

## Contenido

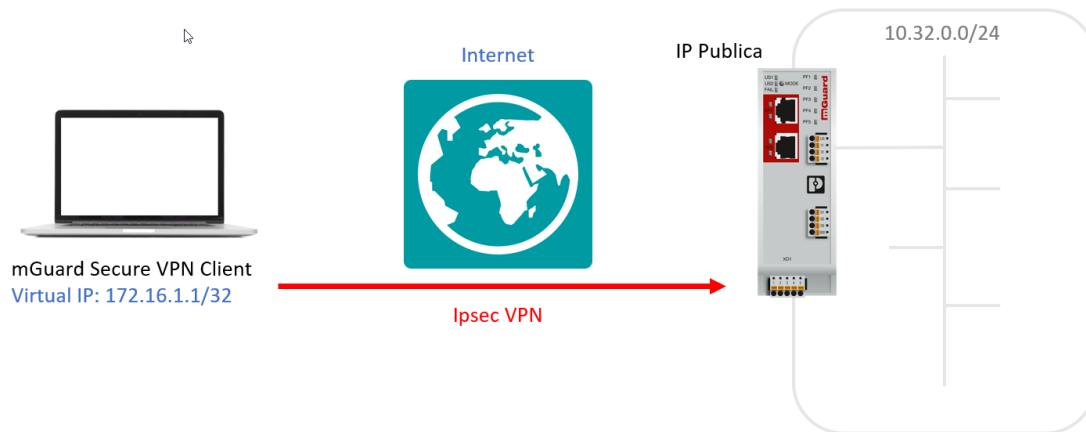
1	Introducción .....	3
2	Certificados X.509 .....	4
2.1	Creación de una base de datos XCA .....	4
2.2	Creación de un certificado CA .....	4
2.3	Creación de un certificado Cliente .....	7
2.4	Exportar los certificados.....	11
3	Configuración del mGuard .....	12
3.1	Importar el certificado de máquina en el mGuard.....	12
3.2	Configuración de la conexión VPN en el mGuard .....	13
3.2.1	Pestaña General .....	13
3.2.2	Pestaña Authentication .....	14
3.2.3	Pestaña Firewall.....	15
3.2.4	Pestaña IKE Options.....	15
4	Configuración del cliente VPN en mGuard Secure VPN Client.....	17
4.1	Importar los certificados.....	17
4.1.1	Certificado CA .....	17
4.1.2	Certificado del cliente VPN .....	18
4.2	Configuración básica con el asistente .....	19
4.3	Parámetros de conexión .....	23
4.4	Establecer/Parar la conexión VPN.....	25
4.4.1	Comprobación de la conexión .....	26
5	Configuración del cliente VPN en Shrewsoft .....	27
5.1	Configuración del perfil de cliente .....	27

# 1 Introducción

La siguiente guía describe los pasos para configurar una conexión VPN entre un mGuard Secure VPN Client (referido en la guía como Cliente VPN) y un mGuard utilizando certificados X.509 para la autenticación de las partes.

En el capítulo 5 se muestra también como crear un perfil de cliente con el software Shrewsoft.

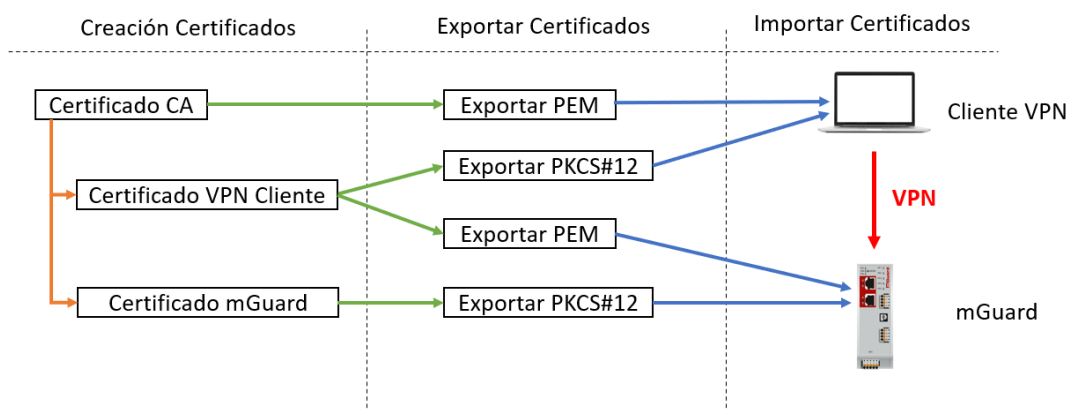
El Cliente VPN inicia la conexión VPN, el mGuard espera la conexión.



## 2 Certificados X.509

Para crear los certificados se puede utilizar el programa freeware **XCA**.

La distribución de certificados que se seguirán es el indicado en la figura.



### 2.1 Creación de una base de datos XCA

Abra el programa **XCA**.

1. Seleccione el menú **File > New Database**
2. Especifique un nombre y una localización de la base de datos.
3. Pulse **Save**.
4. Escriba una contraseña para proteger el uso de la base de datos de certificados.

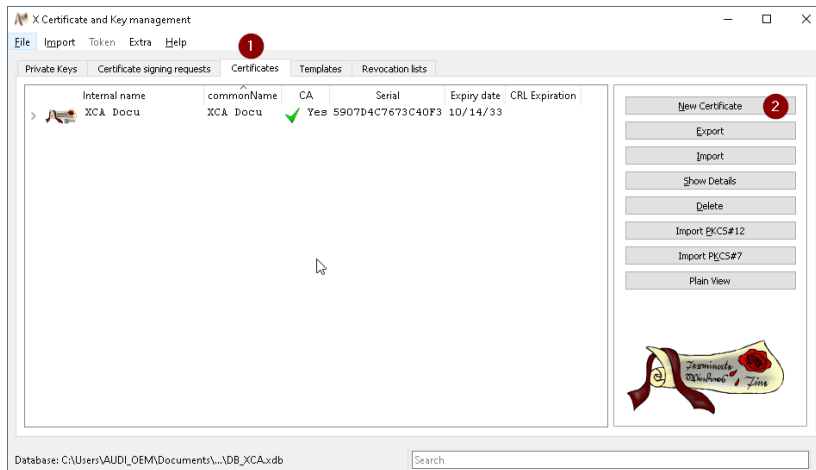
### 2.2 Creación de un certificado CA

Para poder crear y utilizar certificados que no sean autofirmados, si no creados por una autoridad certificadora (CA) podemos crear un certificado CA.

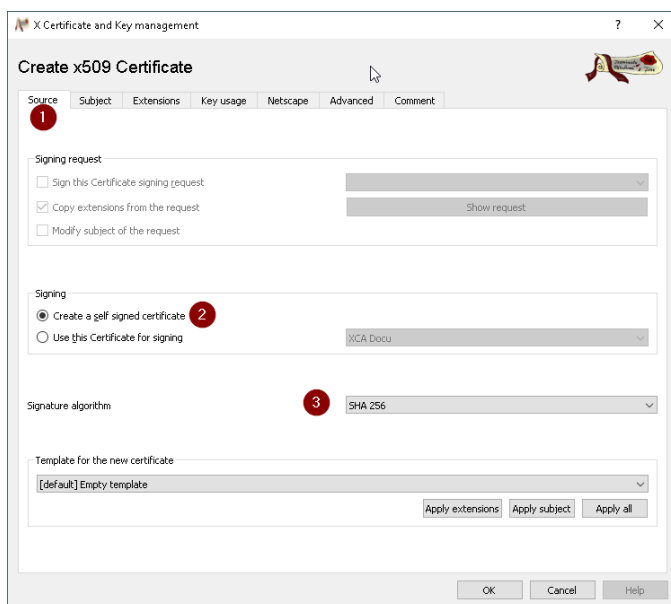
El certificado CA será un certificado autofirmado.

Este certificado CA será el que utilizemos para firmar todo el resto de certificados.

