



Acceso VPN mediante Secure Cloud V3 y FL MGUARD 2102

Phoenix Contact

23 de Octubre de 2024

Contenido

1 Crear Cuenta en Secure..... 3

2 Acceso a la Cuenta de Secure Cloud 5

3 Descarga e instalación del cliente OpenVPN 5

4 Esquema 7

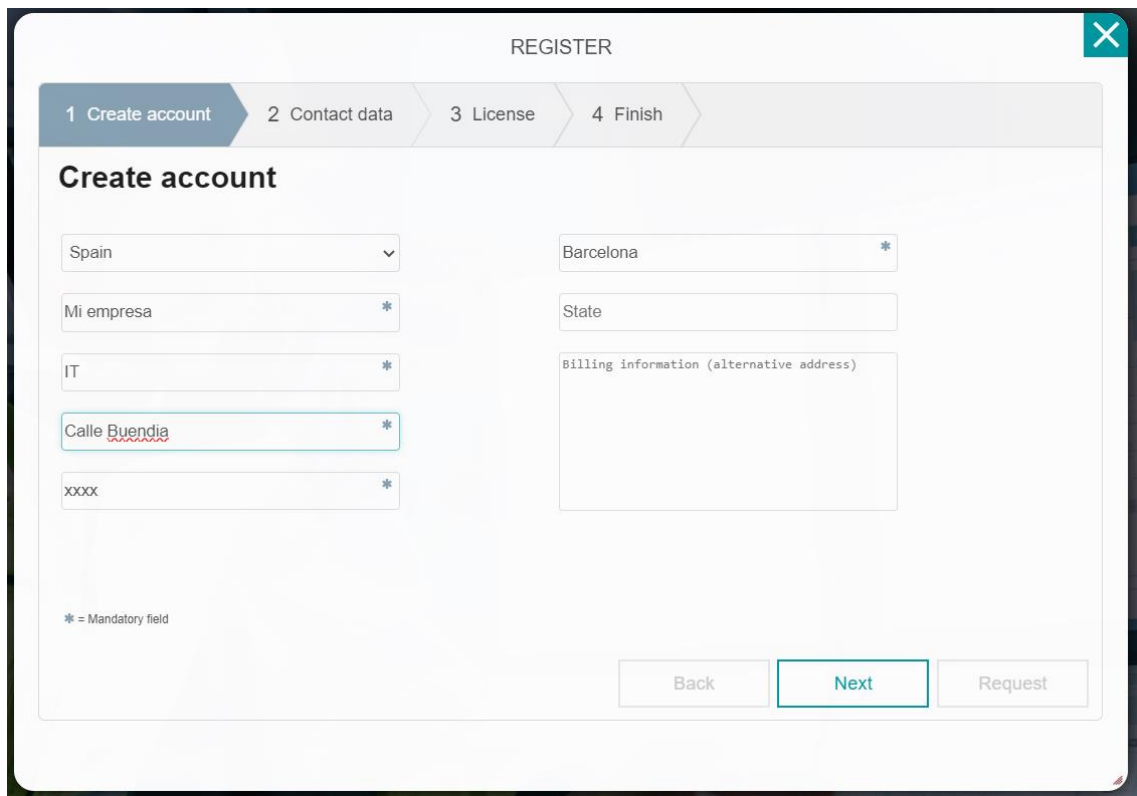
5 Generación e instalación fichero configuración lado router 7

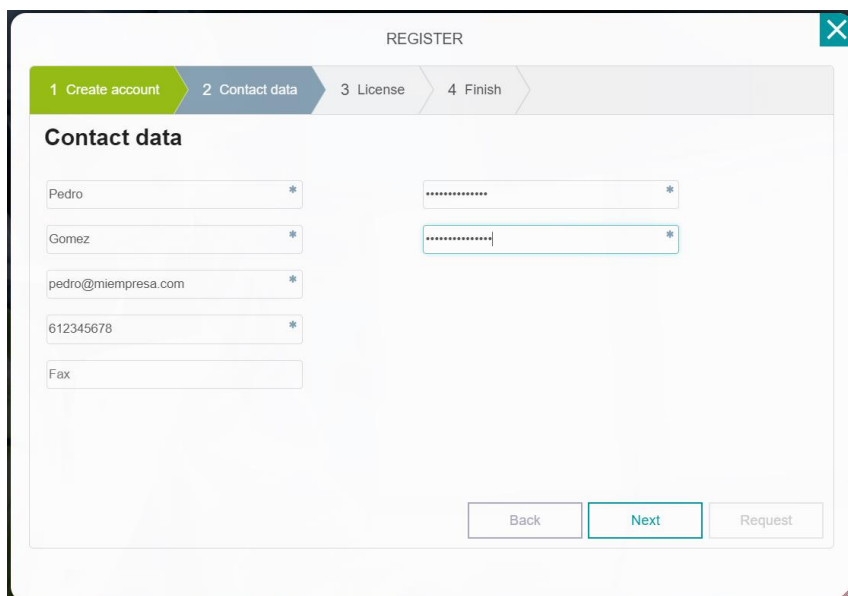
6 Generación e instalación de fichero configuración lado cliente VPN 14

1 Crear Cuenta en Secure

Para crear una Cuenta de empresa hay que entrar en la siguiente URL y registrarse:

<https://secure.phoenixcontact.cloud/>

The image shows a 'REGISTER' form with a progress bar at the top indicating four steps: 1 Create account, 2 Contact data, 3 License, and 4 Finish. The first step, 'Create account', is active. The form contains several input fields: a dropdown for 'Spain', a text field for 'Barcelona', a text field for 'Mi empresa', a text field for 'IT', a text field for 'Calle Buendia', and a text field for 'XXXX'. There is also a text field for 'State' and a larger text area for 'Billing information (alternative address)'. A legend at the bottom left indicates that '*' denotes a mandatory field. At the bottom right, there are three buttons: 'Back', 'Next', and 'Request'. The 'Next' button is highlighted with a blue border.



