



Acceso VPN mediante Secure Cloud V3 y Cloud Client

Phoenix Contact

Abril de 2025

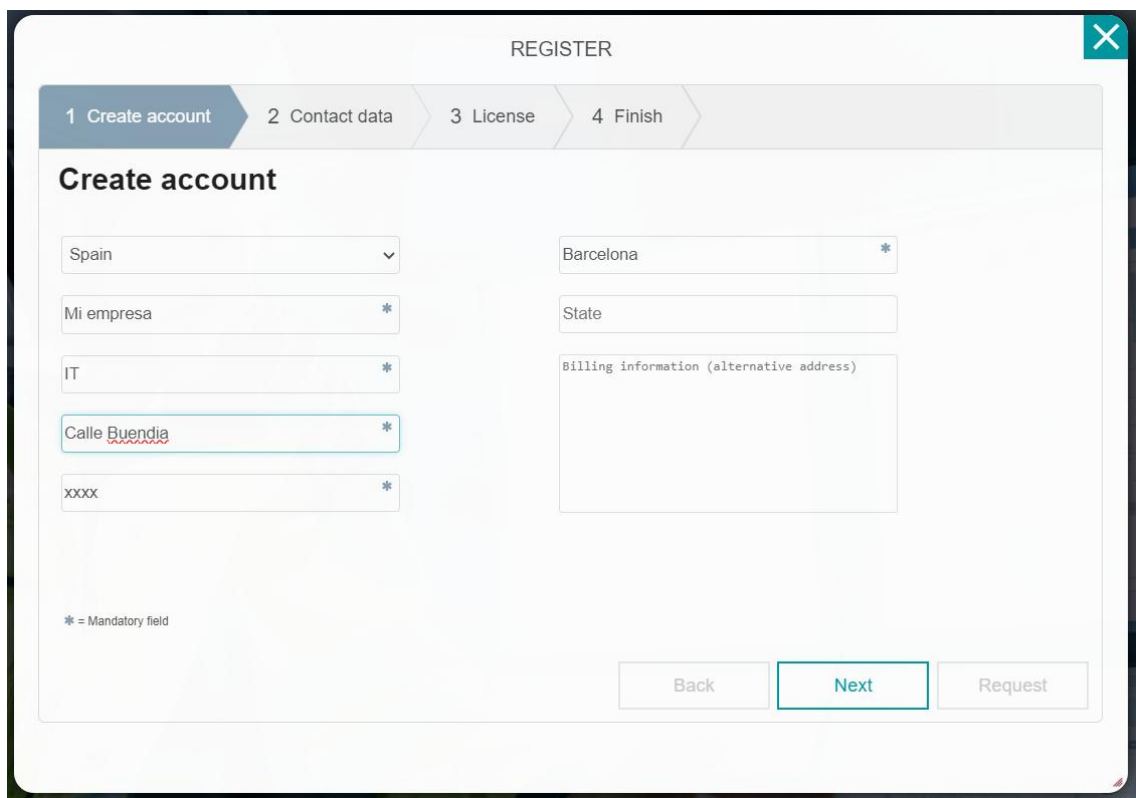
Contenido

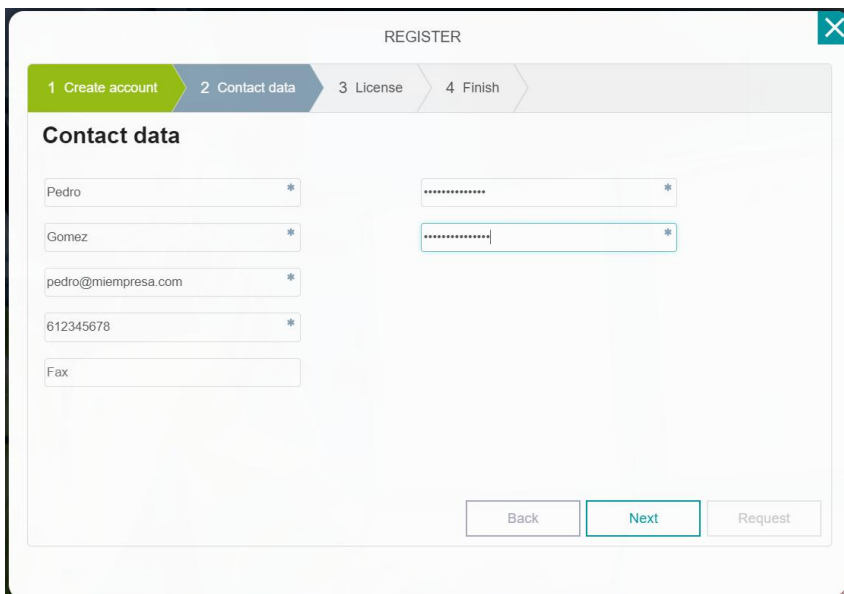
1	Crear Cuenta en Secure.....	3
2	Acceso a la Cuenta de Secure Cloud	5
3	Descarga e instalación del cliente OpenVPN	5
4	Esquema	7
5	Generación e instalación fichero configuración lado router	7
6	Generación e instalación de fichero configuración lado cliente VPN	14
	Anexo 1. Machine Net Pool.....	22

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' modal window with a progress bar at the top indicating four steps: 1 Create account, 2 Contact data, 3 License, and 4 Finish. The 'Create account' step is active. The form contains several input fields: a country dropdown set to 'Spain', a city field with 'Barcelona', a company name field 'Mi empresa', an industry field 'IT', a street address field 'Calle Buendia', and a postal code field 'XXXX'. There is also a 'State' field and a larger 'Billing information (alternative address)' text area. A legend at the bottom left states '* = Mandatory field'. At the bottom right are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Request'.