1. Desde la pestaña **Certificates**
2. **New Certificate**

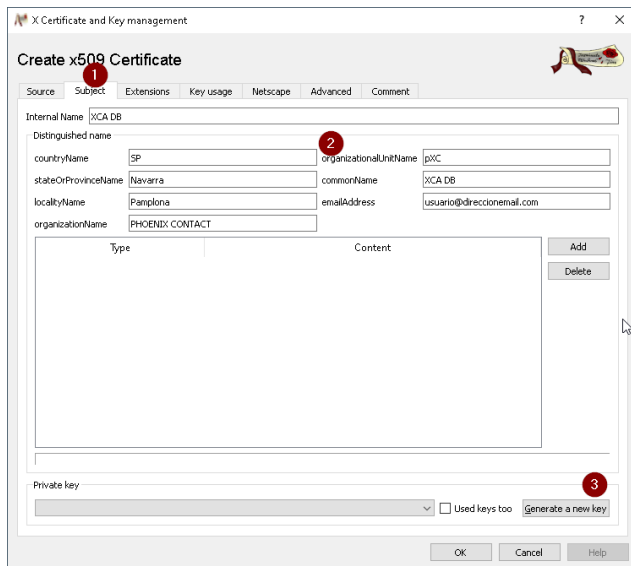


1. Seleccione la pestaña **Source**
2. Seleccione que el certificado **CA** sea autofirmado
3. Seleccione el algoritmo de firma **SHA 256**

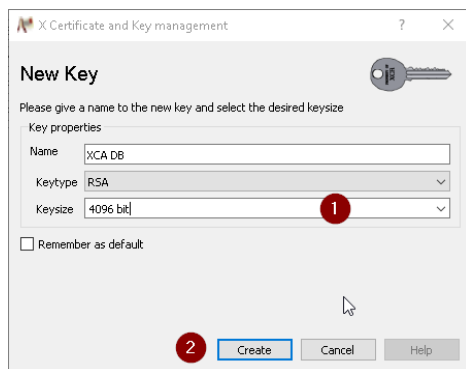


Seleccione la pestaña **Subject**

1. Rellene los campos de **Distinguished Name** e **Internal Name**. Es importante que los campos **Internal Name** y **Common Name** tengan el mismo nombre.

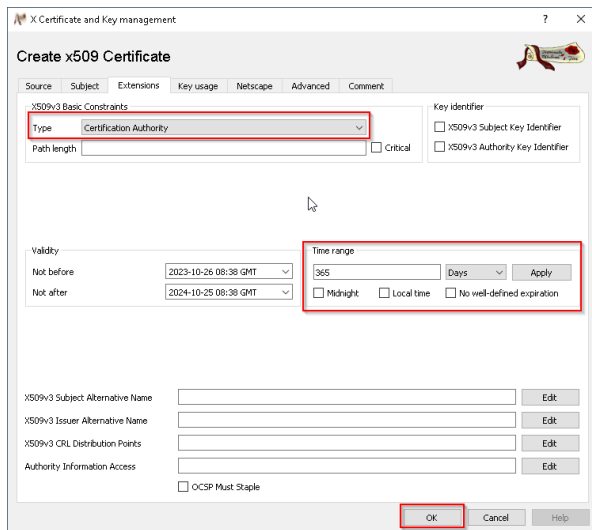


2. Pulse **Generate a new key**. En el siguiente diálogo seleccione la **Keysize** y pulse **Create**



Seleccione la pestaña **Extensions**.

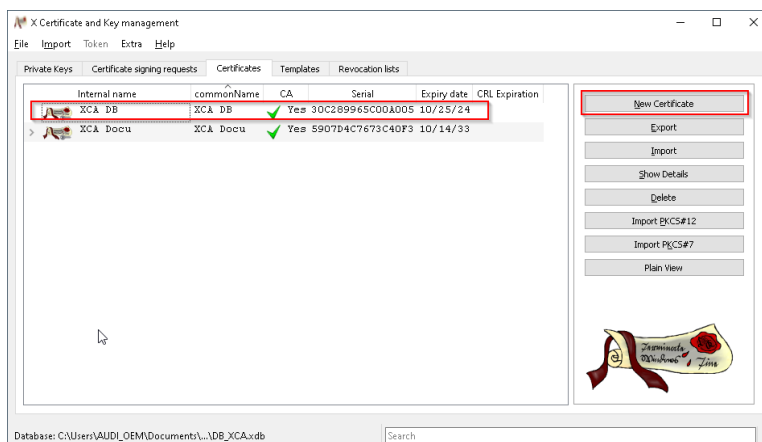
3. Seleccione el tipo **Certification Authority**
4. Seleccione el rango de validez del certificado que les interese. Tenga en cuenta que el resto de certificados que dependan de éste podrán tener como máximo ese rango de validez.
5. Pulse **Apply** y **OK** para terminar



## 2.3 Creación de un certificado Cliente

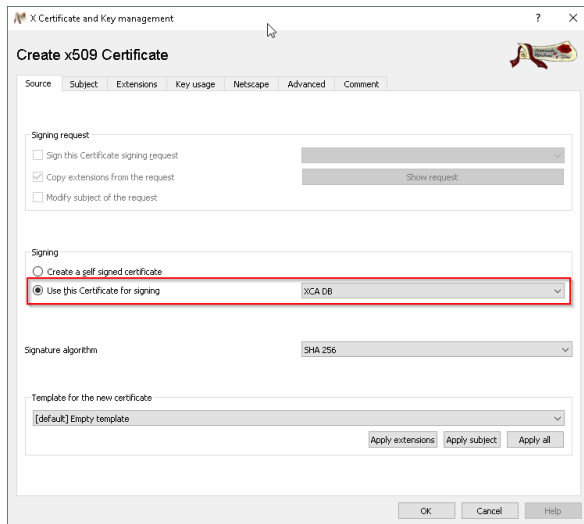
Una vez creado un certificado CA ya se pueden generar certificados clientes firmados por esa CA. Estos certificados cliente pueden ser, por ejemplo, el certificado a utilizar en la máquina (mGuard) o el Cliente VPN.

1. Seleccione la pestaña **Certificates**
2. Seleccione el certificado CA anteriormente creado
3. Pulse **New Certificate**



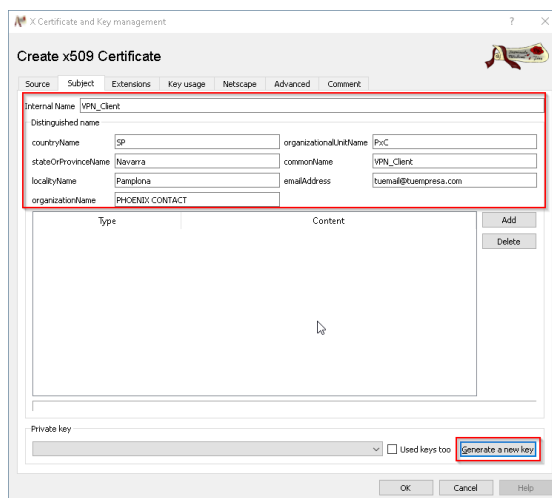
Seleccione la pestaña **Source**

1. En la sección **Signing** seleccione el certificado CA con el que se firmará el certificado a crear



Seleccione la pestaña **Subject**.

1. Rellene los campos **Internal Name** y **Distinguished Name**  
Recuerde utilizar el mismo nombre en **Internal Name** que en **Common Name**



2. Pulse el botón **Generate a new key**
3. En el siguiente dialogo seleccione el tamaño de la llave privada del certificado en **Keysize** y pulse **Create**.



Una vez creada aparece bajo **Private Key**




The screenshot shows the 'Create x509 Certificate' window with various tabs like Source, Subject, Extensions, etc. The 'Private key' dropdown at the bottom is highlighted with a red box, showing 'VPN\_Client (RSA-4096 bit)'.

Seleccione la pestaña Extensions

1. Seleccione en **Type: End Entity**
2. Seleccione el rango de duración del certificado a partir de las fechas de validez.

The screenshot shows the 'Extensions' tab of the 'Create x509 Certificate' window. The 'Type' dropdown is set to 'End Entity'. The 'Time range' is set to '10 Months'. The 'OK' button at the bottom is highlighted with a red box.

El certificado cliente se ha creado y aparece debajo de su certificado CA.

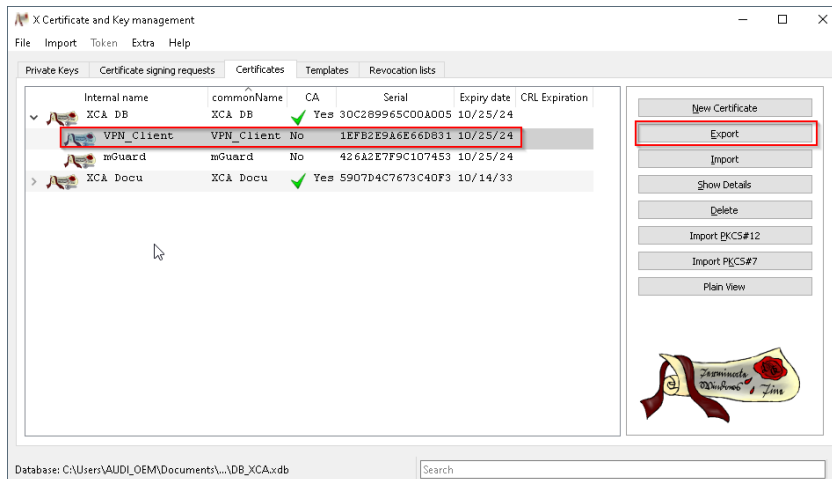
Internal name	commonName	CA	Serial	Expiry date	CRL Expiration
 XCA_DB	XCA_DB	 Yes	30C289965C00A005	10/25/24	
 VPN_Client	VPN_Client	No	1EFB2E9A6E66D831	10/25/24	

Repita el proceso para crear el certificado para el mGuard.