REGISTER

1 Create account 2 Contact data 3 License 4 Finish

Contact data

Pedro *

Gomez *

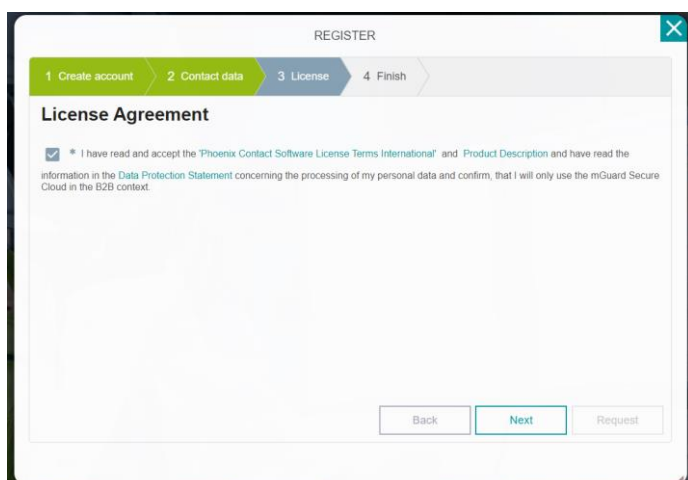
pedro@miempresa.com *

612345678 *

Fax

Back Next Request

La dirección de correo electrónico debe ser corporativa, no se admiten direcciones del tipo gmail, Hotmail, etc.



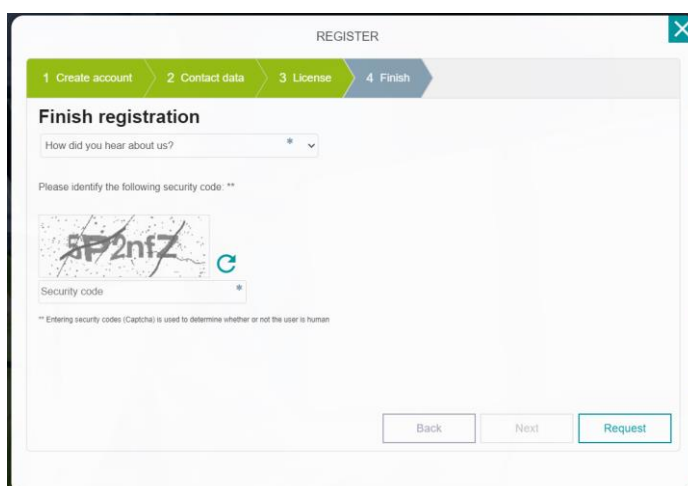
REGISTER

1 Create account 2 Contact data 3 License 4 Finish

License Agreement

☒ * I have read and accept the 'Phoenix Contact Software License Terms International' and 'Product Description' and have read the information in the Data Protection Statement concerning the processing of my personal data and confirm, that I will only use the mGuard Secure Cloud in the 52B context.

Back Next Request



REGISTER

1 Create account 2 Contact data 3 License 4 Finish

Finish registration

How did you hear about us? *

Please identify the following security code: **

Security code *

Back Next Request

Una vez terminado el proceso al presionar **Request** se recibirá un correo electrónico a la dirección facilitada con la cuenta y credenciales necesarias para poder acceder

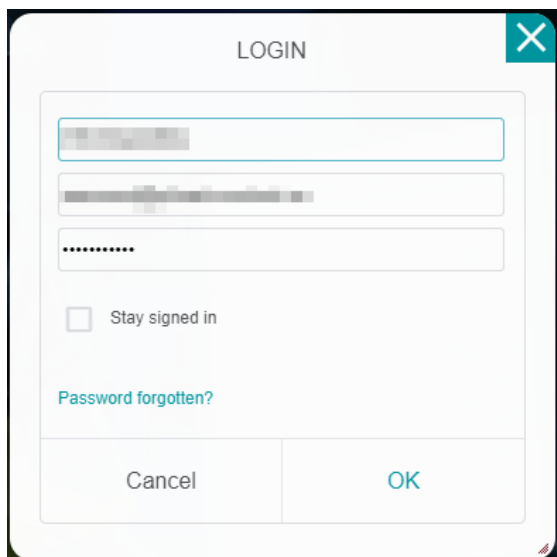
2 Acceso a la Cuenta de Secure Cloud

Para acceder a la cuenta simplemente hay que ir al apartado **LOGIN** de la URL anteriormente usada:

<https://secure.phoenixcontact.cloud/>

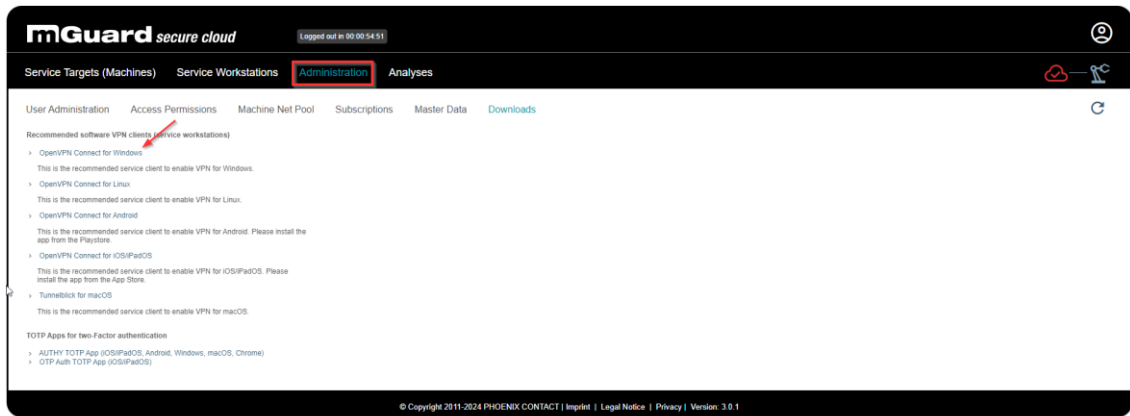


En el diálogo que aparece hay que introducir el número de cuenta recibido en el correo electrónico así como el email y password usados durante el proceso de alta. Ese email irá asociado al usuario con rol admin de la cuenta:

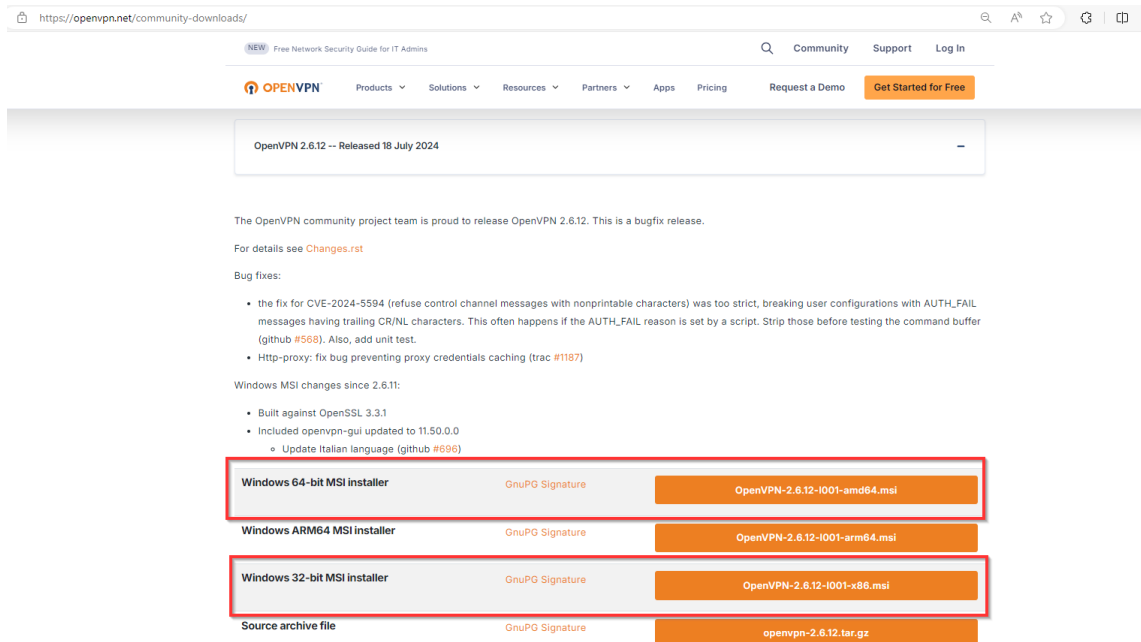


3 Descarga e instalación del cliente OpenVPN

Una vez acreditado en la cuenta de usuario, hay que acceder al apartado Administration y presionar en el enlace indicado con la flecha roja:



Dicho enlace redirige a la web del cliente OpenVPN gratuito usado:



Lo aconsejable es seleccionar la última 'release' disponible y descargar e instalar la versión para 32 o 64 bits en función de nuestro sistema operativo.

4 Esquema

En este ejemplo el esquema que se va a usar es el siguiente:



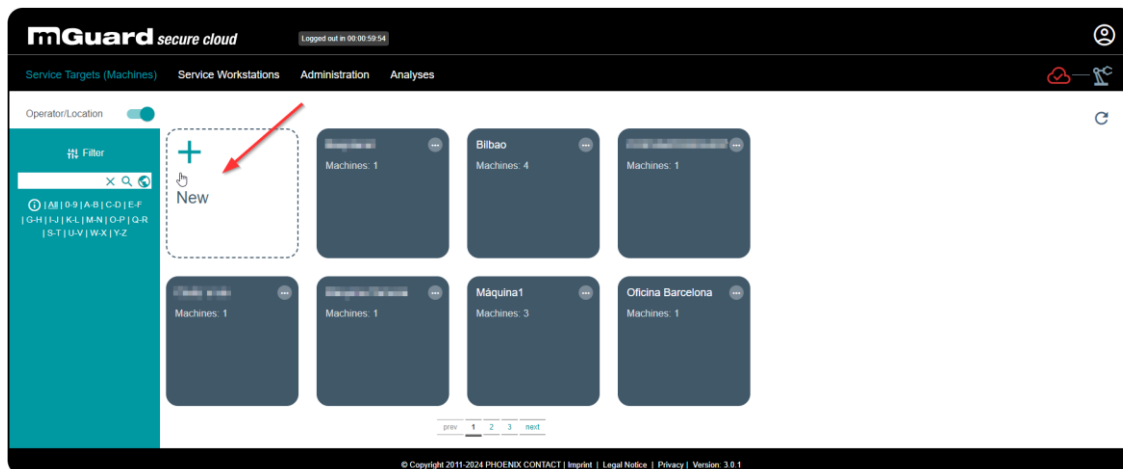
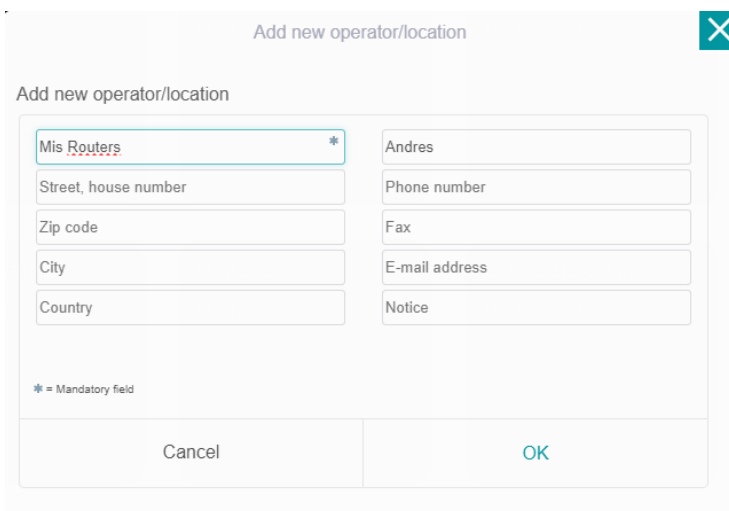
5 Generación e instalación fichero configuración lado router

Primero hay que acceder a la cuenta de usuario del Secure Cloud tal como se ha descrito en el apartado 3.



La página de entrada es la vista de VPNs activas de las máquinas que se hayan definido. Para definir nuevas hay que presionar en el 'switch' al que apunta la flecha roja.

