

Windows VPN Client

Stormshield SNS 4.2 DR Mode Configuration Guide

TheGreenBow is a registered trademark.

Microsoft and Windows 10 are either registered trademarks or brand names owned by Microsoft Corp. in the U.S.A. and/or in other countries.

Stormshield is a trademark of Stormshield in France and other countries.

Any other third-party trademarks mentioned in this document are the property of their respective owners.

All reproduction rights are reserved, including for iconographic or photographic representations. No part of this document may be copied and/or published by any means whatsoever without our express written consent.

All the information provided is subject to modifications at any time and without notice.

Despite our utmost care and attention in producing this document and its regular updates, errors may have been introduced in the information provided. If you notice any issues, please feel free to contact us and let us know. We will make the necessary changes.

Table of contents

1	Introduction	1
1.1	Purpose of document.....	1
1.2	DR mode.....	1
1.3	Software versions used.....	1
2	Configuring the Stormshield firewall.....	2
2.1	Enabling writing mode	2
2.2	Enabling ANSSI Diffusion Restreinte mode	2
2.3	Configuring Network/Interfaces	3
2.4	Creating certificates	3
2.4.1	Creating a Root Authority.....	3
2.4.2	Creating a User Identity	6
2.4.3	Creating a Server Identity.....	10
2.4.4	Exporting certificates.....	14
2.5	VPN encryption profiles	15
2.5.1	IKE profile	16
2.5.2	IPsec profile.....	16
2.6	Identification.....	17
2.7	Peers.....	18
2.8	Creating a CRL.....	23
2.9	Configuring a mobile policy	23
2.10	Filtering rules	25
3	Configuring TheGreenBow VPN Client.....	26
3.1	Launching the VPN Client.....	26
3.2	Creating a new IKE Auth	26
3.2.1	Authentication tab	26
3.2.2	Protocol tab	28
3.2.3	Gateway tab.....	29
3.2.4	Certificate tab.....	29
3.2.5	More Parameters tab	31
3.3	Creating a new Child SA.....	33



- 3.4 Saving the configuration..... 33
- 3.5 Opening the VPN connection 34
- 4 Troubleshooting 35**
 - 4.1 SNS firewall..... 35
 - 4.1.1 Disabled CRL validation is not DR compliant..... 35
 - 4.2 VPN Client..... 37
 - 4.2.1 NO_PROPOSAL_CHOSEN 37
 - 4.2.2 AUTHENTICATION_FAILED 37
 - 4.2.3 No user certificate available for the connection..... 38
 - 4.2.4 Remote IDr rejected..... 38
 - 4.2.5 FAILED_CP_REQUIRED..... 38
- 5 Contact..... 39**
 - 5.1 Information..... 39
 - 5.2 Sales..... 39
 - 5.3 Support 39

Document revision history

Version	Date	Sections/pages concerned	Description of change	Author
1.0	2021-12-01	All	Initial draft	BB
1.1	2022-02-10	All	Updated for SNS 4.2 with new screenshots	AL, NT
1.2	2022-02-18	1.2 4.1.1	Corrected a typographical error. Added another method to enable CRL validation.	
1.3	2022-02-25	1.2 2.7	Corrected the version number of the DR mode. Corrected the CN value to be entered in the Peer ID field.	

1 Introduction

1.1 Purpose of document

This configuration guide describes how to configure TheGreenBow Windows Enterprise VPN Client version 6.8 to establish VPN connections to the Stormshield SNS firewall version 4.2, using ANSSI *Diffusion Restreinte*¹ (DR) mode.

1.2 DR mode

In this document, we will configure the Stormshield SNS firewall with the ANSSI *Diffusion Restreinte* (DR) mode turned on.



For more information on the ANSSI *Diffusion Restreinte* (DR) mode introduced in SNS firewall version 4.2, refer to the following page: https://documentation.stormshield.eu/SNS/v4/en/Content/Release_Notes_SNS/4.2.1-Features.htm.

