850.

You can export the .icd file to load it in the visualisation program through this page.

If you wish to modify any of the following values to be different from the IP on which the equipment is configured:

- IP
- Subnet mask
- Gateway

these values can be set individually.

Fig. 73. IEC-61850 settings.

Otherwise, activate the "automatic" option to automatically load the configuration. Save changes before exporting the file.

3.8. LOGOUT.

Click this button on the right in the top bar when you no longer want to consult the equipment panel or if you prefer to access it with a different access account.

EN

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. 74. Generex main screen.

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

Fig. 75. 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. 76. 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'.

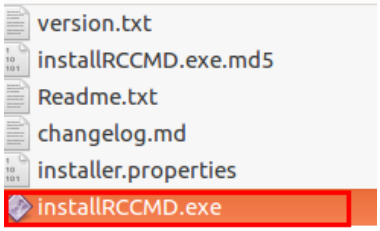


Fig. 77. Binary of execution of RCCMD

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

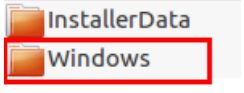


Fig. 78. Windows folder inside the unzipped folder.

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

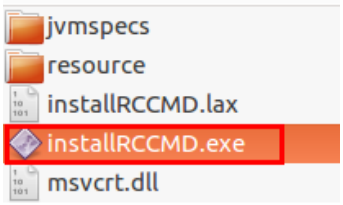


Fig. 79. Binary of execution of RCCMD in the windows folder.

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.

Fig. 80. 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.

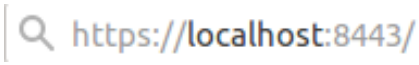
If you have selected this operating system, you will need a licence code, which will be provided by SALICRU.

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.

Fig. 81. 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:



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

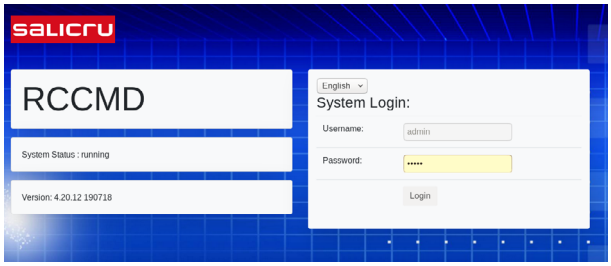


Fig. 82. RCCMD main screen.

In the section 'System Login', enter the credentials provided by SALICRU and click on the button 'Login' *(Fig. 82)*.

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. 83*.

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

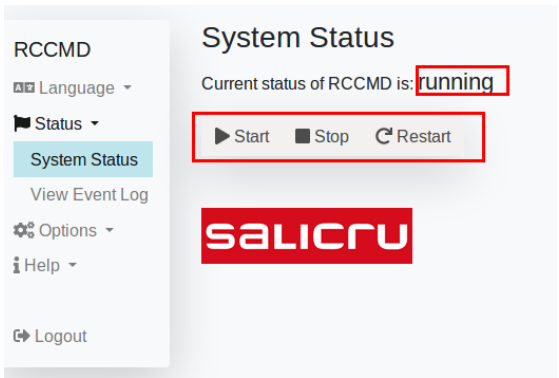


Fig. 83. RCCMD: System status.

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.

EN

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. 84*.

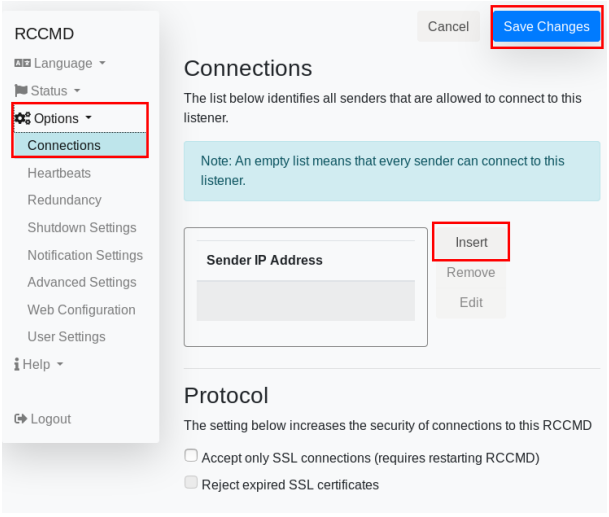


Fig. 84. Pairing screen for the NIMBUS card.