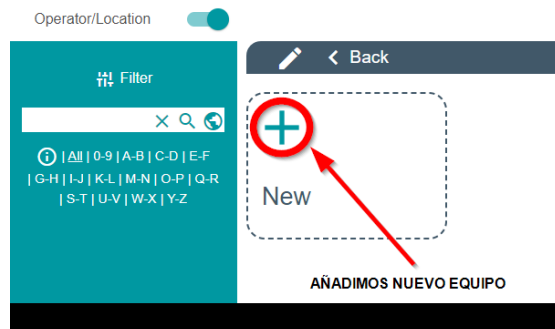
Una vez en esta nueva vista se presiona en New para crear una nueva localización u Operator:

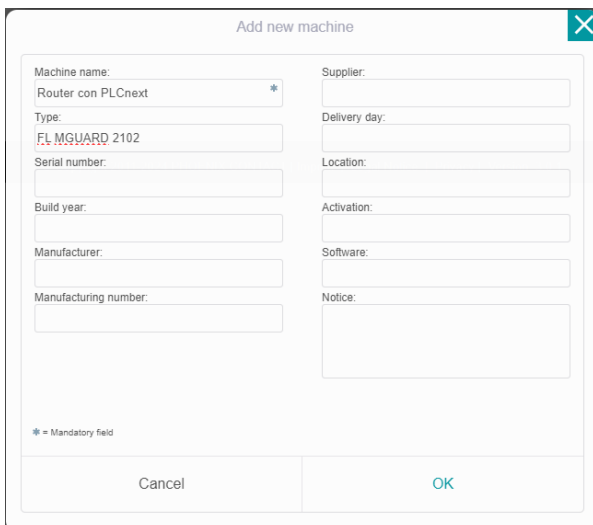
The screenshot shows the 'Add new operator/location' form. The form has a title bar with a close button. Below the title, there is a section for 'Add new operator/location'. The form contains several input fields: 'Mis Routers' (with a red asterisk), 'Andres', 'Street, house number', 'Phone number', 'Zip code', 'Fax', 'City', 'E-mail address', 'Country', and 'Notice'. A legend at the bottom left indicates that a red asterisk (*) denotes a mandatory field. At the bottom of the form, there are 'Cancel' and 'OK' buttons.

Tras aceptar hay que buscar la localización generada para comenzar a poner las máquinas o routers que queremos, en este caso el FL MGUARD 2102:

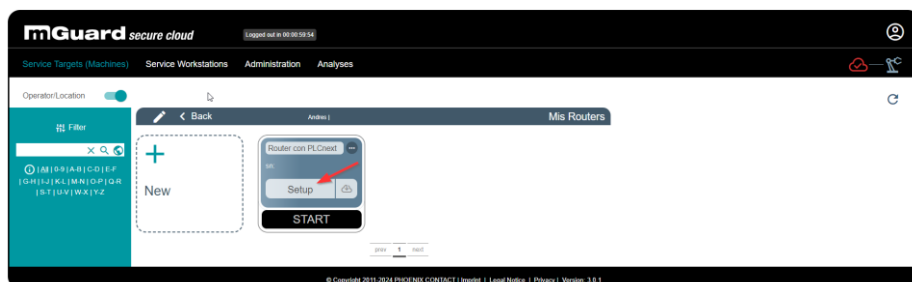
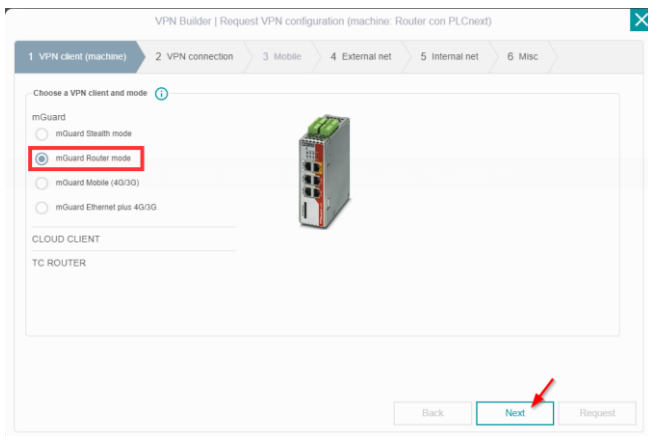




Se rellenan los valores deseados para mayor legibilidad y trazabilidad:



Al aceptar ya se puede definir la configuración (botón Setup) acorde al esquema e IPs del apartado 4:

VPN Builder | Request VPN configuration (machine: Router con PLCnext)

1 VPN client (machine) 2 VPN connection 3 Mobile 4 External net 5 Internal net 6 Misc

Proxy configuration (optional) ⓘ

Proxy IP address or hostname:

Proxy login (if necessary):

Proxy port:

Proxy password (if necessary):

Back Next Request

Si la conexión a internet va a través de un proxy, se configura aquí. Si no usamos proxy simplemente continuamos.

VPN Builder | Request VPN configuration (machine: Router con PLCnext)

1 VPN client (machine) 2 VPN connection 3 Mobile 4 External net 5 Internal net 6 Misc

DNS configuration (optional) ⓘ

IP address of DNS server (optional):

Configure MTU size ⓘ

MTU size:

Configuration external IP address ⓘ

☒ Static IP address ☐ Dynamic IP address (DHCP)

IP address (WAN port): *

Default gateway: *

* = Mandatory field

Back Next Request

Ahora debemos configurar nuestra conexión WAN, la que nos dará acceso a internet. Podemos indicar un DNS específico si fuese necesario, cambiar el tamaño de la MTU y la dirección IP que el Mguard tendrá en ese lado WAN. Puede ser dinámica, asignada por DHCP o fija. En este ejemplo la IP y máscara son fijas y las indicaremos en notación CIDR (www.xxx.yyy.zzz/ab). /24 indica una máscara de red 255.255.255.0 .

VPN Builder | Request VPN configuration (machine: Router con PLCnext)

1 VPN client (machine) 2 VPN connection 3 Mobile/WLAN 4 External net 5 Internal net 6 Misc

Configure Internal Network ⓘ

IP address (LAN port):
192.168.0.1/24 *

External Network:
Dynamic (DHCP)
or static IP

Internal network:
e.g. 192.168.1.10/24

WAN port

LAN port

Machine network:

Machine

Back Next Request

Se indica IP local del router, de nuevo en notación CIDR. Esta será la red de la máquina o sistema al que nos queremos conectar de forma remota.