To do this, we will set up the following configuration:

- Protocol: IPsec IKEv2
- Diffie Hellman: DH19
- Encryption: AES GCM 256
- Authentication: Certificate, using Method 9 (ECDSA with SHA-256 on the P-256 SECP curve and SHA256)
- Certificate revocation: CRL enabled
- UDP port: 4500

1.3 Software versions used

We used the following software versions to draft this document:

- Stormshield SNS version 4.2.8
- TheGreenBow Windows Enterprise VPN Client version 6.86.015

The instructions contained in this configuration guide should also work with newer versions of the Stormshield SNS firewall and TheGreenBow Windows Enterprise VPN Client.

¹ *Diffusion Restreinte* means restricted information.



2 Configuring the Stormshield firewall

This section describes how to configure your Stormshield firewall.

2.1 Enabling writing mode

On the top right corner of the configuration window, you should see the following screen:



You must be in writing mode to be able to edit and save the configuration.

If this is not the case, and you see the following:

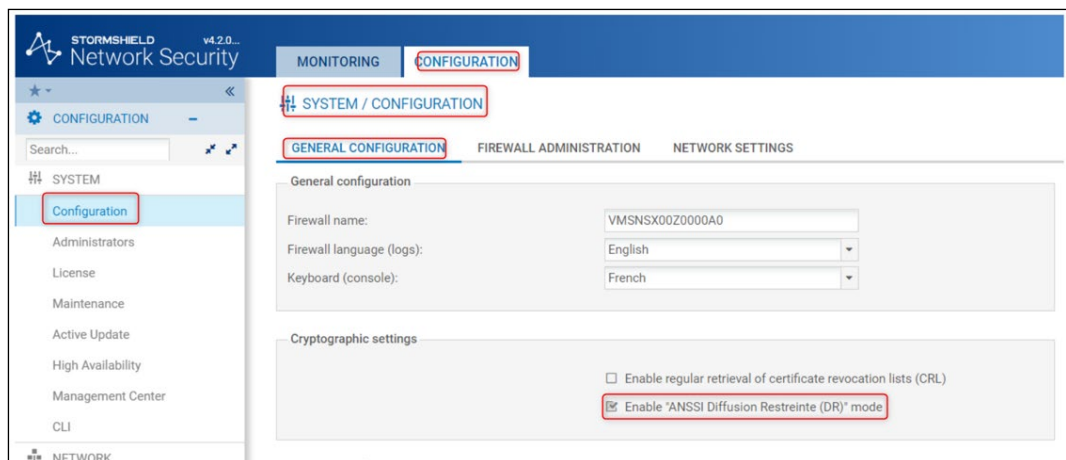


Click **READING**. The writing mode is enabled.

2.2 Enabling ANSSI Diffusion Restreinte mode

Once you have logged in to your Stormshield Network Security firewall, proceed as follows in the user interface:

1. From the left menu, select **SYSTEM** and then **Configuration**.
2. Under the **GENERAL CONFIGURATION** tab, click **Enable "ANSSI Diffusion Restreinte (DR)" mode**.



3. Click **APPLY**.

4. Click **Save This Configuration**.
5. The following message is displayed: “You will need to restart your appliance to apply changes”.

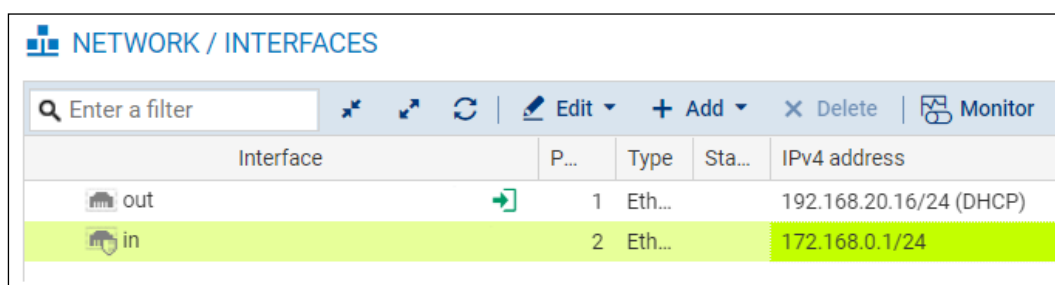


6. Click on the **Restart** icon () to restart.

2.3 Configuring Network/Interfaces

Once you have enabled the ANSSI DR mode, proceed as follows to configure the Network/Interfaces:

1. From the left menu, select **Network** and then **Interfaces**.
2. Configure the WAN (**out**) and LAN (**in**) network interfaces to reflect your network topology. The following is an example:



Interface	P...	Type	Sta...	IPv4 address
out	1	Eth...		192.168.20.16/24 (DHCP)
in	2	Eth...		172.168.0.1/24

2.4 Creating certificates

To create the required certificates, from the left menu, select **OBJECTS / CERTIFICATE AND PKI** and then **CONFIGURATION**.

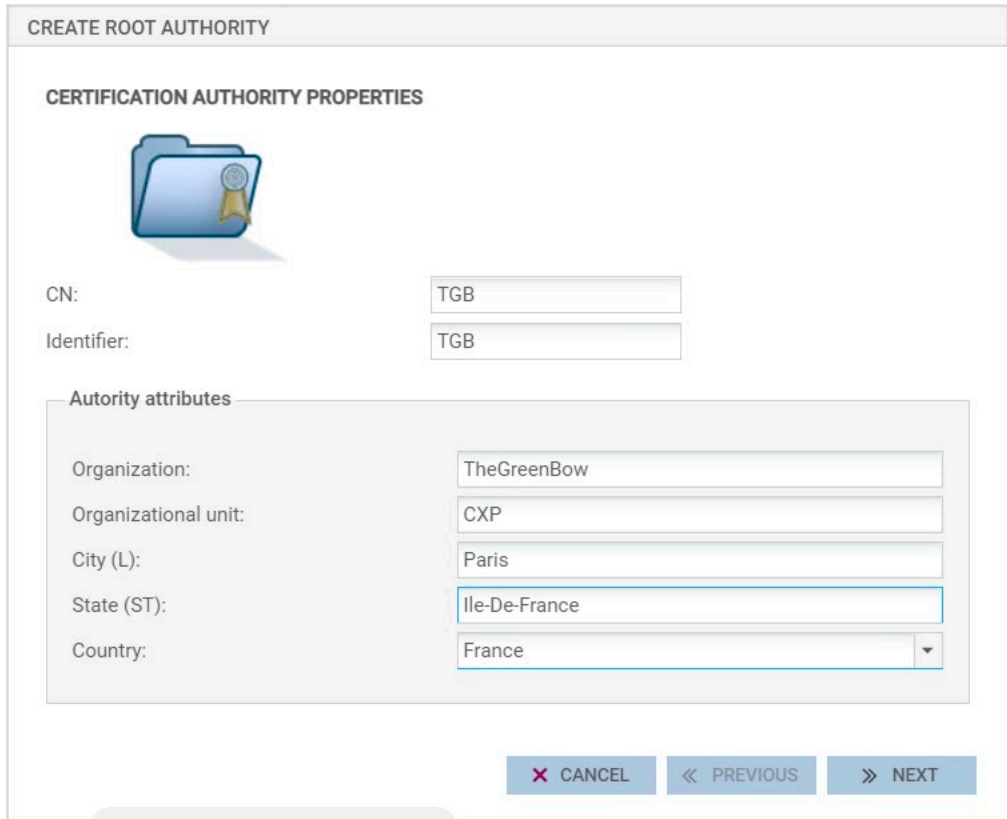
Follow the instructions below to create a set consisting of a Root Authority (CA), a User Identity, and a Server Identity.