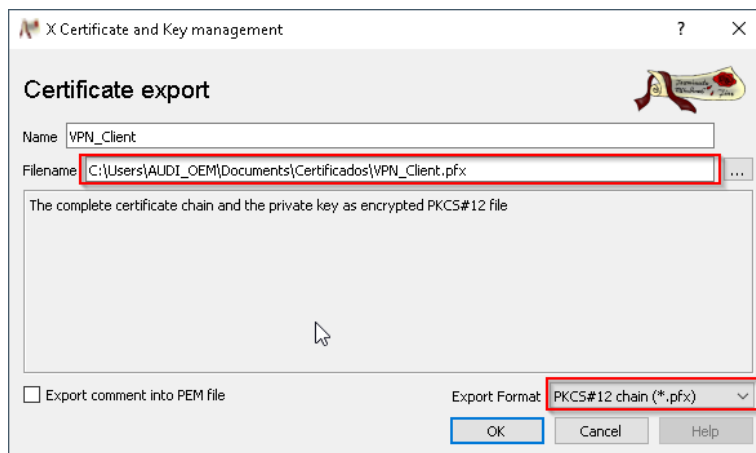
## 2.4 Exportar los certificados

Una vez creados los certificados, estos se deben exportar para poderlos utilizar tanto el en Cliente VPN como en el mGuard de modo que ambos se puedan autenticar entre si.

1. Seleccione el certificado a exportar y pulse **Export**



2. Seleccione la ruta y el nombre del certificado a exportar.
3. Elija el formato del certificado



4. Pulse Ok
5. Repita el proceso para el mGuard y el certificado CA. Al final debe tener estos cuatro ficheros exportados

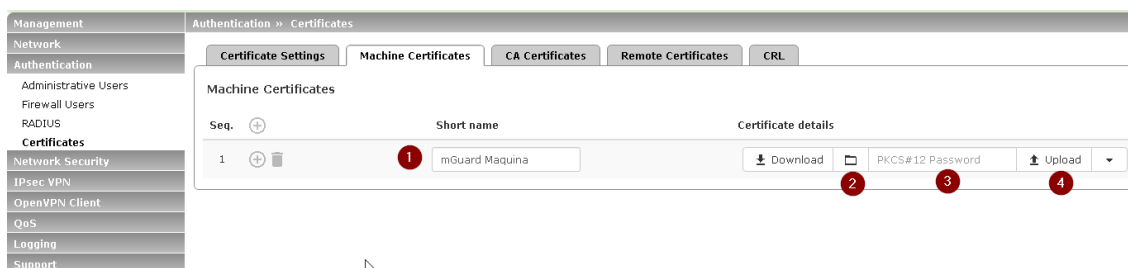
Nombre	Fecha de modificación	Tipo	Tamaño
mGuard.pfx	14/10/2023 11:28	PKCS#12 Certificat...	6 KB
VPN_Client.crt	14/10/2023 11:27	X.509 Certificate	3 KB
VPN_Client.pfx	14/10/2023 11:26	PKCS#12 Certificat...	6 KB
XCA_... .crt	14/10/2023 11:25	X.509 Certificate	3 KB

## 3 Configuración del mGuard

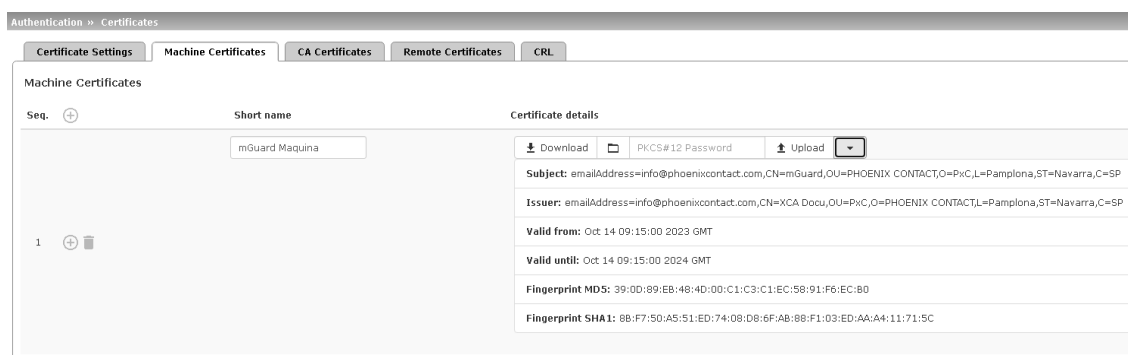
### 3.1 Importar el certificado de máquina en el mGuard

Desde el menú **Authentication > Certificates** en la pestaña **Machine Certificates**

1. Escribe un nombre con el que se identifique el certificado
2. Haga click en la carpeta y seleccione el certificado **pkcs#12** creado para el mGuard.
3. Escriba la contraseña creada para el certificado.
4. Haga click en **Upload**. En la barra superior debe aparecer un mensaje en verde indicando que el certificado ha sido subido al mGuard correctamente.



Una vez subido podemos ver los parámetros del certificado haciendo click en la flecha a la derecha de **Upload**.



Selecciona el menú **Ipsec VPN > Connections**

1. Haga click en **+** para crear una nueva VPN
2. Initial mode > **Started**
3. Escriba un nombre para identificar la VPN

Haga click en el icono de disco en la parte superior derecha para salvar la configuración.

IPsec VPN » Connections

Connections

License Status

VPN license counter	1
OpenVPN license counter	0

Connections

Seq.	Initial mode	State	ISAKMP SA	IPsec SA	Name
1	Started	Started			VPN2

Una vez creada haga click en el icono del lápiz

IPsec VPN » Connections

Connections

License Status

VPN license counter	1
OpenVPN license counter	0

Connections

Seq.	Initial mode	State	ISAKMP SA	IPsec SA	Name
1	Started	Stopped	X	X 0/0	VPN2

## 3.2 Configuración de la conexión VPN en el mGuard

### 3.2.1 Pestaña General

Deje todos los parámetros como aparecen en la siguiente imagen.

1. **Type -Tunnel**
2. Local. Escriba el rango de IP's de máquina al que quiere tener acceso a través de la VPN
3. Remote. Escriba la IP o rango de IP's desde la cual se conectará el cliente VPN.

IPsec VPN » Connections » VPN2

General Authentication Firewall IKE Options

Options

A descriptive name for the connection: VPN2

Initial mode: Started

Address of the remote site's VPN gateway (IP address, hostname, or '%any' for any IP, multiple clients or clients behind a NAT gateway): %any

Interface to use for gateway setting %any: External

Connection startup: Wait

Controlling service input: None

Deactivation timeout: 0:00:00 seconds (hh:mm:ss)

Encapsulate the VPN traffic in TCP: No

Mode Configuration

Mode configuration: Off

Transport and Tunnel Settings

Seq.	Enabled	Comment	Type	Local	Local NAT	Remote	Remote NAT
1	<input checked="" type="checkbox"/>		Tunnel	10.32.0.0/24	No NAT	192.168.254.1/32	No NAT

< Back

### 3.2.2 Pestaña Authentication

- Indicamos el certificado de máquina anteriormente subido al mGuard. Este es el certificado local para el mGuard
- Subimos el certificado remoto del cliente VPN (\*.pem)

IPsec VPN » Connections » VPN2

General Authentication Firewall IKE Options

Authentication

Authentication method: X.509 certificate

Local X.509 certificate: mGuard Maquina (1)

Remote CA certificate: None

Remote certificate: mGuard Maquina (2)

VPN Identifier

Local: [ ]

Remote: [ ]

< Back

Al hacer click en 1 se pueden ver los parámetros del certificado de cliente.

IPsec VPN » Connections » VPN

General Authentication Firewall IKE Options

Authentication

Authentication method: X.509 certificate

Local X.509 certificate: mGuard Maquina

Remote CA certificate: No CA certificate, but the remote certificate below

Remote certificate: [Download] [ ] [Upload] (1)

Subject: emailAddress=info@phoenixcontact.com,CN=VPN\_Client,OU=PHOENIX CONTACT,O=Pamplona,ST=Navarra,C=SP

Issuer: emailAddress=info@phoenixcontact.com,CN=XCA Docu,OU=PxC,O=PHOENIX CONTACT,L=Pamplona,ST=Navarra,C=SP

Valid from: Oct 14 09:18:00 2023 GMT

Valid until: Oct 14 09:18:00 2024 GMT

Fingerprint MD5: 36:A0:51:8D:23:16:8D:C6:B6:74:D5:37:90:78:57:66

Fingerprint SHA1: 0D:48:12:8B:9B:C1:61:90:EE:63:49:DB:4F:37:AD:85:8A:F6:4E:8B

### 3.2.3 Pestaña Firewall

Desde la pestaña firewall se pueden crear reglas de entrada y salida de tráfico en la VPN.