VPN Builder | Request VPN configuration (machine: Router con PLCnext)

1 VPN client (machine) 2 VPN connection 3 Mobile 4 External net 5 Internal net 6 Misc

Choose the format of the VPN configuration for your machine connection ⓘ

Format of the mGuard configuration file:
.atv

Please enter the serial number of the VPN client (optional)

Serial Number:

Shall the vpn connection be initiated via a key switch (Service-IO)?

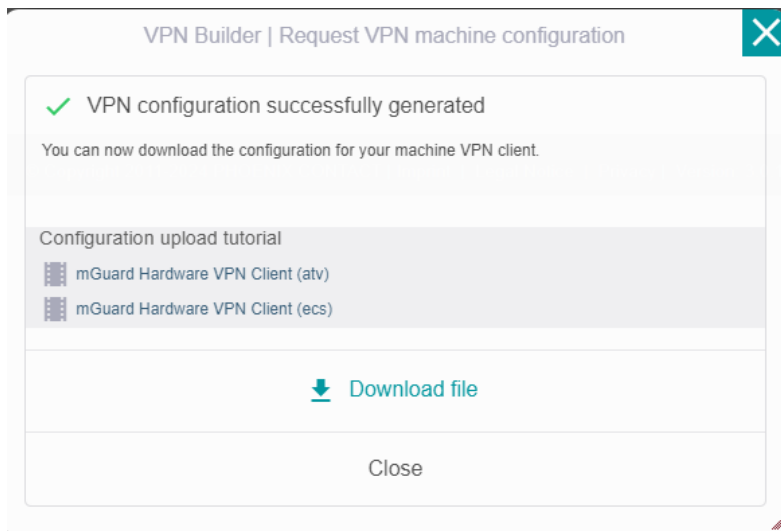
Use key switch:
No

Notify me when machine status changes (optional)

Email:

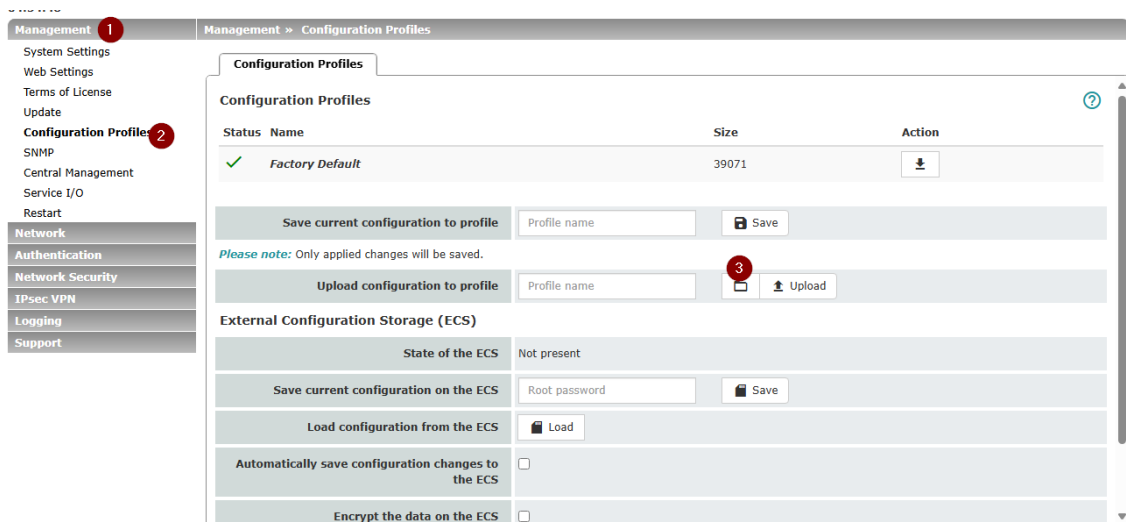
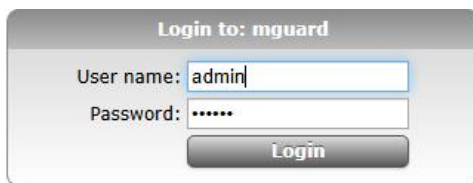
Back Next Request

Dejamos el formato tal como viene, podemos incluir el número de serie del FL MGUARD 2102 si así lo queremos, así como configurar si la VPN se activará siempre o cuando una de las entradas del equipo esté ON. También podemos indicar un correo electrónico al que se notificará cada vez que el FL MGUARD 2102 se conecte con la Secure Cloud. Ninguno de estos campos es obligatorio.

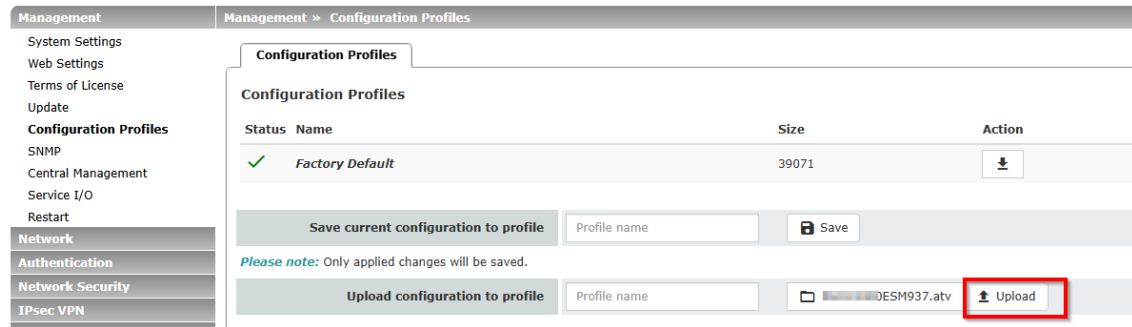
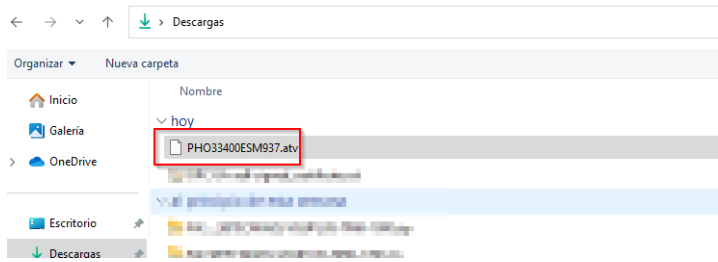


Podemos ahora descargarnos la configuración que acabamos de crear.