If the 'Sender IP Address' field is left empty, the server will still be able to listen to and therefore execute any shut-down 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. 85*.

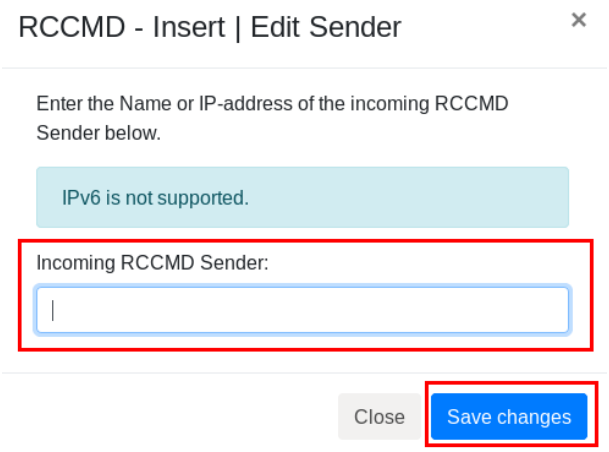


Fig. 85. Insert IP screen.

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. 86*.

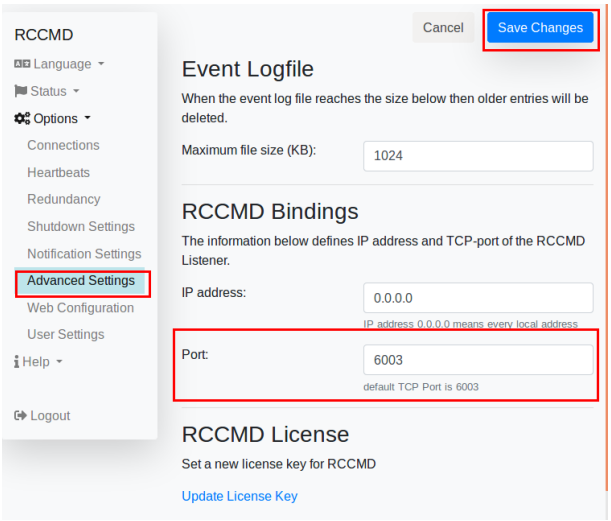


Fig. 86. Advanced Settings screen.

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.

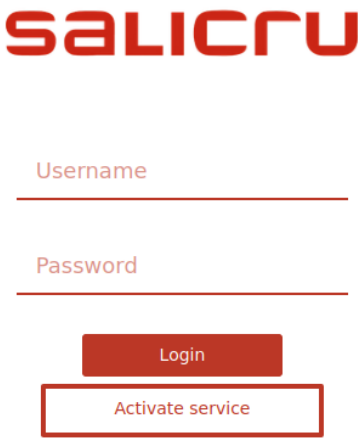


Fig. 87. Activate service.

3. 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.
IEC 61850	Protocolo de comunicación secundario. Permite recibir MMS

(*) 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. 6. Optional packages.

6. APPENDIX I. CONNECTIVITY

For any 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.

Hostmane	Puerto
europe-west1-g5-mqtt.clearblade.com	443 y 8883
europe-west1.clearblade.com	443

Tab. 7. List of IPs / ports for correct connection to the remote maintenance panel.

6.2. SERIES SLC TWIN PRO3 Y SLC TWIN RT3.

These series of UPS allow integrated connectivity of the device without the need to use the Nimbus card. This integrated connectivity can be achieved through an Ethernet or WiFi connection, in the latter case a device capable of capturing the WiFi signal will be needed.

6.2.1. Integrated connectivity via Ethernet.

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

Review the firewall requirements for using the OTA firmware update. Access must be enabled at http://firmware.salicru.com and tomqtt.2030.ltsapis.google.

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

6.2.2. Integrated connectivity via WiFi device.

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

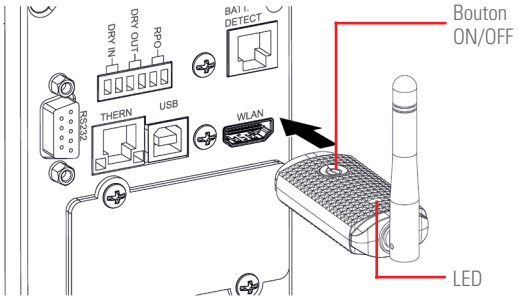


Fig. 88. WiFi device connection.