IPsec VPN » Connections » VPN

General Authentication Firewall IKE Options

Incoming

General firewall setting: Use the firewall ruleset below

Seq.	Protocol	From IP	From port	To IP	To port	Action	Comment	Log
1	All	0.0.0.0/0		0.0.0.0/0		Accept	default rule - please add	<input type="checkbox"/>

Log entries for unknown connection attempts: ☐

Outgoing

General firewall setting: Use the firewall ruleset below

< Back

### 3.2.4 Pestaña IKE Options

1. La fase 1, ISAKMP SA (Key Exchange) necesita conocer el algoritmo de encriptación, hash y Diffie-Hellman con el que va a negociar la key con el cliente VPN.
2. La fase 2, IPsec SA (Data Exchange) del mismo modo necesita que los algoritmos de encriptación y Hash coincidan con los parametrizados en el cliente VPN.

IPsec VPN » Connections » VPN

General Authentication Firewall IKE Options

ISAKMP SA (Key Exchange)

Seq. + 1 **1** Encryption AES-256 Hash SHA-512 Diffie-Hellman 1536 bits (group 5)

IPsec SA (Data Exchange)

Seq. + 1 **2** Encryption AES-256 Hash SHA-256

Perfect Forward Secrecy (PFS) (Activation recommended. The remote site must have the same entry.) Yes

Lifetimes and Limits

ISAKMP SA lifetime	1:00:00	seconds (hh:mm:ss)
IPsec SA lifetime	8:00:00	seconds (hh:mm:ss)
IPsec SA traffic limit	0	bytes
Re-key margin for lifetimes (applies to ISAKMP SAs and IPsec SAs)	0:09:00	seconds (hh:mm:ss)
Re-key margin for the traffic limit (applies to IPsec SAs only)	0	bytes
Re-key fuzz (applies to all re-key margins)	100	percent
Keying tries (0 means unlimited tries)	0	

Dead Peer Detection

Delay between requests for a sign of life	0:00:30	seconds (hh:mm:ss)
Timeout for absent sign of life after which peer is assumed dead	0:02:00	seconds (hh:mm:ss)

Activar Windows < Back

El resto de parámetros se pueden dejar tal y como aparecen en la figura.

Haz click en el icono del disco (parte superior izquierda) para salvar la configuración.




## 4 Configuración del cliente VPN en mGuard Secure VPN Client

Se puede descargar en el siguiente link

[MGuard Secure VPN Client LIC - Licencia - 2702579 | Phoenix Contact](#)

Descargas > Software

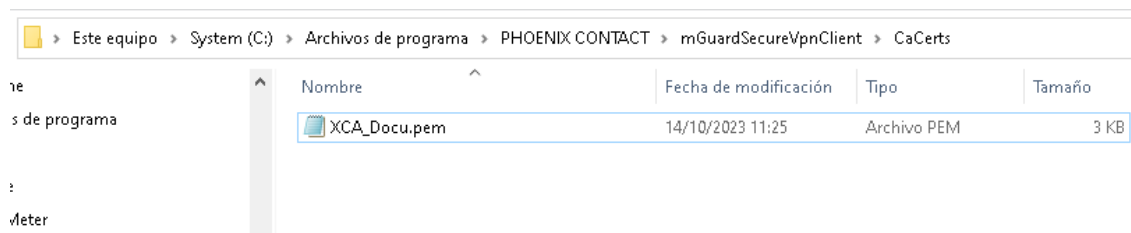
 mGuard-Secure-VPN-Client_Win_x86-64_1114_42039.zip	(55,9 MB)	64 bits, versión de prueba de 30 días del cliente mGuard Secure VPN para conectar PCs a mGuard VPN Appliances y mGuard Secure Cloud	Plurilingüe	11.14
SHA256 suma de control: 66f5e76e2d7a232dc7f984170d88748486367364 574208dab57911986e9752bf				

Tras instalarse ofrece una versión de prueba de 30 días.

### 4.1 Importar los certificados

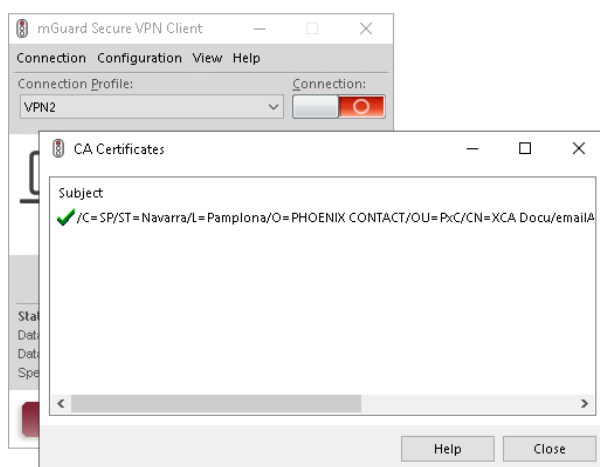
#### 4.1.1 Certificado CA

Copie el certificado CA exportado en formato **PEM** en el directorio **CaCerts** de la ruta de instalación del **mGuard Secure VPN Client**.



La extensión del certificado debe ser **PEM** si no el **mGuard Secure VPN Client** no lo encontrará. Si el archivo tiene otra extensión renómbrela con la extensión PEM.

Para verificar que el mGuard Secure VPN Client puede cargar el certificado, seleccione el menú **Connection > Certificates > Display CA Certificates**

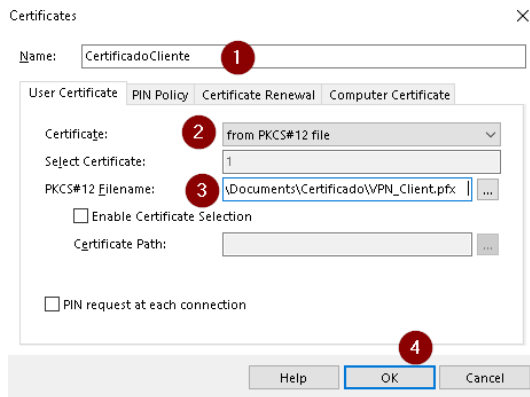


#### 4.1.2 Certificado del cliente VPN

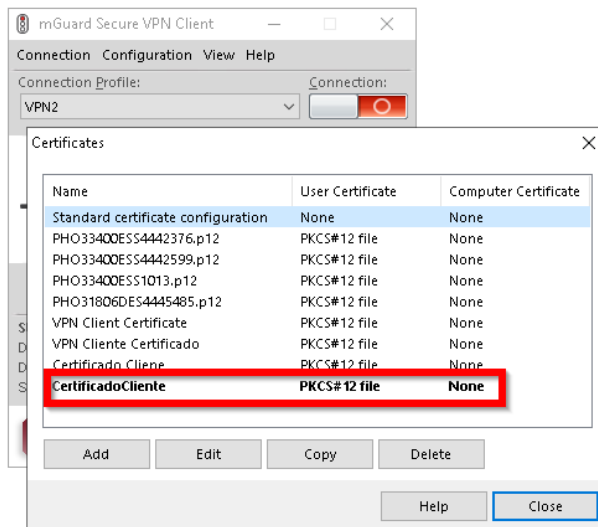
Selecciona el menú **Configuration > Certificates**. Clica **Add**

En la pestaña **User Certificate**:

1. Escriba un nombre para identificar el certificado
2. Seleccione la opción **from PKCS#12 file**
3. Seleccione el archivo **pkcs#12** del certificado.  
Si la contraseña utilizada para exportar este certificado tiene menos de 6 caracteres cambie a la pestaña **PIN** e indique el número de caracteres de la contraseña.
4. Pulse **Ok**.



Desde el menú **Configuration > Certificates** se debe ver listado el nuevo certificado importado.

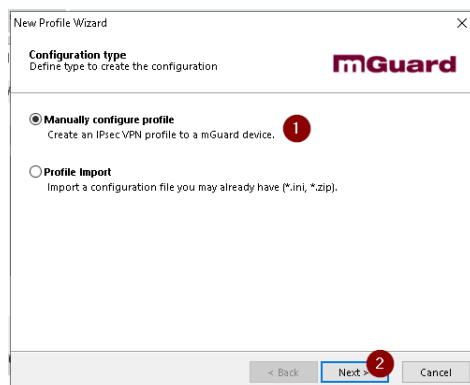


## 4.2 Configuración básica con el asistente

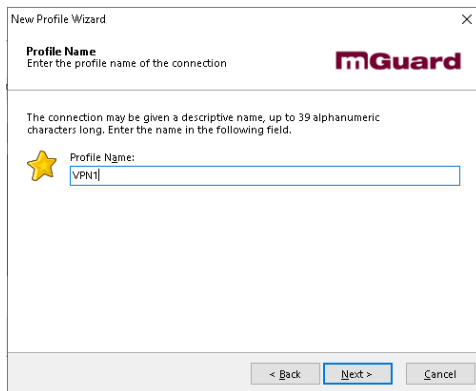
Seleccione **Configuration > Profiles** en el menú.