2.4.1 Creating a Root Authority

To create a Root Authority, proceed as follows:

1. Click **+ Add Root Authority**.

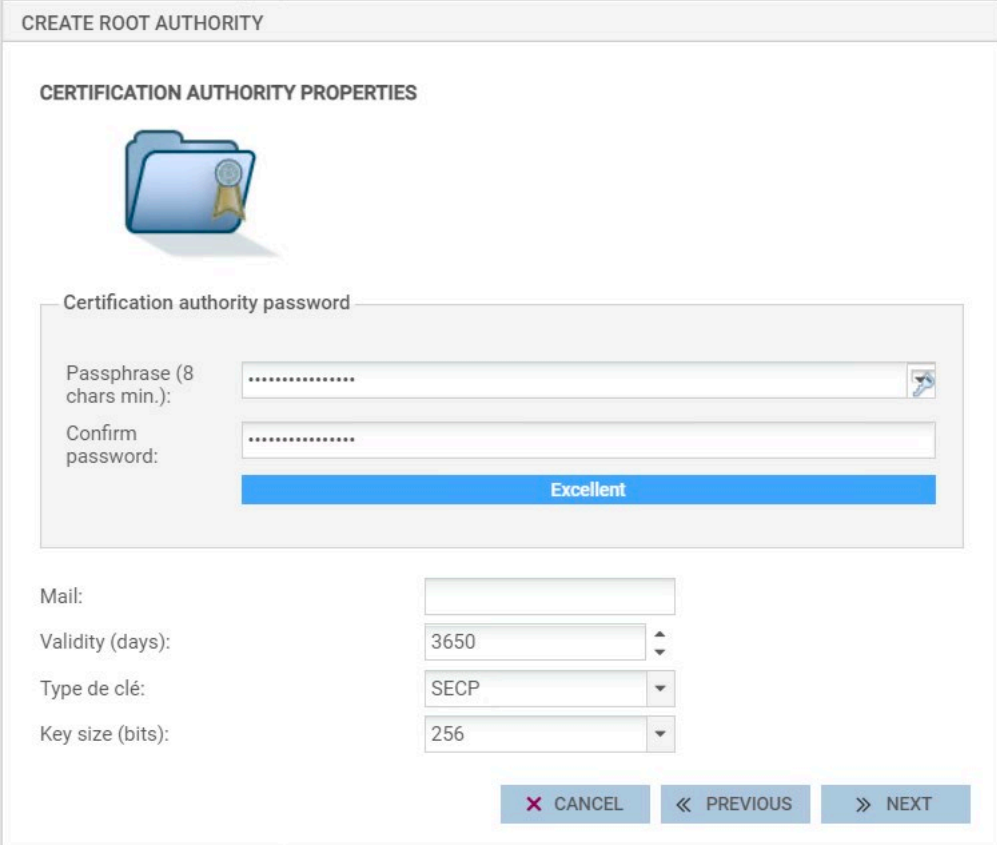
2. Fill in the **Root Authority Certificate** with relevant values for the **Authority attributes**, i.e. Organization, Organizational unit, City, State, and Country, as shown in the following screenshot.



The screenshot shows a Windows dialog box titled "CREATE ROOT AUTHORITY". Inside, there is a section for "CERTIFICATION AUTHORITY PROPERTIES" with a folder icon. Below the icon, there are two input fields: "CN:" with the value "TGB" and "Identifier:" with the value "TGB". A section titled "Authority attributes" contains five fields: "Organization:" (TheGreenBow), "Organizational unit:" (CXP), "City (L):" (Paris), "State (ST):" (Ile-De-France), and "Country:" (France). At the bottom right, there are three buttons: "X CANCEL", "<< PREVIOUS", and ">> NEXT".


3. Click » **NEXT**.

4. Enter a passphrase to secure the certification authority, making sure to keep it for later use.
5. Choose the relevant **Validity** (days), and then select **SECP** with a key size of 256 bits.