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 can enter the WiFi network credentials.

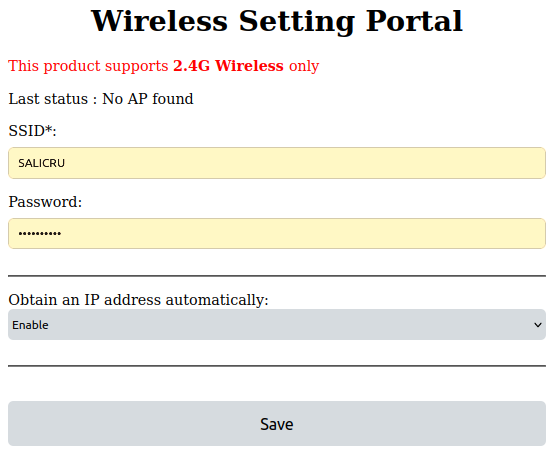


Fig. 89. WiFi configuration portal.

You may need to click on the "Advanced >. Continue on "unsafe site" the first time you enter the web page.

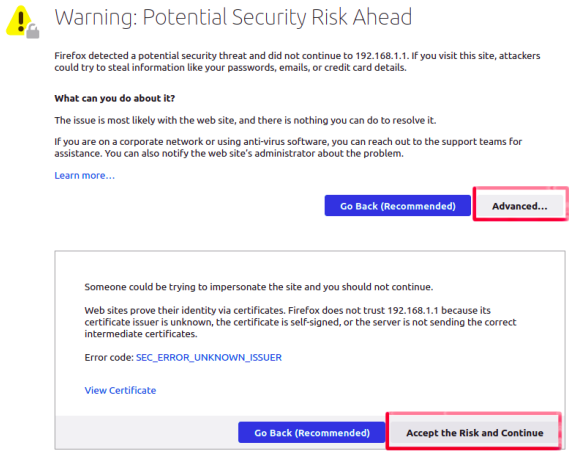


Fig. 90. Security warning.

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

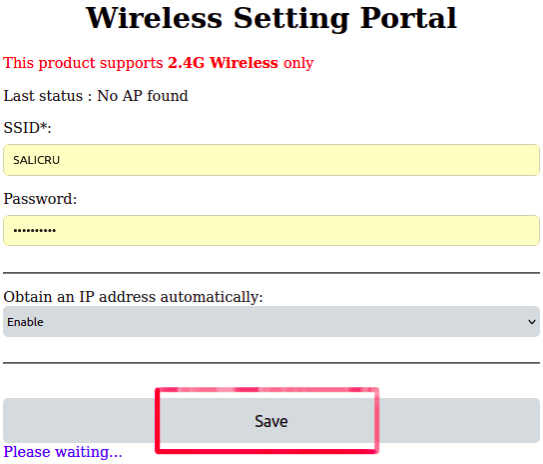


Fig. 91. Saved from WiFi settings.

Important: There are the following WiFi network limitations that must be considered to achieve a successful connection:

- The WiFi name (SSID) must contain only numbers and letters. Special characters are not supported.
- Public WLAN networks that require a second authentication are not supported. 5GB WiFi routers are not supported.
- 5GB WiFi routers are not supported.
- Some WLAN networks that need to enable special functions like "MAC whitelist" will require that extra step.

6. Finally, make sure to enable the integrated IoT service of the UPS through the screen in order 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, review the following board.

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

Tab. 8. LED states and actions to take.

EN

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

6.3.1. 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. 92. Main login screen on the remote maintenance panel.

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

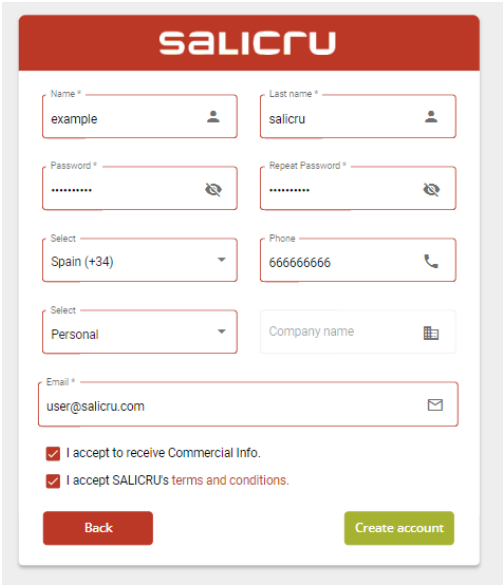


Fig. 93. User registration screen.