Haga click en **Add/Import**.

En el diálogo seleccione la configuración del perfil manual.



Escriba un nombre para identificar el perfil.



**New Profile Wizard**

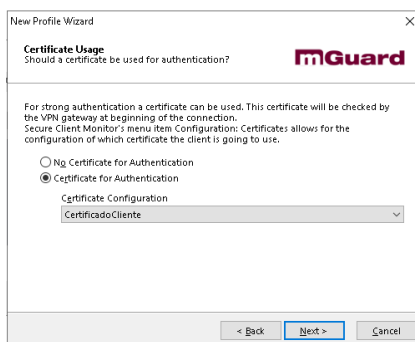
**Profile Name**  
Enter the profile name of the connection

The connection may be given a descriptive name, up to 39 alphanumeric characters long. Enter the name in the following field.

★ Profile Name:

< Back Next > Cancel

Seleccione el certificado de cliente anteriormente importado.



**New Profile Wizard**

**Certificate Usage**  
Should a certificate be used for authentication?

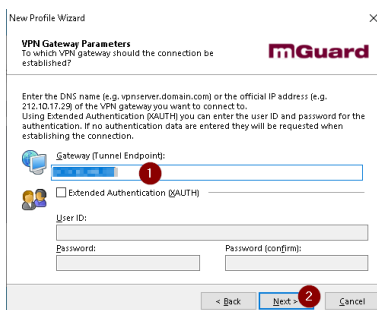
For strong authentication a certificate can be used. This certificate will be checked by the VPN gateway at beginning of the connection. Secure Client Monitor's menu item Configuration: Certificates allows for the configuration of which certificate the client is going to use.

☐ No Certificate for Authentication  
☒ Certificate for Authentication

Certificate Configuration

< Back Next > Cancel

Escriba la dirección publica o dirección DNS por la que acceder al servidor VPN.



**New Profile Wizard**

**VPN Gateway Parameters**  
To which VPN gateway should the connection be established?

Enter the DNS name (e.g. vpnserver.domain.com) or the official IP address (e.g. 212.10.17.29) of the VPN gateway you want to connect to. Using Extended Authentication (EAUTH) you can enter the user ID and password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

Gateway (Tunnel Endpoint):

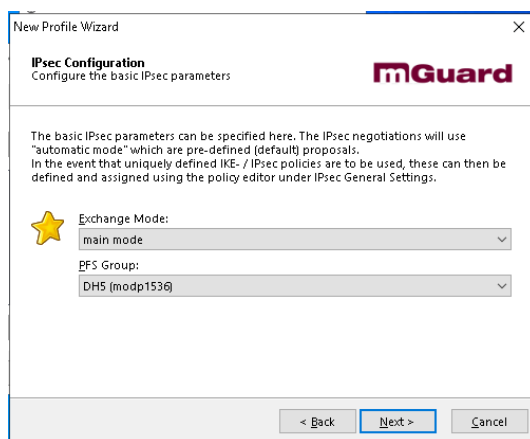
☐ Extended Authentication (EAUTH)

User ID:

Password:  Password (confirm):

< Back Next > Cancel

Deje los parámetros por defecto (**Exchange Mode = Main Mode, PFS Group= DH-Group 5**)



**New Profile Wizard**

**IPsec Configuration**  
Configure the basic IPsec parameters

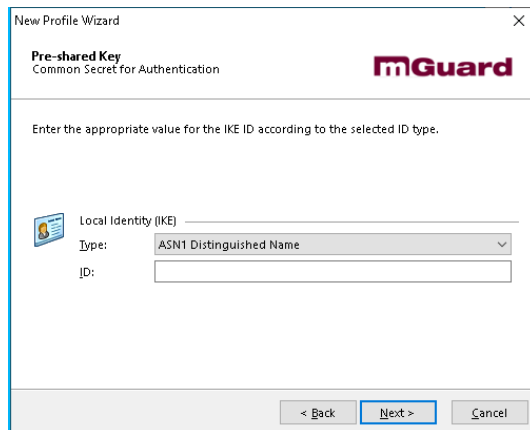
The basic IPsec parameters can be specified here. The IPsec negotiations will use "automatic mode" which are pre-defined (default) proposals. In the event that uniquely defined IKE- / IPsec policies are to be used, these can then be defined and assigned using the policy editor under IPsec General Settings.

★ Exchange Mode:

PFS Group:

< Back Next > Cancel

Deje los parámetros por defecto y continúe.



**New Profile Wizard**

**Pre-shared Key**  
Common Secret for Authentication

Enter the appropriate value for the IKE ID according to the selected ID type.

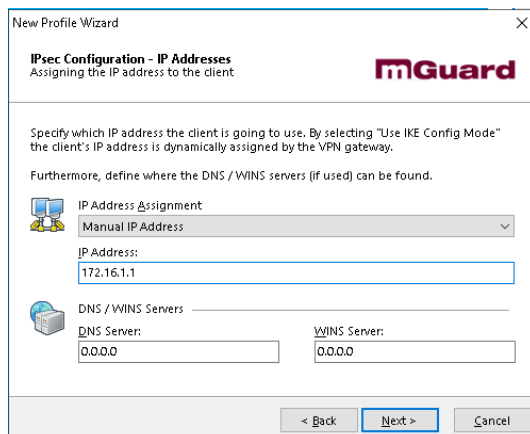
Local Identity (IKE)

Type:

ID:

< Back Next > Cancel

Seleccione la IP del cliente VPN con la que quieres crear la VPN.



**New Profile Wizard**

**IPsec Configuration - IP Addresses**  
Assigning the IP address to the client

Specify which IP address the client is going to use. By selecting "Use IKE Config Mode" the client's IP address is dynamically assigned by the VPN gateway.

Furthermore, define where the DNS / WINS servers (if used) can be found.

IP Address Assignment

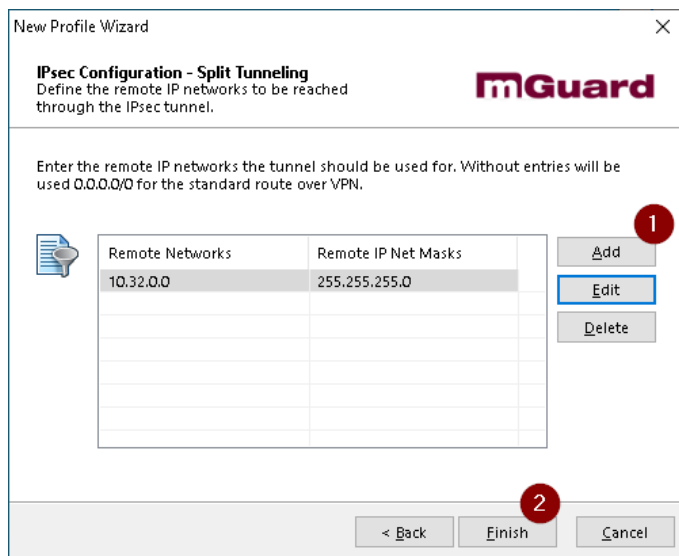
IP Address:

DNS / WINS Servers

DNS Server:  WINS Server:

< Back Next > Cancel

1. Haga click en Add y escriba la red interna y máscara de subred a la que se accederá a través del mGuard con la VPN. Ejemplo 10.32.0.0/24.
2. Haga click en Finish para terminar de crear el perfil de cliente VPN.



New Profile Wizard

**IPsec Configuration - Split Tunneling**  
Define the remote IP networks to be reached through the IPsec tunnel.

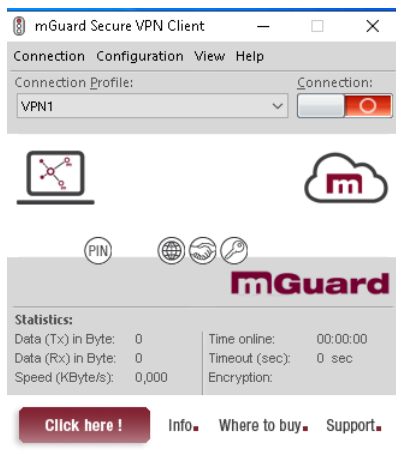
Enter the remote IP networks the tunnel should be used for. Without entries will be used 0.0.0.0/0 for the standard route over VPN.