CREATE ROOT AUTHORITY

CERTIFICATION AUTHORITY PROPERTIES



Certification authority password

Passphrase (8 chars min.):

Confirm password:

Excellent

Mail:

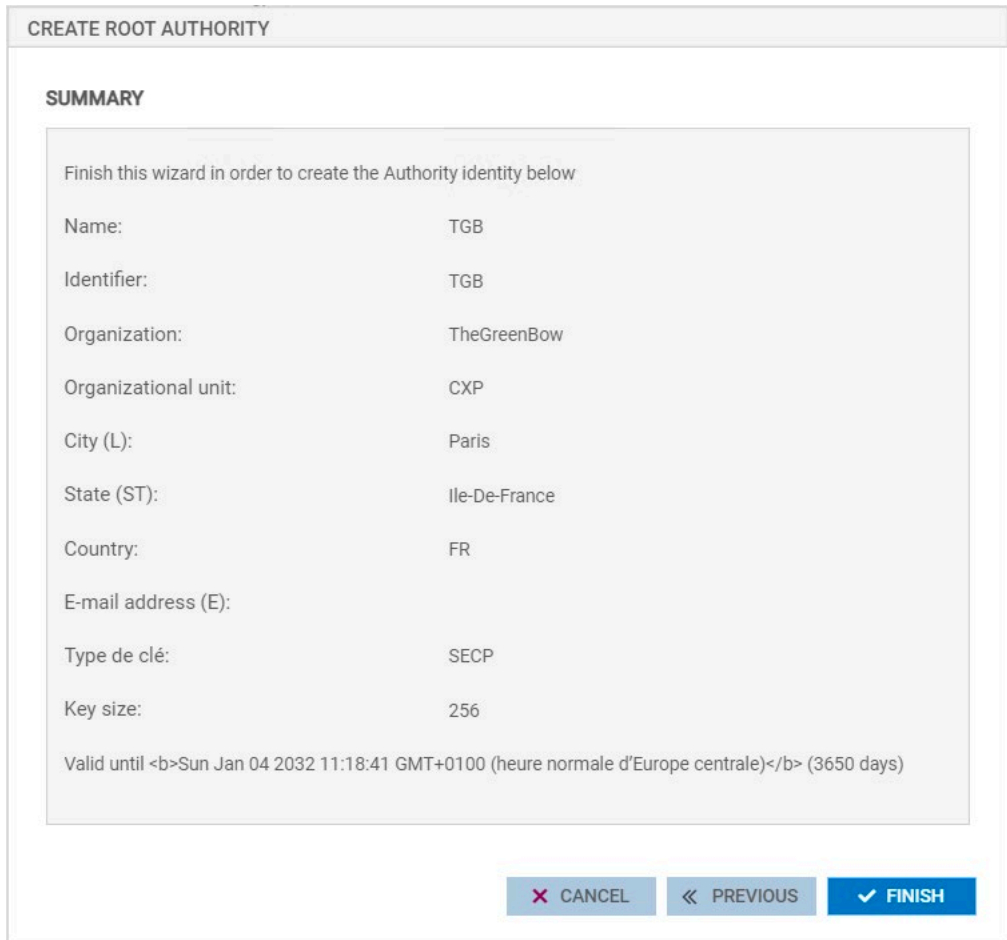
Validity (days):

Type de clé:

Key size (bits):

6. Click » **NEXT**.

The summary should appear as follows:



CREATE ROOT AUTHORITY

SUMMARY

Finish this wizard in order to create the Authority identity below

Name:	TGB
Identifier:	TGB
Organization:	TheGreenBow
Organizational unit:	CXP
City (L):	Paris
State (ST):	Ile-De-France
Country:	FR
E-mail address (E):	
Type de clé:	SECP
Key size:	256

Valid until Sun Jan 04 2032 11:18:41 GMT+0100 (heure normale d'Europe centrale) (3650 days)

X CANCEL **<< PREVIOUS** **✓ FINISH**

7. Click **FINISH**.

2.4.2 Creating a User Identity


To create a User Identity, proceed as follows:

1. Click **+ Add User Identity**.

2. Fill in the **CN**, **Identifier**, and **Mail** fields.

CREATE A USER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



CN:

Identifier:


Mail:

3. Click » **NEXT**.

4. In the **Parent CA** drop-down list, select the Root Authority that you created in the previous section.
5. Enter the **CA passphrase** that you have set for this Root Authority.
6. Fill in the **Authority attributes** fields.