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.

6.3.2. 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.

6.3.2.1. 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.

6.3.2.2. 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.

6.3.3. 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.

6.3.3.1. 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.

6.3.3.2. 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.

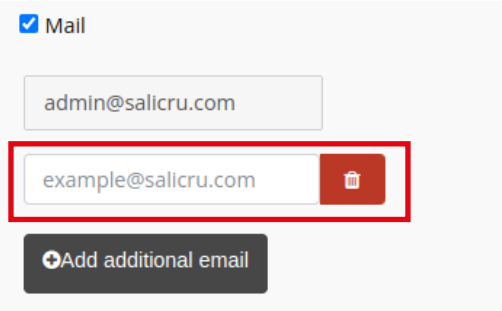


Fig. 94. Add an extra email address.

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

6.3.3.3. 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.

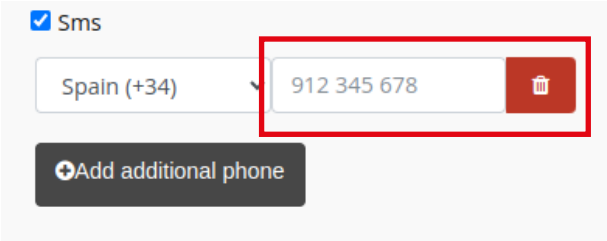


Fig. 95. Add another phone number.

6.3.4. 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.

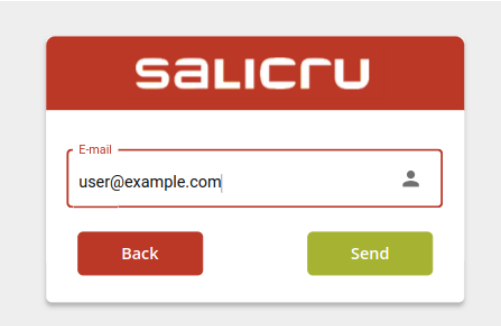


Fig. 96. Lost password recovery page.

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.

EN

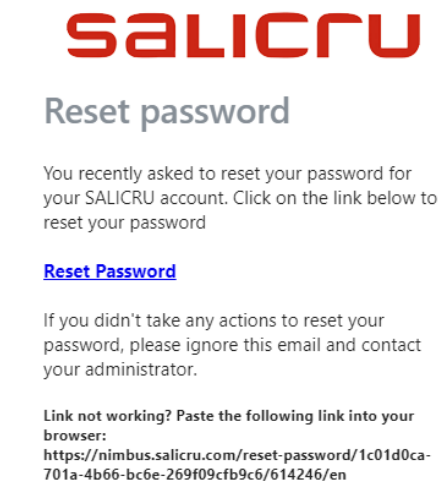


Fig. 97. Restore password.

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.

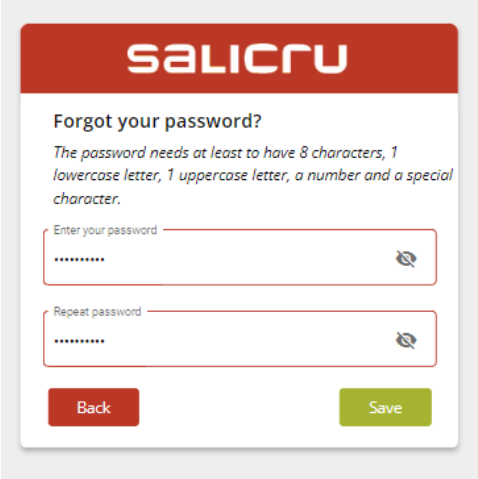


Fig. 98. Save changes.

7. ANNEX II. CARD UPDATE PROCEDURE.

7.1. NECESSARY MATERIAL.

- MicroSD card of 8 GB or higher.
- SD or MicroSD adapter and peripheral on the computer to read SD cards.
- Balena Etcher software (balenaEtcher - Flash OS images to SD cards & USB drives), Win 32 disk Imager (https://sourceforge.net/projects/win32diskimager/files/latest/download) or similar.

7.2. PERFORM A BACKUP OF THE CARD CONFIGURATION.

1. Connect to the embedded panel of the card with the "engineer" user.
2. Expand the "System" section and select the last tab "Reset settings."