REGISTER

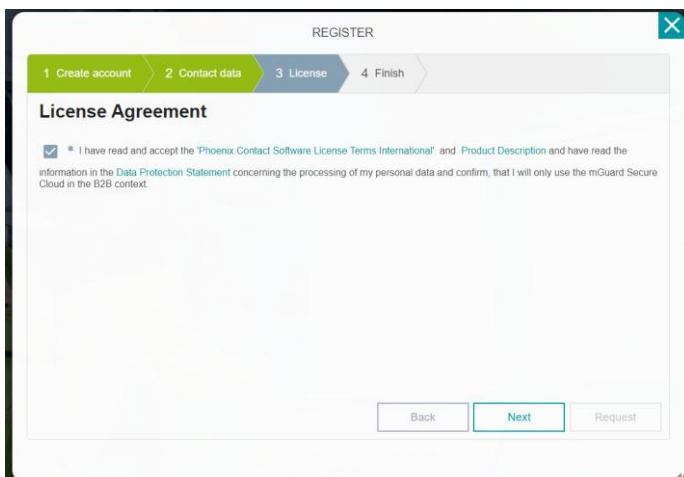
1 Create account 2 Contact data 3 License 4 Finish

Contact data

* *
 * *
 *
 *

Back Next Request

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



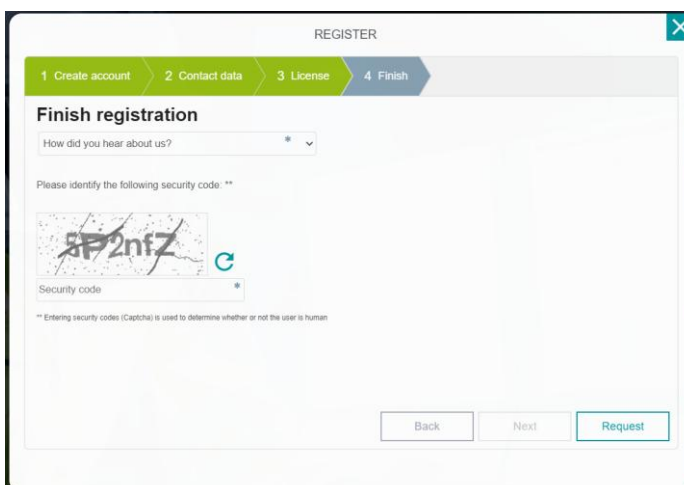
REGISTER

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: **

 *
 *

** Entering security codes (Captcha) is used to determine whether or not the user is human

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

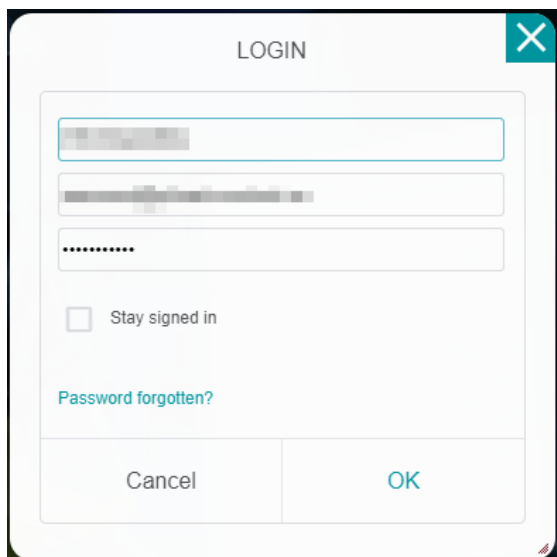
2 Acceso a la Cuenta de Secure Cloud

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

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

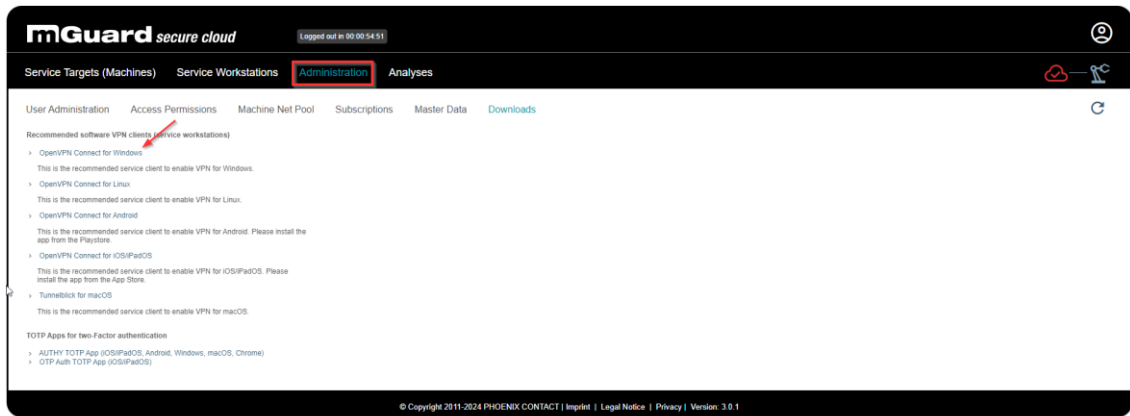


En el diálogo que aparece hay que introducir el número de cuenta recibido en el correo electrónico así como el email y password usados durante el proceso de alta. Ese email irá asociado al usuario con rol admin de la cuenta:

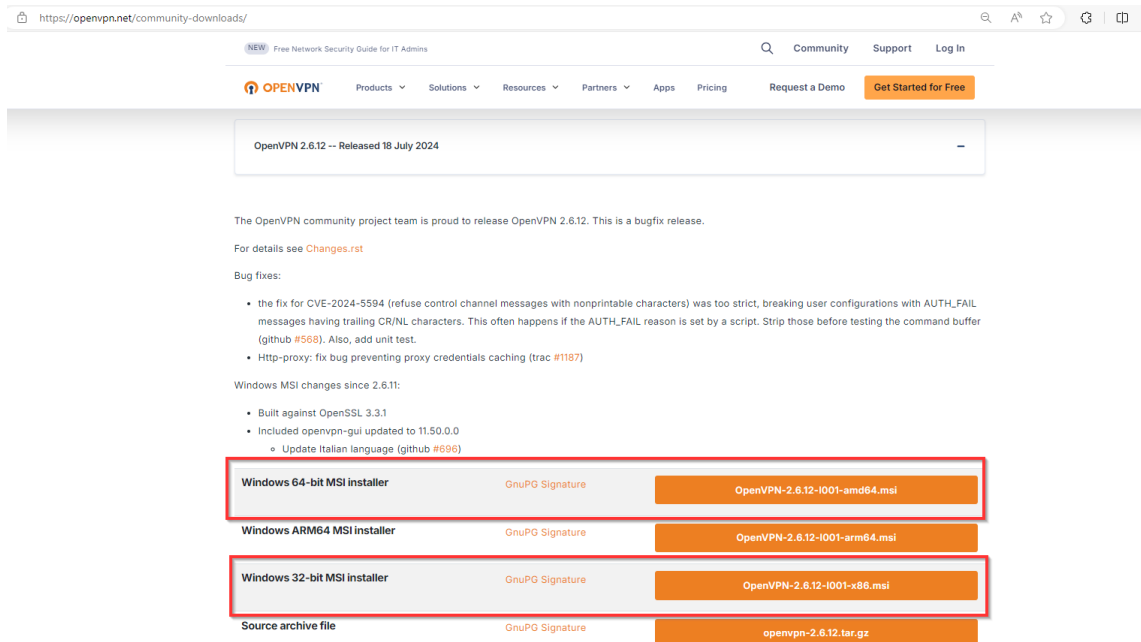


3 Descarga e instalación del cliente OpenVPN

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:



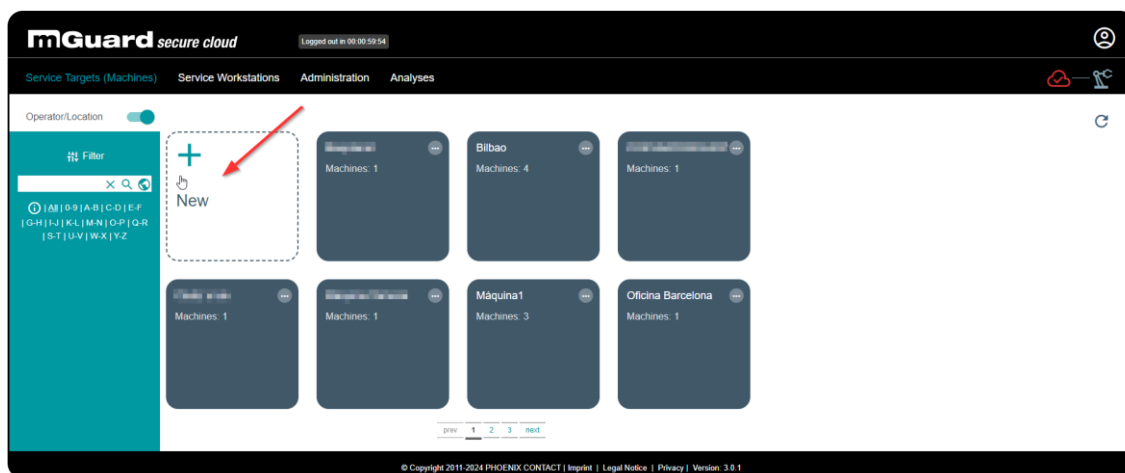
5 Generación e instalación fichero configuración lado router

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 Operador:



Add new operator/location

Add new operator/location

Mis Routers

Street, house number

Zip code

City

Country

Andres

Phone number

Fax

E-mail address

Notice

* = Mandatory field

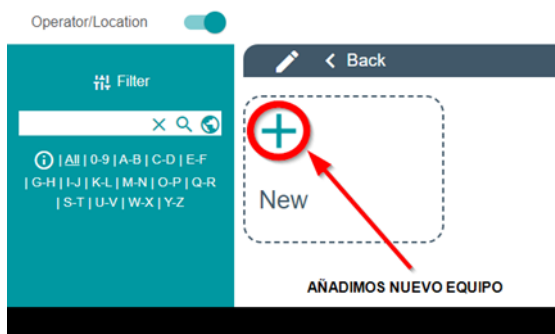
Cancel

OK

Tras aceptar hay que buscar la localización generada para comenzar a poner las máquinas o routers que queramos, en este caso el Cloud Client 1101T-TX/TX:



Se rellenan los valores deseados para mayor legibilidad y trazabilidad:



Add new machine

Machine name:
Cloud Client

Type:
Cloud Client 1101T

Serial number:

Build year:

Manufacturer:

Manufacturing number:

Supplier:

Delivery day:

Location:

Activation:

Software:

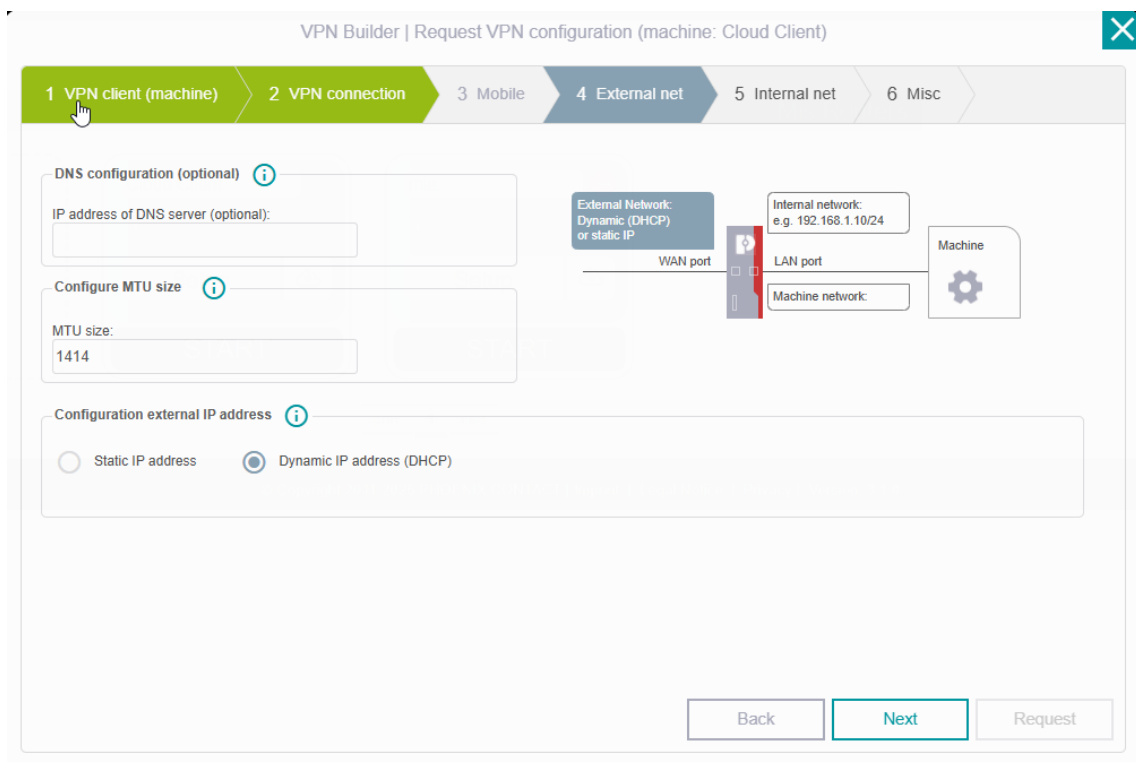
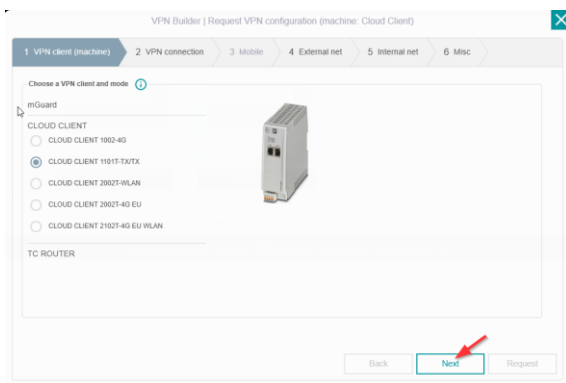
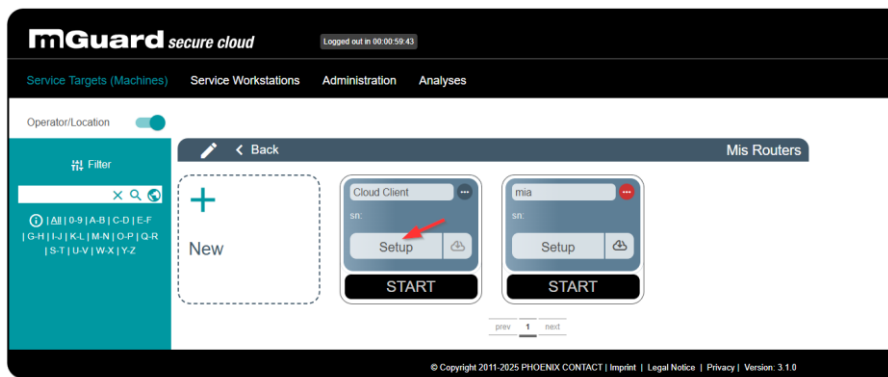
Notice:

Mandatory field

Cancel

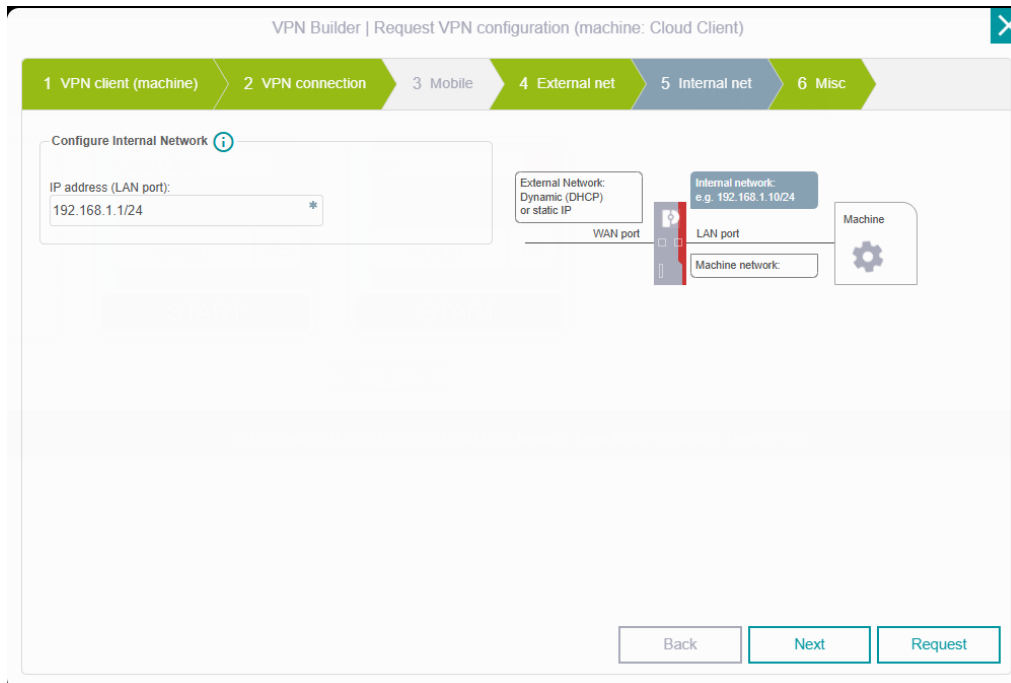
OK

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

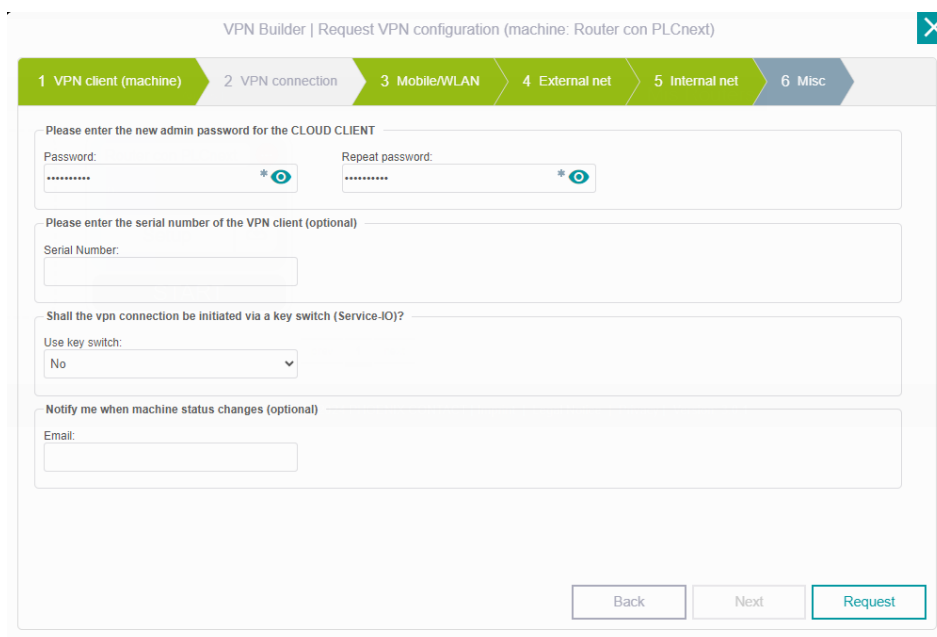


Se escoge IP externa o de lado WAN por DHCP, es decir, el router que da acceso a Internet le otorgará una IP en su rango para permitir el acceso remoto.