CREATE A USER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Select the parent Authority

Parent CA:	TGB	▼ ×
CA passphrase:	🔒

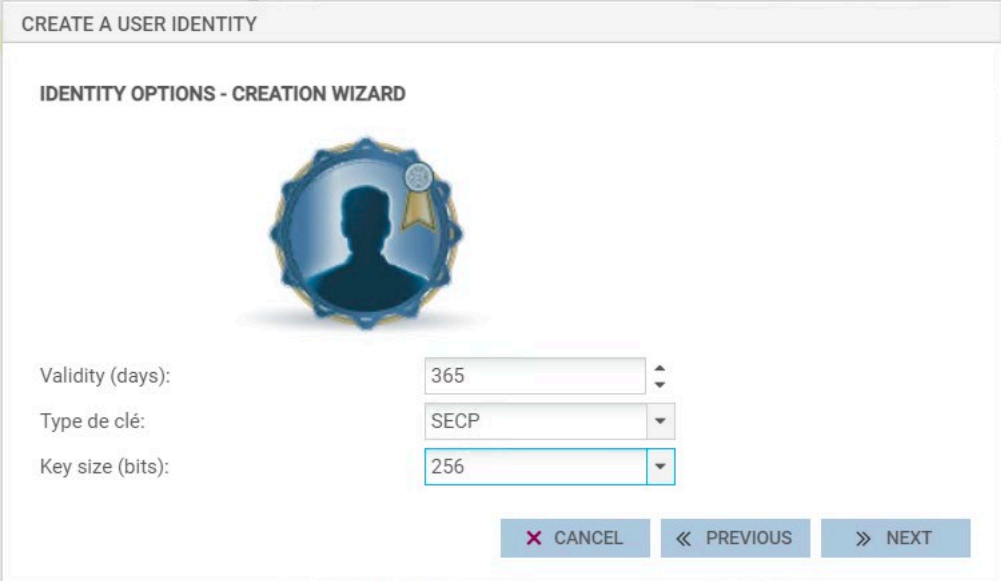
Authority attributes

Organization:	TheGreenBow	
Organizational unit:	CXP	
City (L):	Paris	
State (ST):	Ile-De-France	
Country:	France	▼