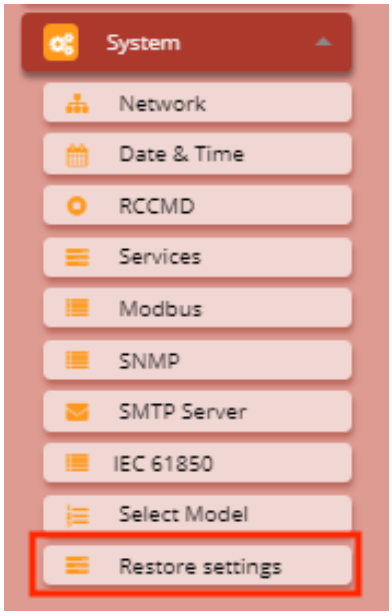


Fig. 99. Reset settings.

3. Click the "Export" button to download the current card configuration. This includes network configurations (the IP will be maintained), as well as services (threshold configurations, alarms, SNMP server, RCCMD, Modbus, ...).

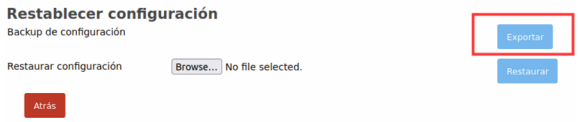


Fig. 100.Export in Reset Settings.

4. Save the document for use after the update.

7.3. UPDATE PROCEDURE.

1. Download the latest firmware version.
2. Connect the SD Adapter or the MicroSD card directly to the computer. Wait to receive confirmation that the card has been read correctly.
3. Open the downloaded program to flash the firmware to the card.
4. Load the firmware into the program and start burning it to the card. The procedure may take a few minutes.
5. Once finished, carefully remove the card. Insert the microSD card into the NIMBUS card, right into the corresponding "microSD Connector" slot (see Tab. 1).
6. For a nimbus MAXI:
   a. Power the card by inserting it back into the UPS or by connecting a USB cable between the computer and the card in the "COM1 Port" slot (see Table 1). Once powered, the "Power LEDs" will begin a flash sequence from left to right and vice versa. This procedure may take about 10 minutes.
   b. When this procedure is finished, the LEDs will turn off. Remove power from the NIMBUS card and then remove the microSD from the slot. The microSD will no longer be necessary.
   c. Insert the NIMBUS card back into the corresponding UPS and start the configuration again.
7. For a nimbus MINI:
   a. Once the micro SD card is inserted, the NIMBUS card can be connected to the UPS again. No recording procedure will be necessary.
   b. Reset settings.

7.4. BACKUP LOADING PROCEDURE.

If a backup of the card parameters has previously been made, reload them once the update has been completed. To do this, perform the following steps:

1. Connect to the point-to-point card (see section 2.1.1. Point-to-point connection (Ethernet cable)) and access the panel with the "engineer" user.
2. Expand the "System" section and select the last tab "Reset settings."
3. Load the backup, previously downloaded, by using the "Browse" button. When it is loaded, apply it using the "Restore" button.

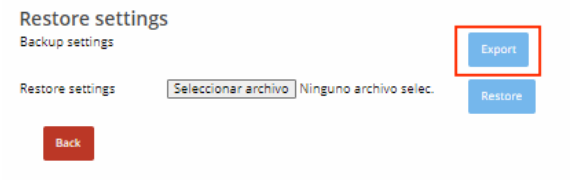


Fig. 101. Reset settings.

EN

4. Once applied, a page like the following will appear, meaning that the changes are being applied. The procedure may take about 5 minutes.

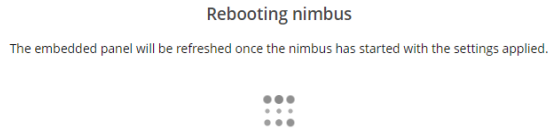


Fig. 102. Nimbus reset screen.

5. Once it has been restarted, the NIMBUS card will be fully operational and with the latest updated version.

8. APPENDIX II. GENERAL TECHNICAL SPECIFICATIONS.

In the *Tab. 9* 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. 9. Technical specifications of the NIMBUS card.

REF. EL139Q01 REV. Q CODE 401*

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)
Solar inverters
Variable frequency drives
DC systems
Transformers and Autotransformers
Voltage Stabilisers
Protective Power Strips
Batteries