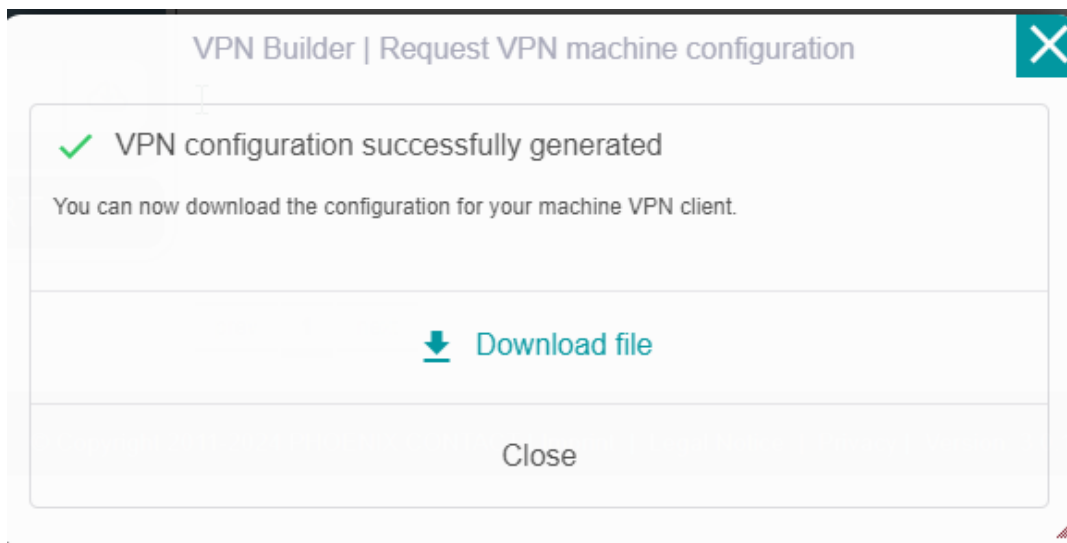
MUY IMPORTANTE, el rango WAN y LAN no pueden coincidir pues habría error de enrutado. Como ya se ha visto en el esquema de la instalación, apartado 4 de la guía, el lado WAN del Cloud Client adoptará una IP en el rango 192.168.68.x mientras que el PLC en el lado LAN opera con la IP 192.168.1.100. Al usar ambas redes máscaras 255.255.255.0, no se verán entre sí.



Se indica IP local del router y CIDR o máscara de red de dicha red local, en este caso 24 que equivale a 255.255.255.0)

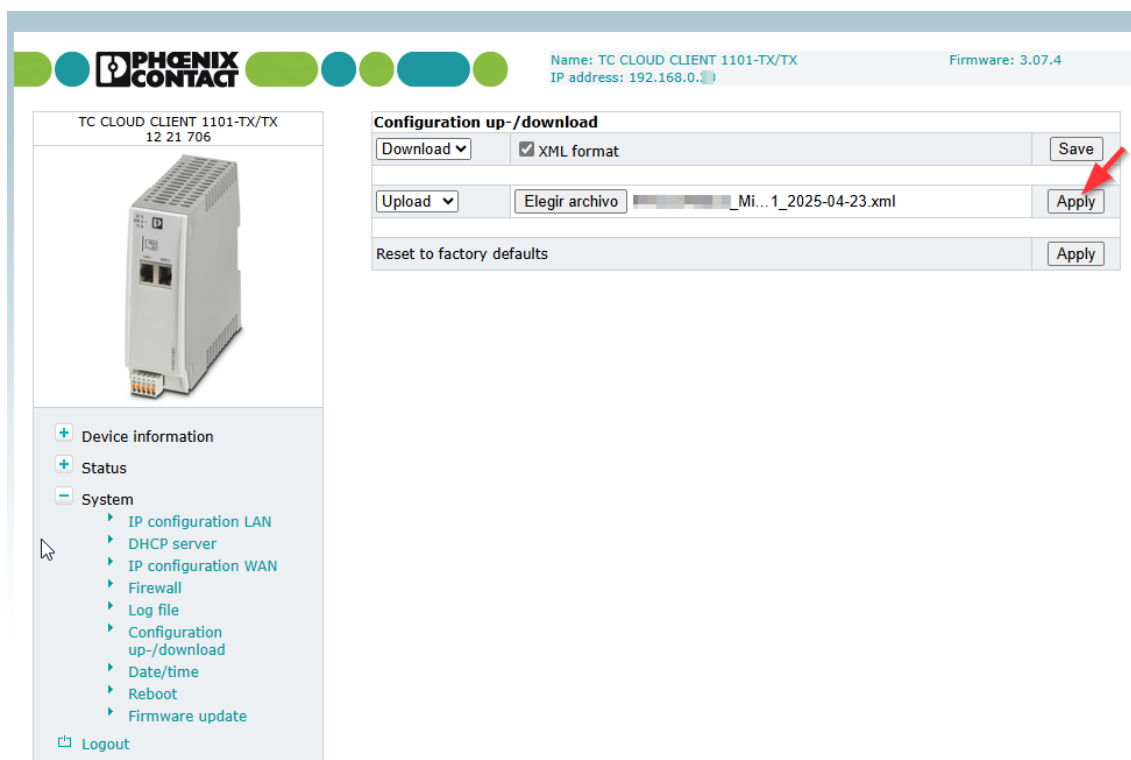


Se indica contraseña con la cual se accederá al equipo vía web.



Ahora se puede descargar la configuración del equipo en formato .xml.

A continuación hay que acceder al equipo a través de su puerto local(LAN) e IP que tenga actualmente, en el caso del ejemplo 192.168.1.1, y con las credenciales definidas, usuario 'admin' y contraseña 'admin' por defecto:



Se entra en el apartado **System** y subapartado **Configuration up-/download**. Se selecciona el fichero .xml descargado de la web Secure Cloud y se pulsa en Apply.