Remote Networks	Remote IP Net Masks
10.32.0.0	255.255.255.0

Add Edit Delete

< Back Finish Cancel

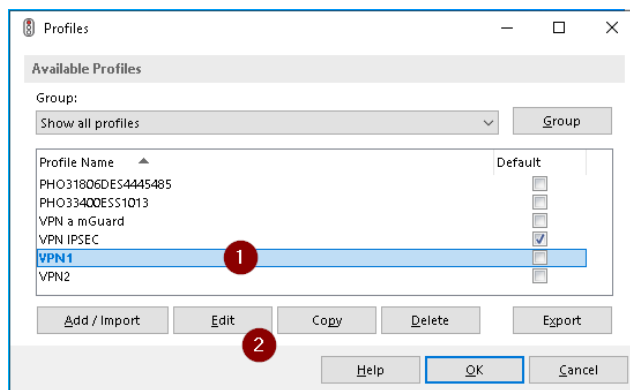
Una vez creado ya se encuentra disponible en la lista de perfiles para iniciar la conexión VPN.



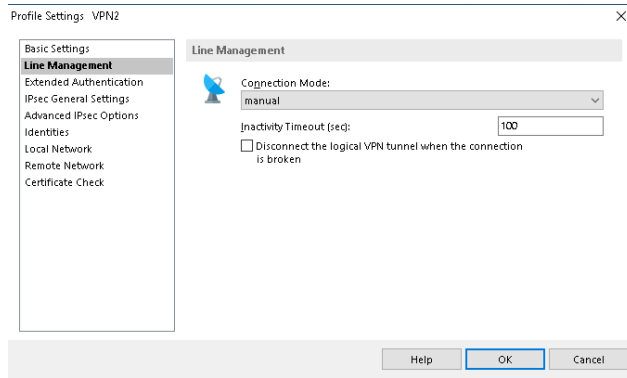
### 4.3 Parámetros de conexión

Para ajustar los parámetros, menú **Configuration > Profiles**.

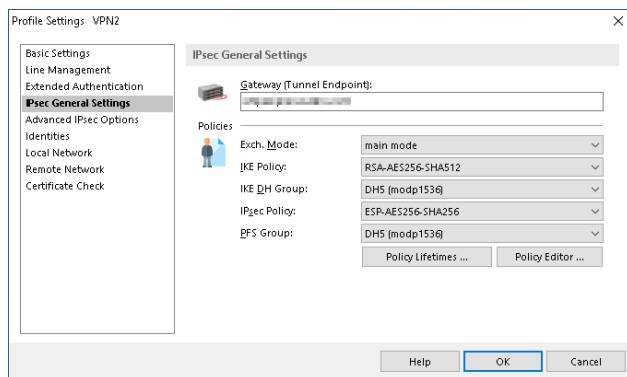
1. Seleccione el perfil.
2. Haga click en **Editar**.



Seleccione el menú **Line Management** y deje **Connection Mode** en **manual**.



En el menú **IPSec General Settings** configure las **Políticas** tal y como se indica en la figura.



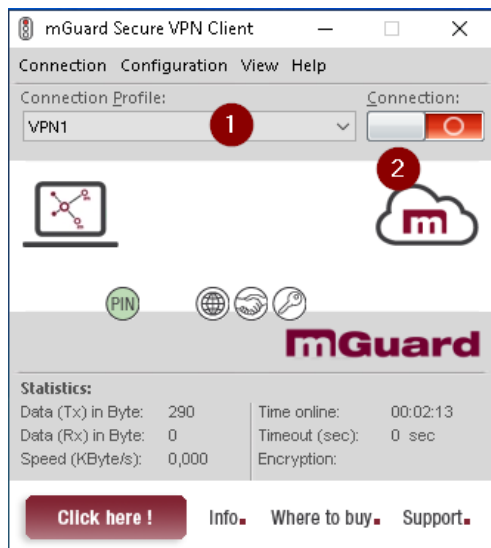
Es importante que estos algoritmos de encriptación y hash sean los mismos que en la configuración del **VPN Server (mGuard)**.

Al pulsar **OK** la configuración del perfil **VPN Client** finaliza.

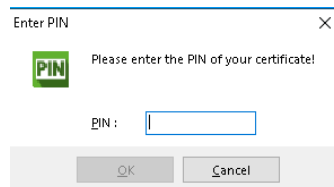


#### 4.4 Establecer/Parar la conexión VPN

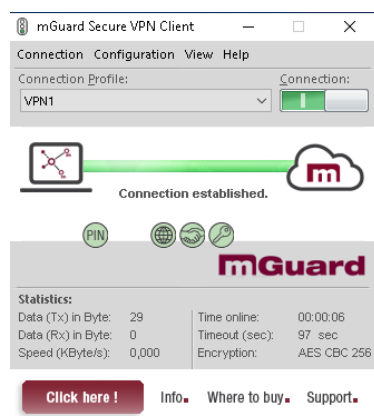
1. Seleccione el perfil de conexión
2. Pulse el botón para iniciar la conexión



Escriba la contraseña pkcs#12 creada para el certificado del cliente.  
Esta contraseña protege al cliente de un uso no autorizado.



Si todo es correcto la conexión se debe establecer.



#### 4.4.1 Comprobación de la conexión

Con la VPN activa, abra el CMD de Windows y teclee el comando **ipconfig**.

Comprobará que se ha creado un nuevo interfaz con la IP del cliente configurada en el perfil.

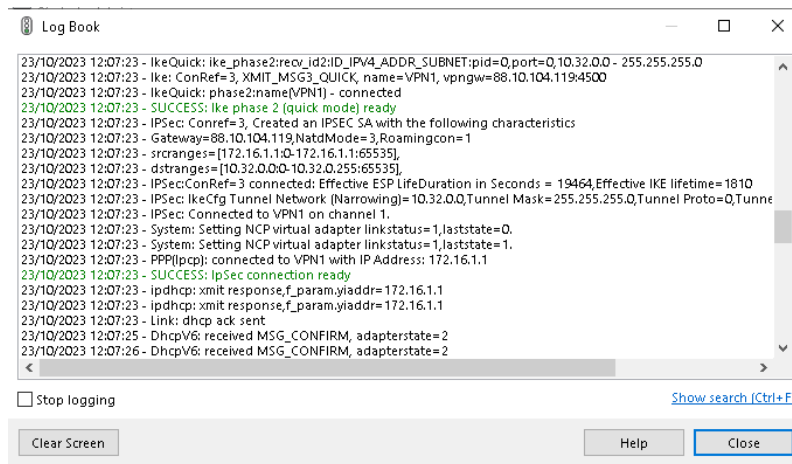
```
C:\Users\...>ipconfig

Configuración IP de Windows

Adaptador desconocido LAN-Verbindung:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::11c2:8b70:726b:eb88%10
    Dirección IPv4. . . . . : 172.16.1.1
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :
```

Desde mGuard Secure VPN Client, menú **Help > Logbook** puede abrir el log que muestra el estado de los pasos de la conexión.



## 5 Configuración del cliente VPN en Shrewsoft

Shrewsoft es un cliente de VPN Ipsec por lo que se puede utilizar como cliente para establecer una conexión con el mGuard.

Se puede descargar en internet.

Se debe tener en cuenta que la ultima versión es de 2013.

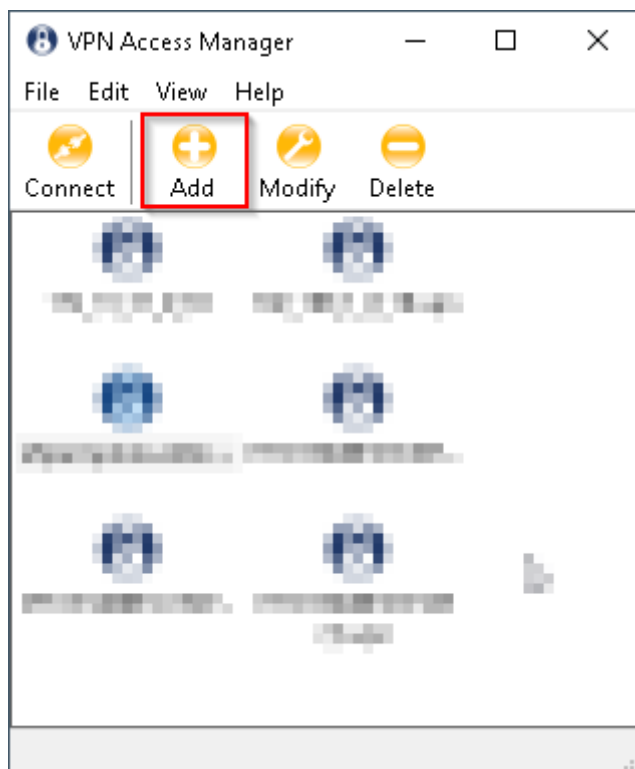
Es un software ajeno a Phoenix Contact, por el cual no se da soporte desde Phoenix Contact.