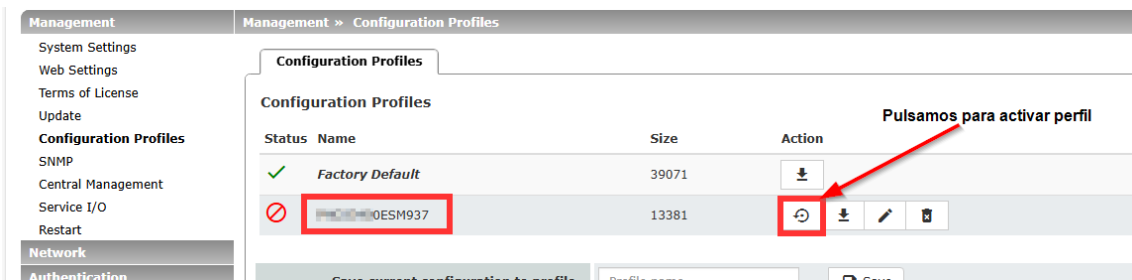
A continuación, hay que acceder al equipo con cualquier navegador a través de su puerto local (XF2) y con la IP que tenga actualmente. Por defecto es la 192.168.1 (<https://192.168.1.1>), y las credenciales, usuario 'admin' y contraseña 'mGuard':



Accedemos a Management → Configuration Profiles → Upload configuration to profile y pulsando el botón de la carpeta seleccionamos la configuración que acabamos de generar en la nube.

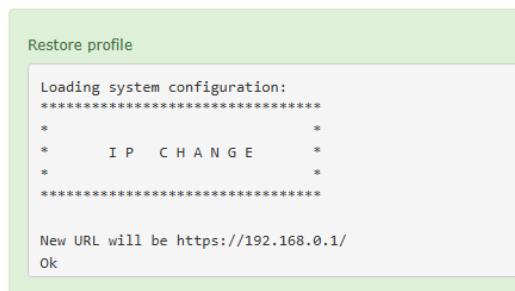


Pulsamos Upload para terminar de cargar la configuración:



El nuevo perfil que hemos cargado aparece en la lista de los disponibles. Debemos activarlo.

Como el FL MGUARD 2102 partía de la ip por defecto 192.168.1.1 y en nuestro perfil que hemos creado en la nube le hemos dicho que la parte LAN tendrá la 192.168.0.1, nos avisa de que se produce este cambio y ahora el equipo ya no será accesible en la IP antigua.



Transcurrido un momento ya el equipo no es accesible con la IP anterior y se debe acceder con la nueva IP local indicada, en este caso la 192.168.0.1.

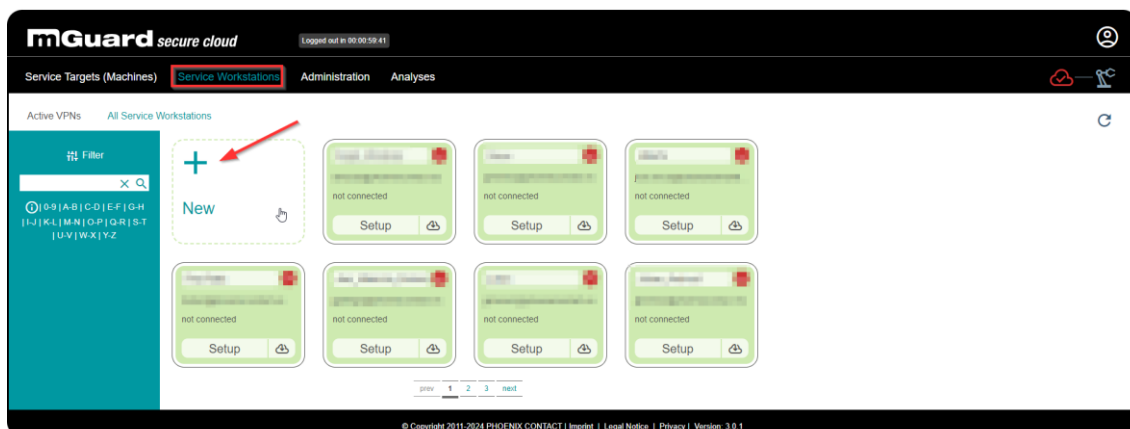
Para asegurarse que el túnel VPN entre router y Secure Cloud está establecido se accede a nuestra cuenta de Secure Cloud y se observan las VPNs activas:



Aún no se puede iniciar la conexión extremo a extremo porque falta el túnel de estación de servicio o PC a la Secure Cloud. Se verá en el siguiente apartado.

6 Generación e instalación de fichero configuración lado cliente VPN

Dentro de la Secure Cloud se accede al apartado **Service Workstations** y se crea una nueva estación de trabajo:



Add new service workstation

Add new service workstation

mi_PC *

Notice

* = Mandatory field

Cancel

OK

Una vez creada se accede a Setup y siguen los pasos descritos:

Active VPNs
All Service Workstations

Filter

0-9 | A-B | C-D | E-F | G-H | I-J | K-L | M-N | O-P | Q-R | S-T | U-V | W-X | Y-Z

+

New

mi_PC
not connected
Setup

not connected
Setup

nueva
no user
not connected
Setup

not connected
Setup

not connected
Setup

not connected
Setup

not connected
Setup

prev 1 2 3 next

VPN Builder | Request VPN configuration (service: mi_PC)

1 VPN client (service) 2 VPN User 3 Machine network

Choose a VPN client mode

In which mode would you like to use OpenVPN? Choose 'TUN' mode to connect on layer 3. Choose TAP mode to connect on layer 2. Note that TAP connections are not supported in Android and iOS/iPadOS.

☒ OpenVPN TUN Mode

☐ OpenVPN TAP Mode

Choose operating system

Windows

Please enter the client password

Password: *

Repeat password: *

* = Mandatory field: Passwords must be at least 8 characters long and should contain letters, numbers and special characters.