Name: TC CLOUD CLIENT 1101-TX/TX
IP address: 192.168.0.20

Firmware: 3.07.4

TC CLOUD CLIENT 1101-TX/TX
12 21 706

- + Device information
- + Status
- System
 - IP configuration LAN
 - DHCP server
 - IP configuration WAN
 - Firewall
 - Log file
 - Configuration up-/download
 - Date/time
 - Reboot
 - Firmware update

Logout

```
xml parsed
/tmp/cfg_import/etc/sysconf/openvpn removed
/tmp/cfg_import/etc/conf/iptables/masq_tbl removed
/tmp/cfg_import/etc/conf/iptables/nat_enable removed
/tmp/cfg_import/etc/conf/iptables/nat_fw removed
/tmp/cfg_import/etc/conf/iptables/nat_vs removed
/tmp/cfg_import/etc/conf/iptables/nat_xfrom removed
/tmp/cfg_import/etc/conf/iptables/nat_xhost removed
/tmp/cfg_import/etc/conf/iptables/nat_xlog removed
/tmp/cfg_import/etc/conf/iptables/nat_xmasq removed
/tmp/cfg_import/etc/conf/iptables/xssh removed
update /etc/conf/ipsec/vpn1/remote_id
update /etc/conf/ipsec/vpn1/remote_cert
update /etc/conf/ipsec/vpn1/remote_addr
update /etc/conf/ipsec/vpn1/pfsgroup
update /etc/conf/ipsec/vpn1/nat
update /etc/conf/ipsec/vpn1/name
update /etc/conf/ipsec/vpn1/local_cert
update /etc/conf/ipsec/vpn1/local_addr
update /etc/conf/ipsec/vpn1/leftsendcert
update /etc/conf/ipsec/vpn1/12tp
update /etc/conf/ipsec/vpn1/ike_life
update /etc/conf/ipsec/vpn1/ike_hash
update /etc/conf/ipsec/vpn1/host
update /etc/conf/ipsec/vpn1/force_encaps
update /etc/conf/ipsec/vpn1/esp_life
update /etc/conf/ipsec/vpn1/esp_hash
update /etc/conf/ipsec/vpn1/auth
update /etc/conf/iptables/xwbm
update /etc/conf/network/interface/lan/ipaddr
update /etc/conf/system/httpaccess
update /etc/conf/auth/user
update /etc/conf/auth/admin
install /etc/ipsec.d/private/L2TPv3M_5551_61.pem
install /etc/ipsec.d/ldir/L2TPv3M_5551_61.p12
install /etc/ipsec.d/certs/local/L2TPv3M_5551_61.crt
install /etc/ipsec.d/cacerts/L2TPv3M_5551_61.crt
setup new config done

please reboot next
```

A continuación solicita un Reboot para que la nueva configuración aplique, para ello hay que ir al apartado reboot o hacer un reset de tensión:

Name: TC CLOUD CLIENT 1101-TX/TX
IP address: 192.168.0.20

Firmware: 3.07.4

TC CLOUD CLIENT 1101-TX/TX
12 21 706

- + Device information
- + Status
- System
 - IP configuration LAN
 - DHCP server
 - IP configuration WAN
 - Firewall
 - Log file
 - Configuration up-/download
 - Date/time
 - Reboot
 - Firmware update

Logout

Reboot

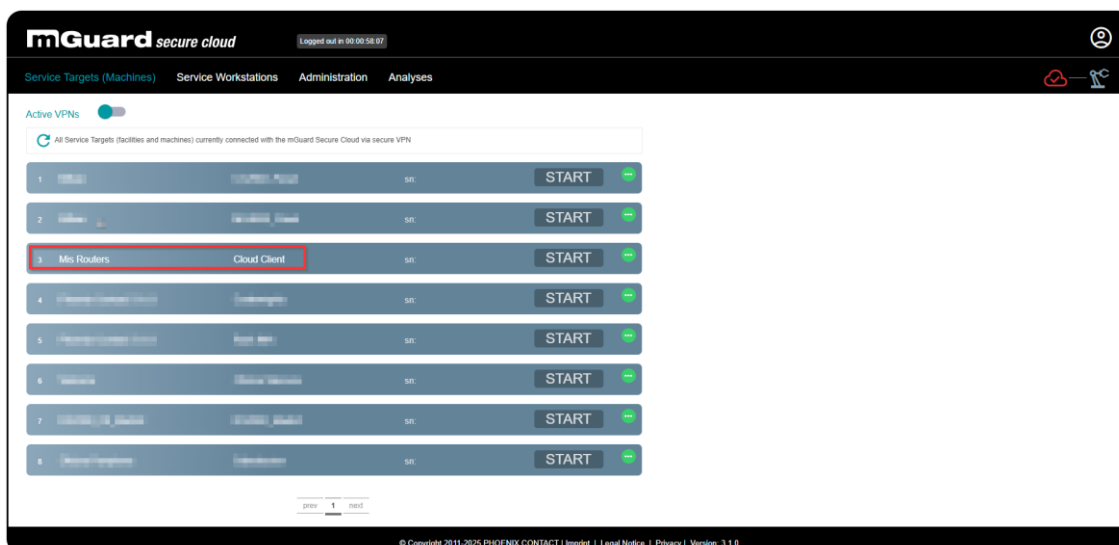
Reboot NOW!

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Daily reboot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time	01:00						

Apply

Transcurrido un momento el equipo deberá reiniciar con las configuraciones definidas y, por tanto, hay que conectar su boca WAN al router que da acceso a Internet y su boca LAN al PLC o equipo al que se quiere acceder de manera remota.

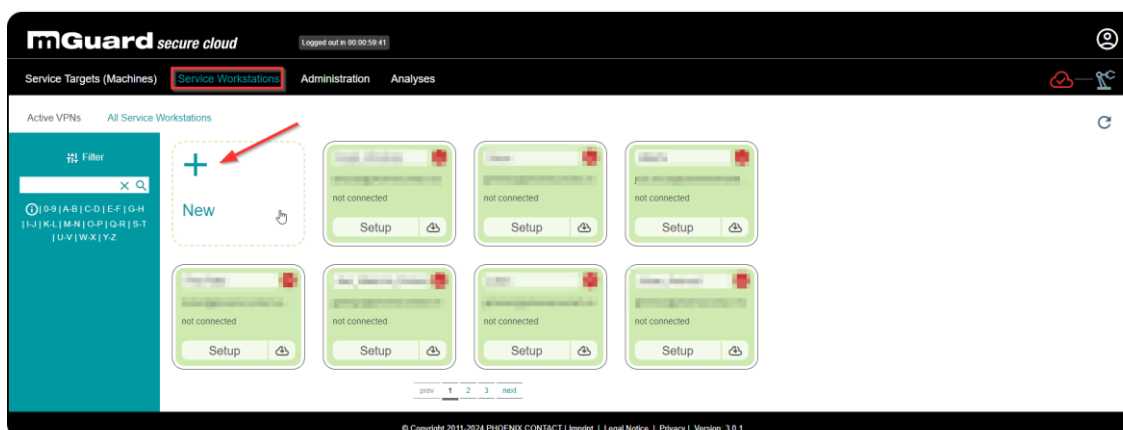
Para asegurarse que el túnel VPN entre router y Secure Cloud está establecido se accede a nuestra cuenta de Secure Cloud y se observan las VPNs activas:



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 ⓘ

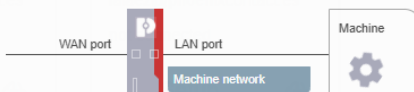
Machine network
192.168.1.0/24 *

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

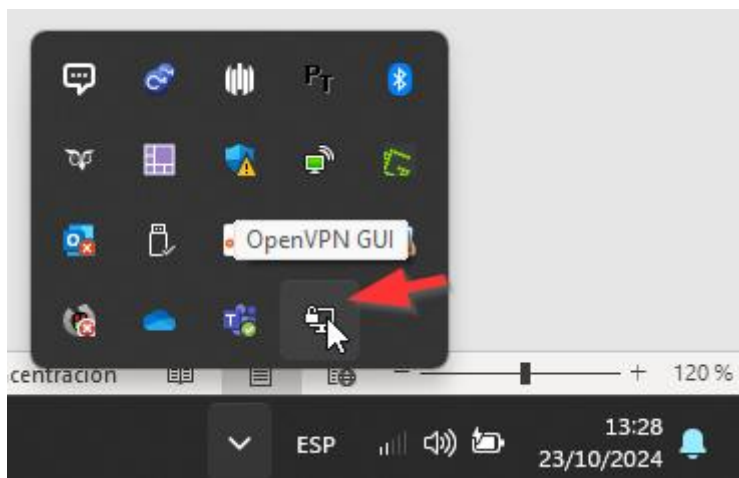
You can now download the configuration for your Service Workstation VPN client.

Download file

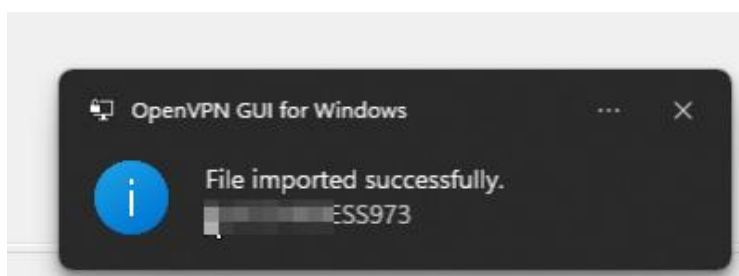
Close

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

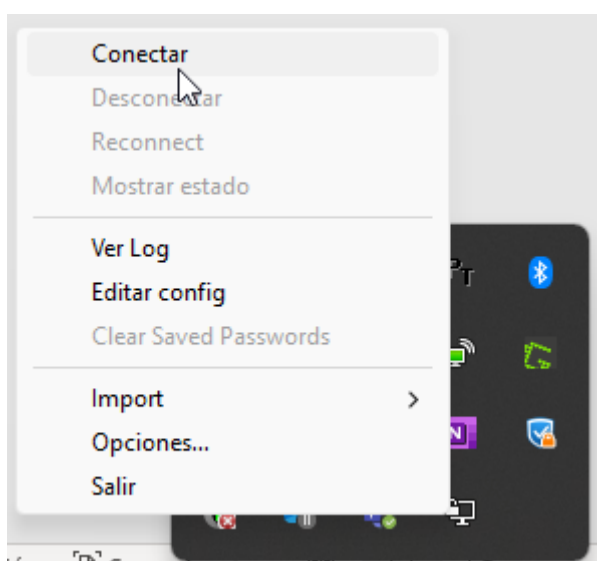
Para importar dicho fichero en el cliente VPN hay que mostrar los iconos ocultos en la barra de tareas:

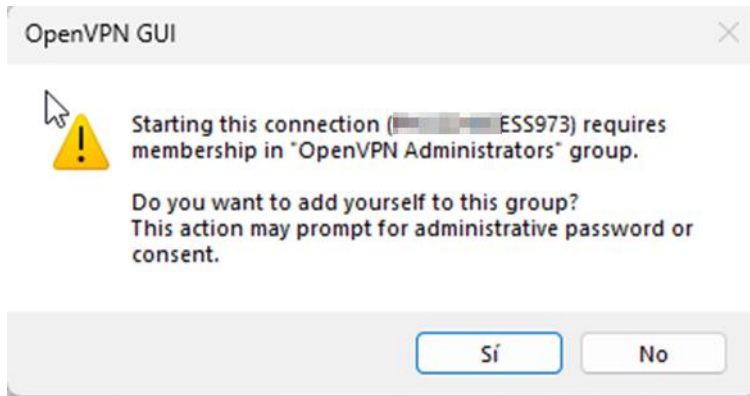


Presionando botón derecho del ratón sobre dicho icono se puede importar ficheros externos como el que se acaba de descargar de la Secure Cloud:

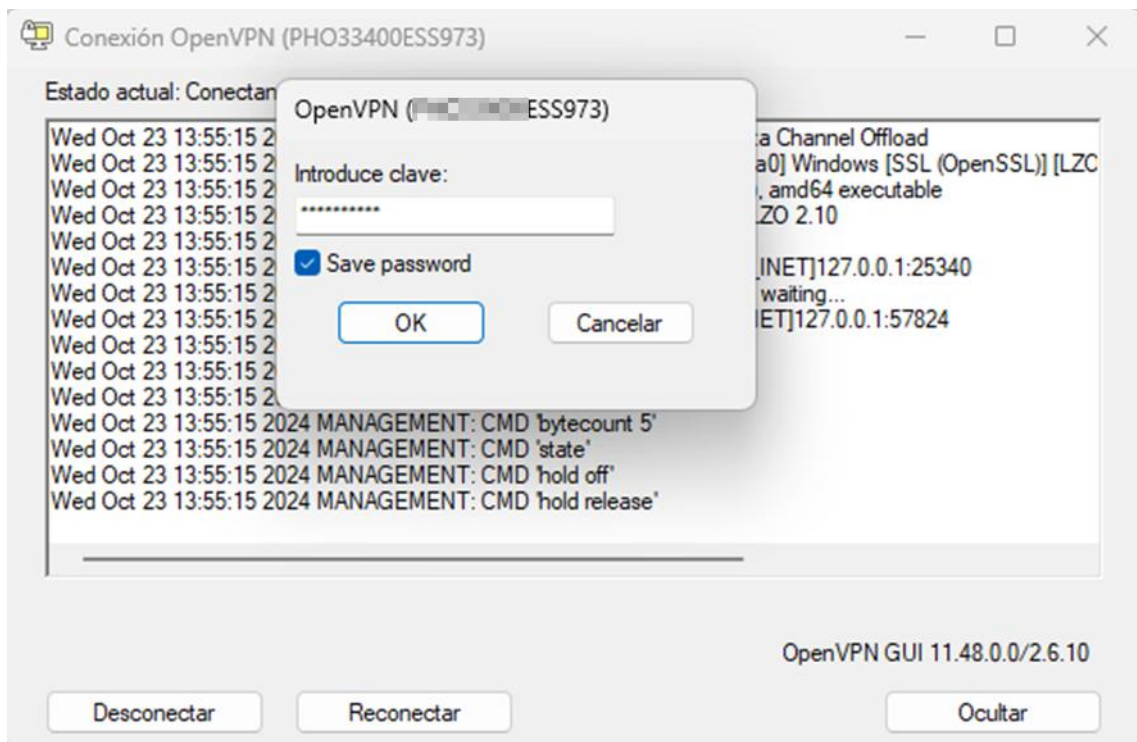


Nuevamente presionando botón derecho del ratón y **Conectar** se procede a establecer el túnel con la Secure Cloud:

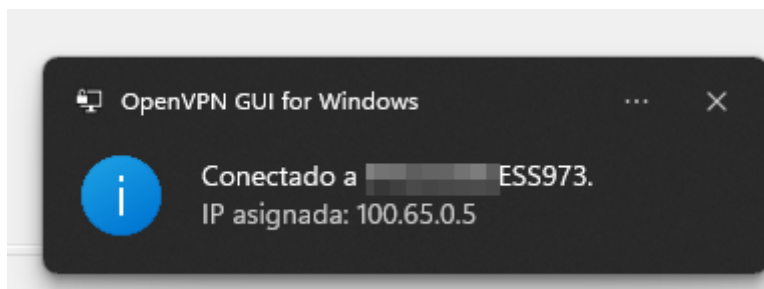




Puede aparecer este mensaje que simplemente se acepta.

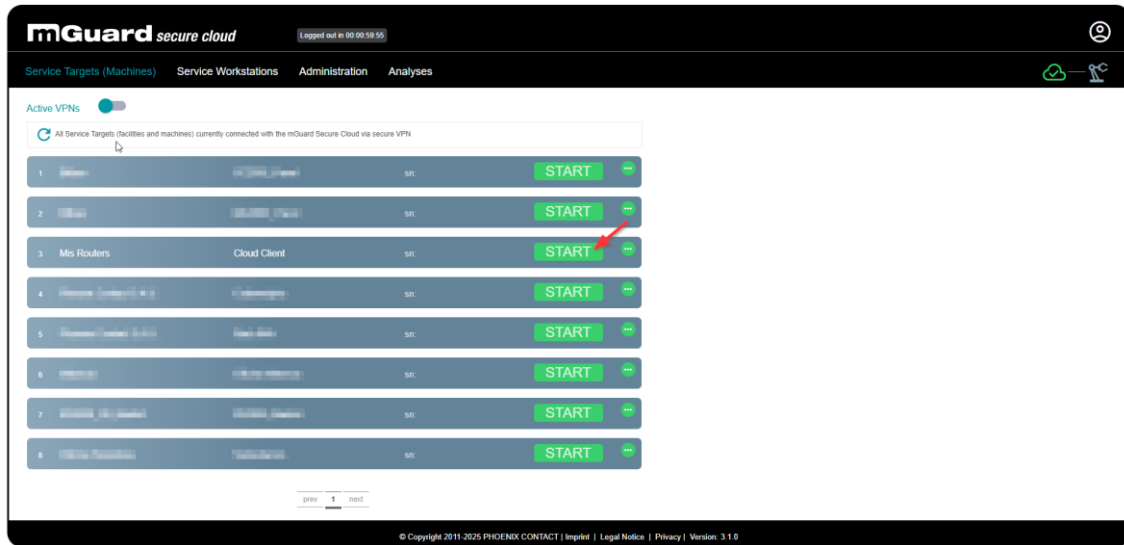


Seguidamente se solicita la contraseña introducida durante el proceso de generación del fichero de configuración del cliente VPN.

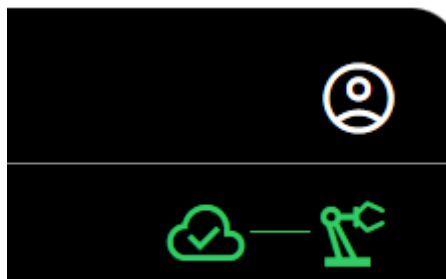


Mensaje de confirmación de túnel establecido.

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:

```


Simbolo del sistema
Microsoft Windows [Versión 10.0.26100.3775]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\essa02>ping 192.168.1.100

Haciendo ping a 192.168.1.100 con 32 bytes de datos:
Respuesta desde 192.168.1.100: bytes=32 tiempo=186ms TTL=63
Respuesta desde 192.168.1.100: bytes=32 tiempo=147ms TTL=63
Respuesta desde 192.168.1.100: bytes=32 tiempo=162ms TTL=63
Respuesta desde 192.168.1.100: bytes=32 tiempo=186ms TTL=63

Estadísticas de ping para 192.168.1.100:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 147ms, Máximo = 186ms, Media = 170ms

C:\Users\essa02>
  
```



enhance your automation thinking

PLCnext Control
Many thanks for choosing a controller with PLCnext Technology. Discover the advantages of this open control platform, which provides completely new levels of your freedom for automation.

PLCnext user community:
Many application examples, instructions for use, instructional videos, and FAQs or software and firmware downloads are also available to you in our user community. Become a member of this community and discuss your personal experiences, ideas and questions with other users.

Easy configuration:
Click here for the web-based management of the PLCnext Control.

PLCnext Technology on the Web:
Also visit our PLCnext website. There you will find more information about the PLCnext Technology.

☐ Do not show this page in the future and go directly to the WBM

Anexo 1. Machine Net Pool

OpenVPN necesita al menos una dirección IP libre y que no se esté utilizando en el rango de IP's de máquina.

Es necesario definir cual o cuales serán estas direcciones IP.

Para ello desde la cuenta de la mGuard Secure Cloud se debe definir una o más direcciones IP dentro del rango de máquina.



La máscara CIDR (ejemplo /32) junto a la dirección IP define si es una o varias direcciones IP las que se reservan para la conexión OpenVPN en la red de máquina.

Por ejemplo con la CIDR /32 solo la dirección IP definida se reservará. Con la CIDR /31 serán dos direcciones IP reservadas, 192.168.0.254 y 192.168.0.253.