En los siguientes puntos se describe como configurar un perfil client.

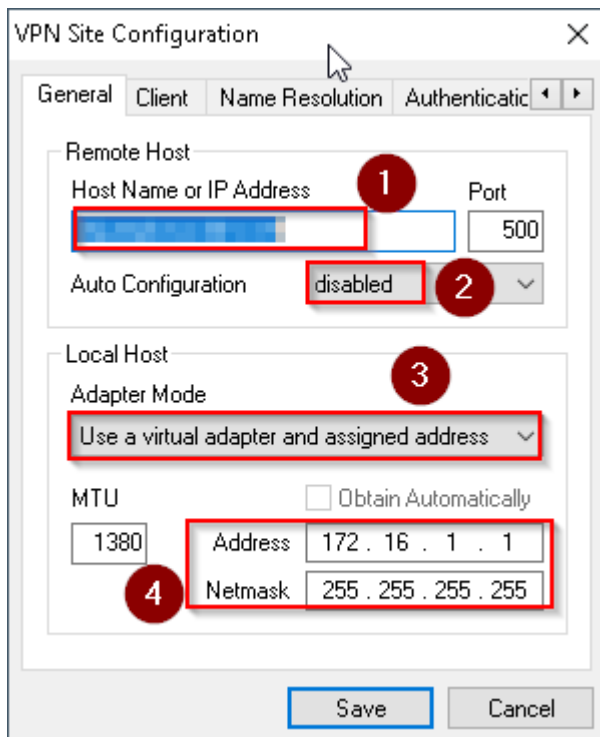
### 5.1 Configuración del perfil de cliente

Inicie el software Shrew Soft VPN Client

Haga click en Add para añadir una nueva conexión.

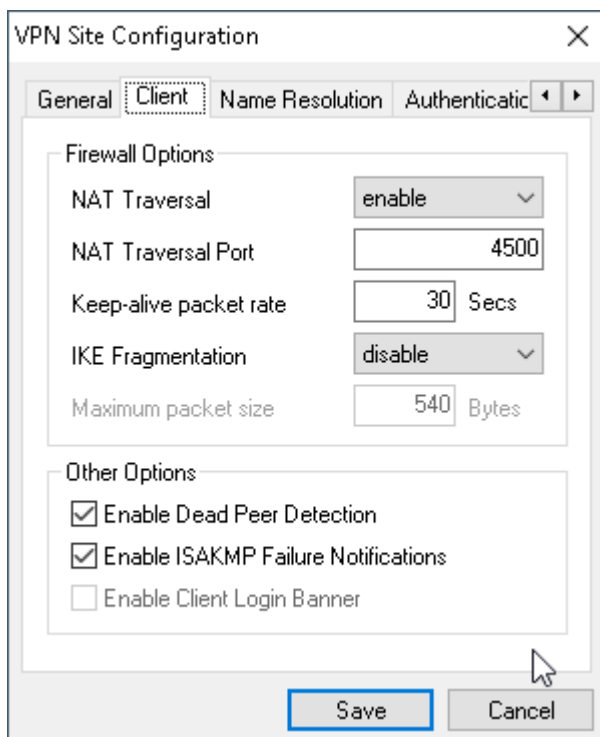


1. Escriba la dirección IP Publica o dirección DNS del servidor (mGuard)
2. Auto Configuration > Disabled
3. Adapter Mode > Use a virtual adapter and assigned address
4. Seleccione la dirección y máscara que desee para el cliente VPN



Seleccione la pestaña **Client**.

Configure los parámetros como se indican en la siguiente figura.



Seleccione la pestaña **Name Resolution**.

Deshabilite todos los checkbox, tal como muestra la siguiente figura.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Name Resolution' tab selected. Inside this tab, there are two sub-tabs: 'DNS' and 'WINS'. The 'DNS' sub-tab is active. It contains the following controls:

- ☐ Enable DNS
- ☐ Obtain Automatically
- Server Address #1: [Text box with dots]
- Server Address #2: [Text box with dots]
- Server Address #3: [Text box with dots]
- Server Address #4: [Text box with dots]
- ☐ Obtain Automatically
- DNS Suffix: [Text box]

At the bottom of the dialog are 'Save' and 'Cancel' buttons. A mouse cursor is pointing at the bottom left of the dialog.

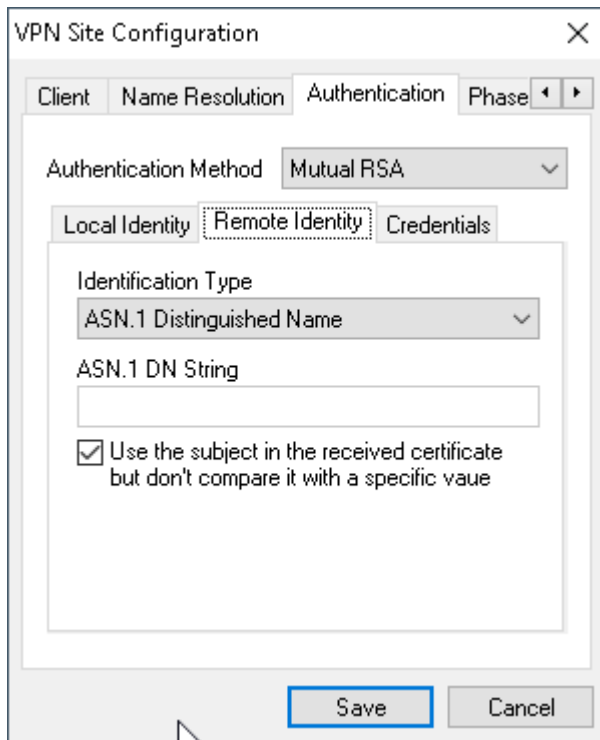
Vaya a la pestaña **Authentication**.

Configure según las siguientes figuras.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Authentication' tab selected. It contains the following controls:

- Authentication Method: [Dropdown menu showing 'Mutual RSA']
- Local Identity | Remote Identity | Credentials (sub-tabs)
- Identification Type: [Dropdown menu showing 'ASN.1 Distinguished Name']
- ASN.1 DN String: [Text box]
- ☒ Use the subject in the client certificate

At the bottom of the dialog are 'Save' and 'Cancel' buttons. A mouse cursor is pointing at the bottom left of the dialog.

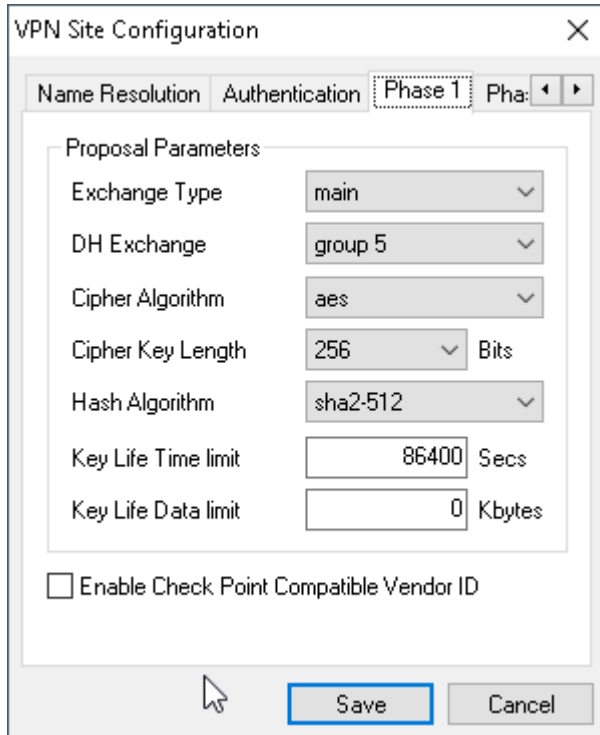


1. Incluya el certificado CA anteriormente exportado
2. Incluya el certificado publico del cliente anteriormente exportado.
3. Incluya el certificado privado del cliente anteriormente exportado.

Seleccione la pestaña **Phase 1**.

Configure los parámetros tal y como se indica en la siguiente figura.