Back Next Request

Se selecciona el modo TUN y se genera contraseña para establecer el túnel VPN contra la Secure Cloud

VPN Builder | Request VPN configuration (service: mi_PC)

1 VPN client (service) 2 VPN User 3 Machine network

Choose the service user

Back Next Request

Selección del usuario de la cuenta que utilizará este acceso.

VPN Builder | Request VPN configuration (service: mi_PC)

1 VPN client (service) 2 VPN User 3 Machine network

Configure machine network ⓘ

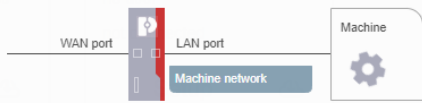
Machine network
192.168.0.0/24 *

Additional Reachable Subnets

Proxy configuration (optional) ⓘ

☒ No Proxy ☐ HTTP Proxy

Back Next Request



Se indica el rango de IPs local de la máquina a la que queremos acceder, incluyendo la máscara de subred en formato CIDR.

VPN Builder | Request service VPN configuration

✓ VPN configuration successfully generated

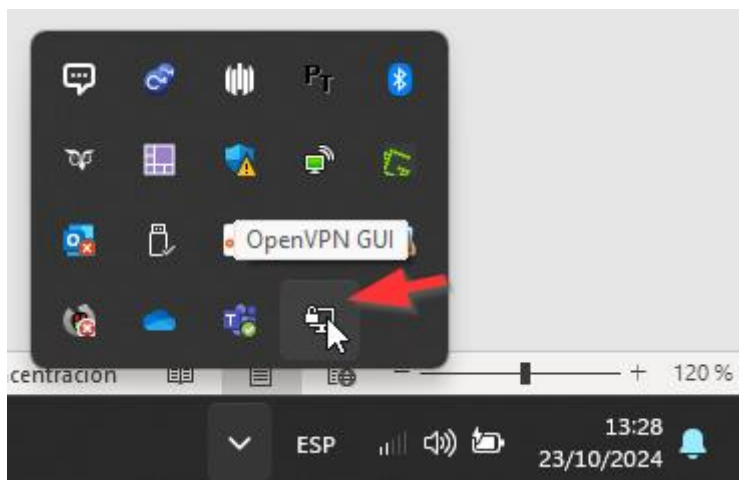
You can now download the configuration for your Service Workstation VPN client.

Download file

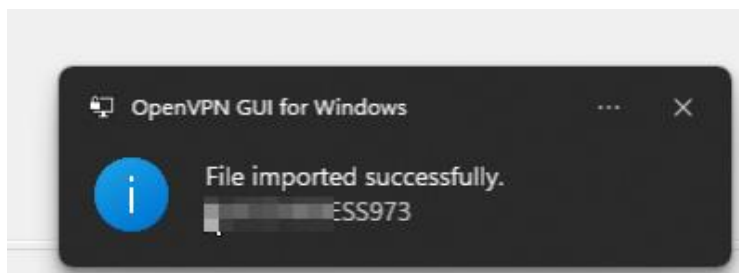
Close

Por último se descarga el fichero de configuración del cliente VPN OpenVPN GUI en formato .ovpn

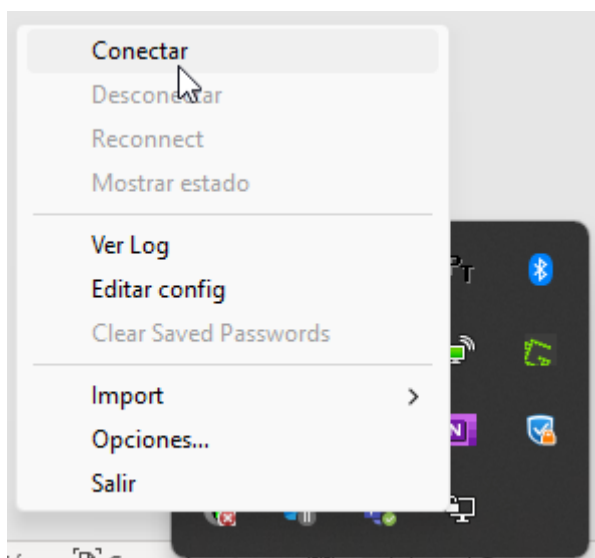
Para importar dicho fichero en el cliente VPN hay que mostrar los iconos ocultos en la barra de tareas:

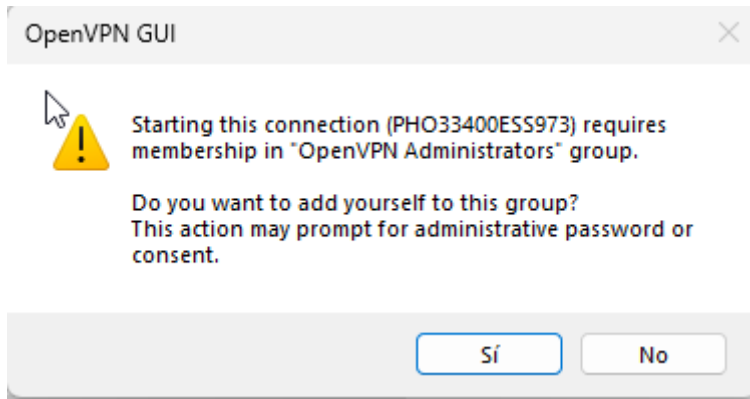


Presionando botón derecho del ratón sobre dicho icono se puede importar ficheros externos como el que se acaba de descargar de la Secure Cloud:

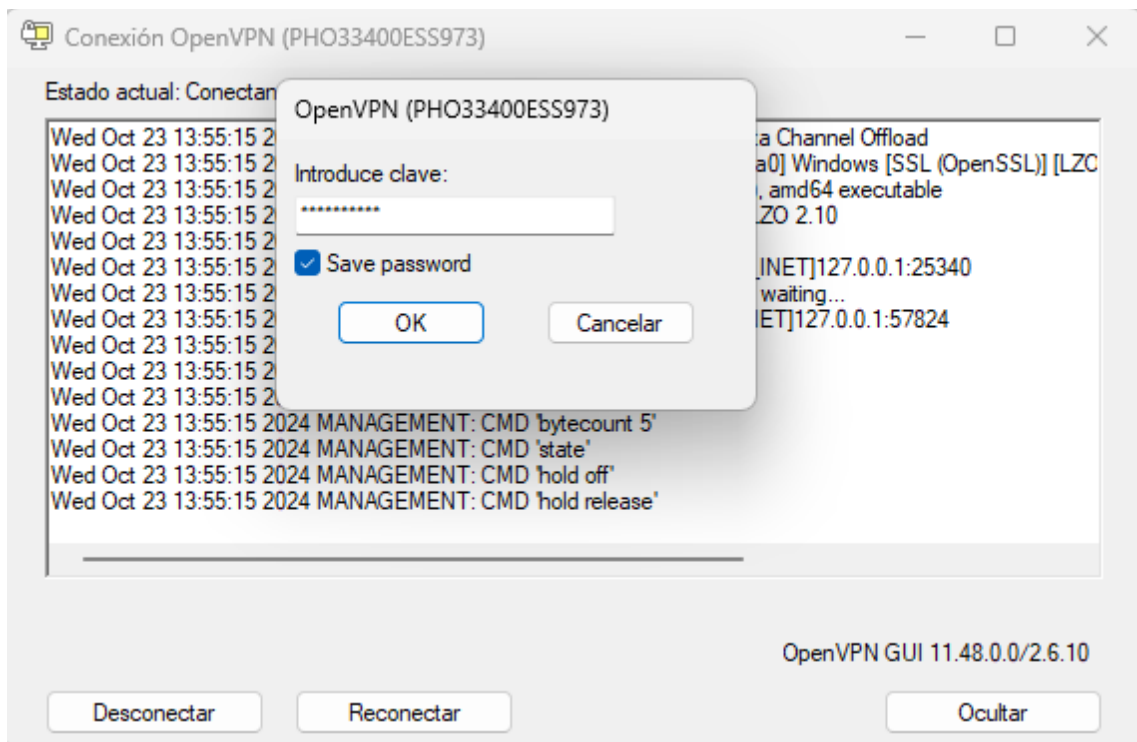


Nuevamente presionando botón derecho del ratón y **Conectar** se procede a establecer el túnel con la Secure Cloud:

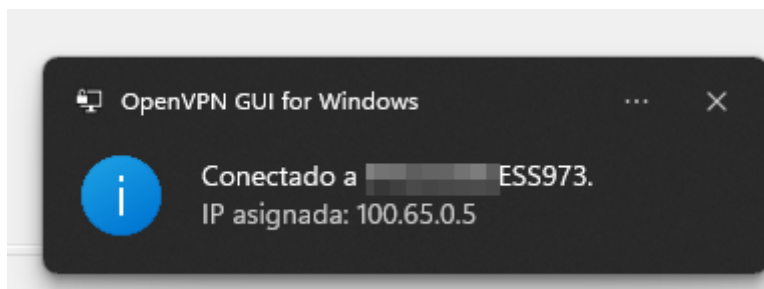




Puede aparecer este mensaje que simplemente se acepta.

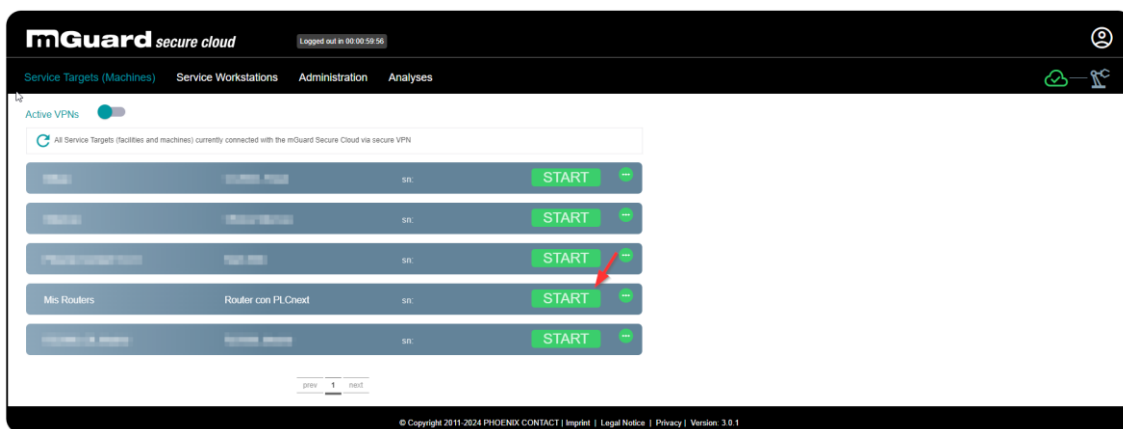


Seguidamente se solicita la contraseña introducida durante el proceso de generación del fichero de configuración del cliente VPN.

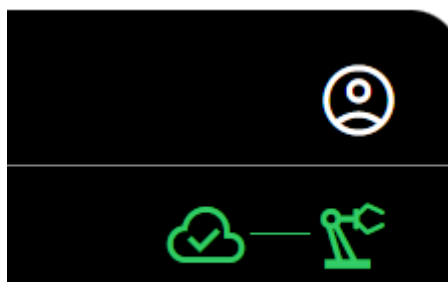


Mensaje de confirmación de túnel establecido.

Por último, para unir las dos partes del túnel hay que presionar el botón START desde la cuenta de Secure Cloud:



Fijándose en la esquina superior derecha se muestra como hay conexión extremo a extremo:



Ahora ya es posible acceder al PLC remoto con su IP local mediante ping o accediendo a su servidor web:

```

C:\Users\essa02>ping 192.168.0.12

Haciendo ping a 192.168.0.12 con 32 bytes de datos:
Respuesta desde 192.168.0.12: bytes=32 tiempo=198ms TTL=63
Respuesta desde 192.168.0.12: bytes=32 tiempo=176ms TTL=63
Respuesta desde 192.168.0.12: bytes=32 tiempo=136ms TTL=63
Respuesta desde 192.168.0.12: bytes=32 tiempo=147ms TTL=63

Estadísticas de ping para 192.168.0.12:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
            Mínimo = 136ms, Máximo = 198ms, Media = 164ms

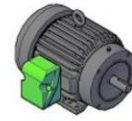
C:\Users\essa02>
    
```

SAFETY

☒ Estado seguridad

☐ Petición de rearme

Rearmar
seguridad



Izquierda

Derecha