✖ CANCEL
⏪ PREVIOUS
NEXT ⏩

7. Click » **NEXT**.

8. Choose the relevant **Validity** (days), and then select **SECP** with a key size of 256 bits.



CREATE A USER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD

Validity (days): 365

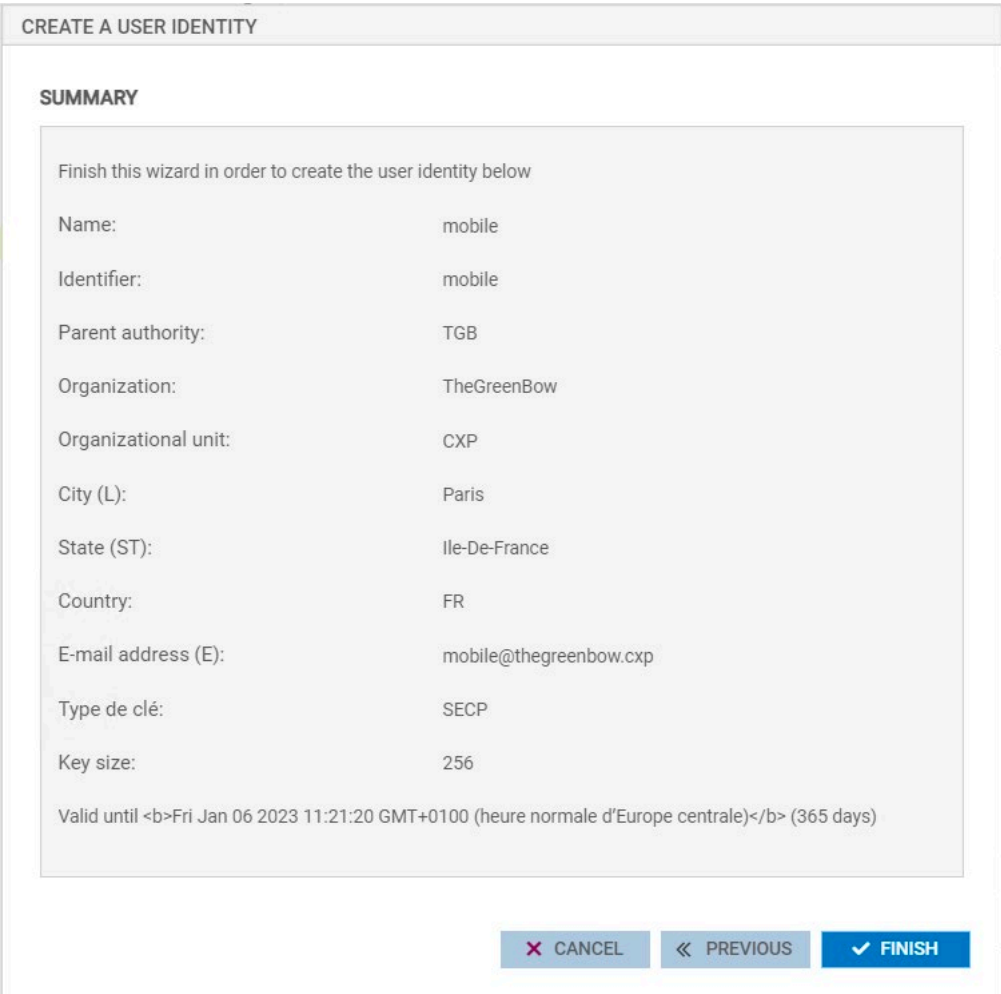
Type de clé: SECP

Key size (bits): 256

X CANCEL << PREVIOUS >> NEXT

9. Click » **NEXT**.

The summary should appear as follows:



CREATE A USER IDENTITY

SUMMARY

Finish this wizard in order to create the user identity below

Name:	mobile
Identifier:	mobile
Parent authority:	TGB
Organization:	TheGreenBow
Organizational unit:	CXP
City (L):	Paris
State (ST):	Ile-De-France
Country:	FR
E-mail address (E):	mobile@thegreenbow.cxp
Type de clé:	SECP
Key size:	256

Valid until Fri Jan 06 2023 11:21:20 GMT+0100 (heure normale d'Europe centrale) (365 days)

X CANCEL **<< PREVIOUS** **✓ FINISH**

10. Click **FINISH**.

2.4.3 Creating a Server Identity

To create a Server Identity, proceed as follows:

1. Click **+ Add Server Identity**.

2. Fill in the **FQDN** and **ID** fields.



CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD

Fully Qualified Domain Name (FQDN): firewallecdsa.xp

ID: firewallecdsa


X CANCEL << PREVIOUS >> NEXT

3. Click » **NEXT**.

4. In the **Parent CA** drop-down list, select the Root Authority that you created in the previous section
5. Enter the **CA passphrase** that you have set for this Root Authority.
6. Fill in the **Authority attributes** fields.

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Select the parent Authority

Parent CA:

CA passphrase:

Authority attributes

Organization:

Organizational unit:

City (L):

State (ST):

Country:


✖ CANCEL
⏪ PREVIOUS
» NEXT

7. Click » **NEXT**.

- Choose the relevant **Validity** (days), and then select **SECP** with a key size of 256 bits.