Fíjese como estos parámetros concuerdan con los parametrizados en el servidor (mGuard)



The screenshot shows the 'VPN Site Configuration' dialog box with the 'Phase 1' tab selected. The 'Proposal Parameters' section contains the following settings:

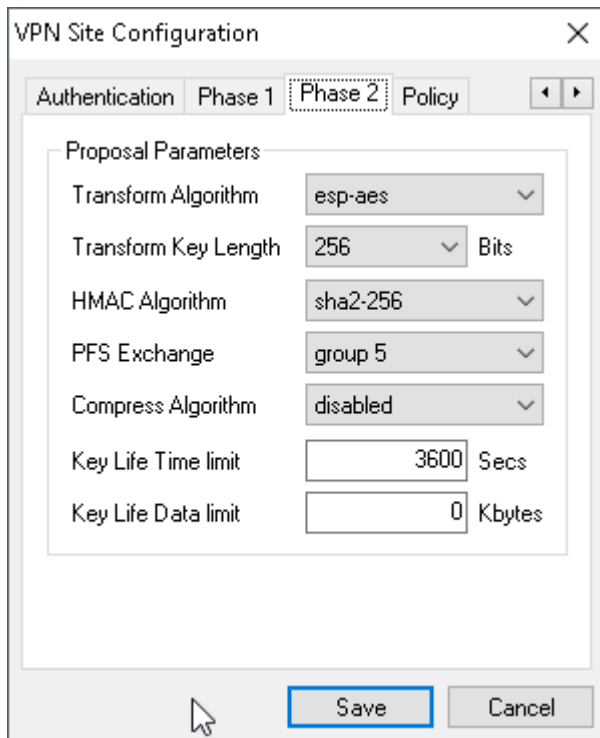
Parameter	Value	Unit
Exchange Type	main	
DH Exchange	group 5	
Cipher Algorithm	aes	
Cipher Key Length	256	Bits
Hash Algorithm	sha2-512	
Key Life Time limit	86400	Secs
Key Life Data limit	0	Kbytes

Below the parameters, there is a checkbox labeled 'Enable Check Point Compatible Vendor ID' which is currently unchecked. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

Seleccione la pestaña **Phase 2**.

Configure los parámetros tal y como se indica en la siguiente figura.

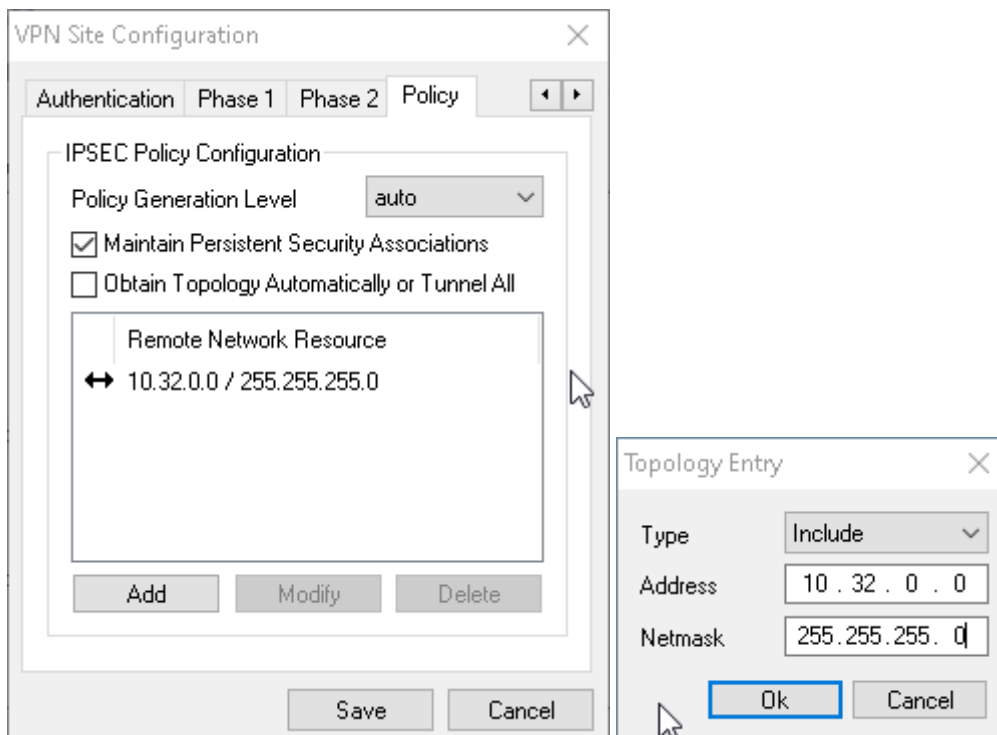
Fíjese como estos parámetros concuerdan con los parametrizados en el servidor (mGuard)



Seleccione la pestaña **Policy**.

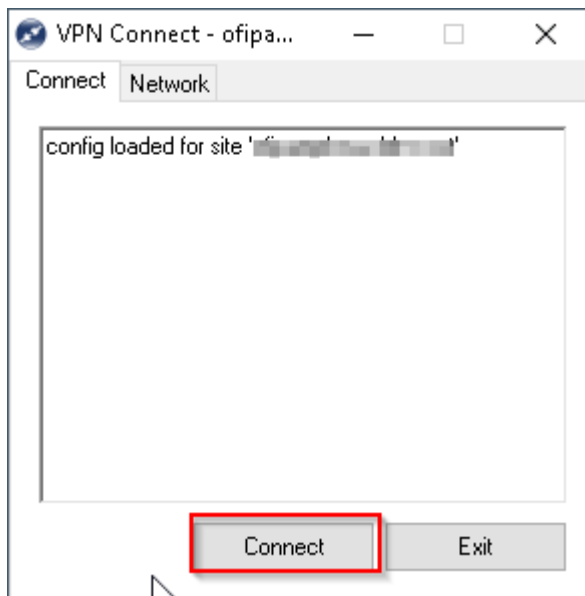
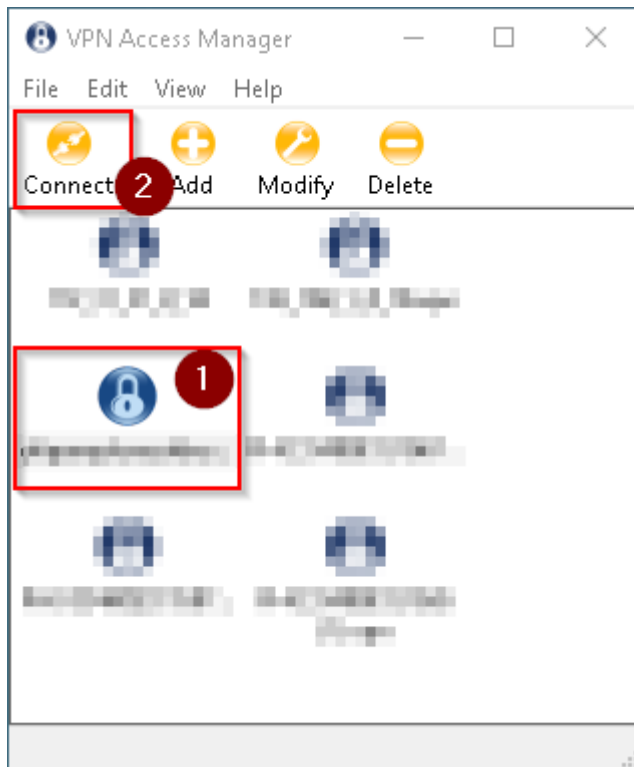
Configure los parámetros según se muestran en la siguiente figura.

Click Add y parámetroice el rango de IP al que debe dar acceso la VPN.

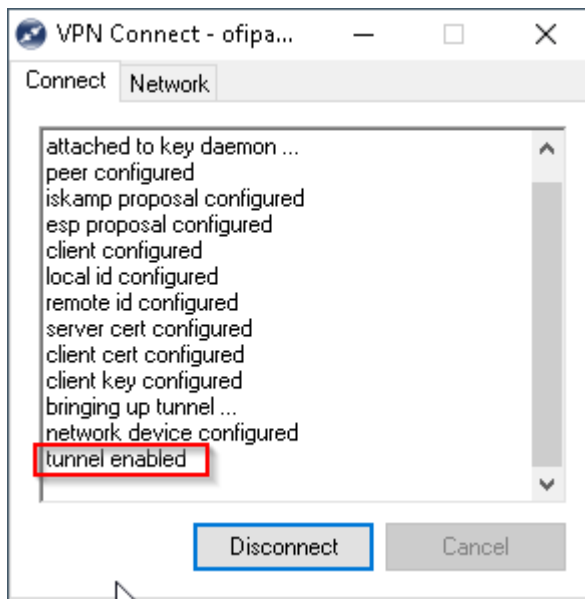
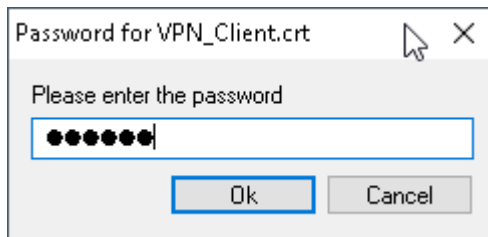




Una vez creado seleccione el perfil y haga click en **Connect**.



Escriba la contraseña del certificado del cliente y pulse OK.



Una vez indica que se ha habilitado el tunel ya se tiene creada la VPN.