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Validity (days): 365

Type de clé: SECP

Key size (bits): 256

- Click » **NEXT**.

The summary should appear as follows:

CREATE A SERVER IDENTITY

SUMMARY

Finish this wizard in order to create the server identity below

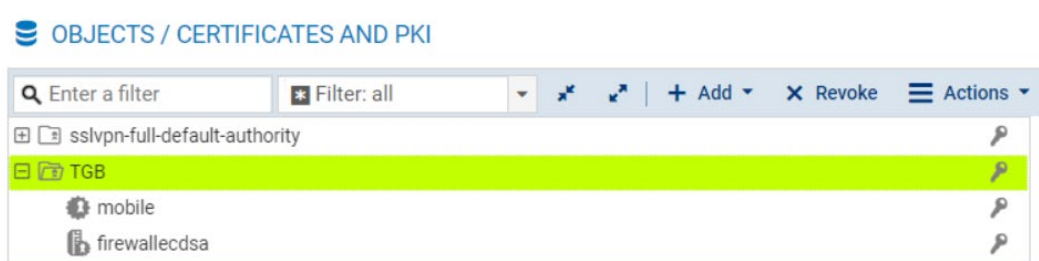
Name:	firewallecdsa.cxp
Identifier:	firewallecdsa
Parent authority:	TGB
Organization:	TheGreenBow
Organizational unit:	CXP
City (L):	Paris
State (ST):	Ile-De-France
Country:	FR
Type de clé:	SECP
Key size:	256

Valid until Fri Jan 06 2023 11:23:37 GMT+0100 (heure normale d'Europe centrale) (365 days)

10. Click **FINISH**.

In the left-hand menu, you should now see the following:

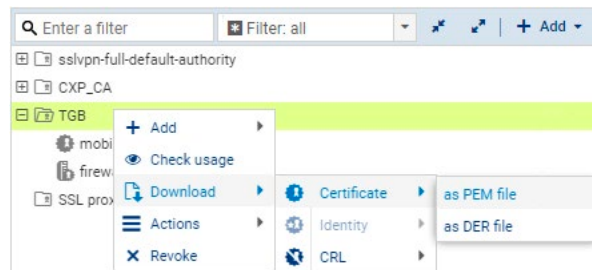
- A Root Authority (e.g. **TGB**) that contains the following two items:
 - A User Identity (e.g. **mobile**)
 - A Server Identity (e.g. **firewallecdsa**)



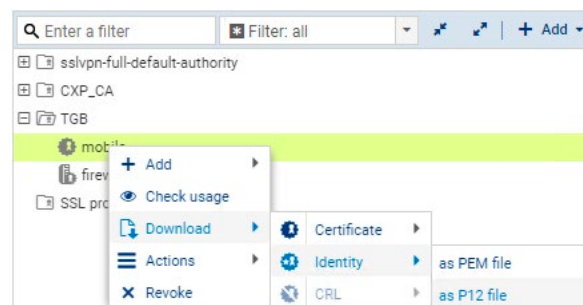
2.4.4 Exporting certificates

To export the certificates, proceed as follows:

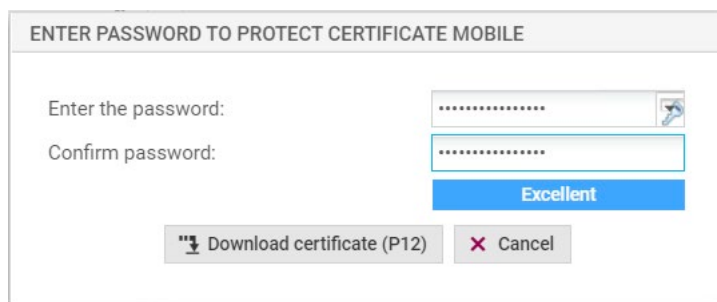
1. Start by downloading the Root Authority. To do so, right-click the Root Authority (e.g. TGB), and then select **Download > Certificate > as PEM file**.



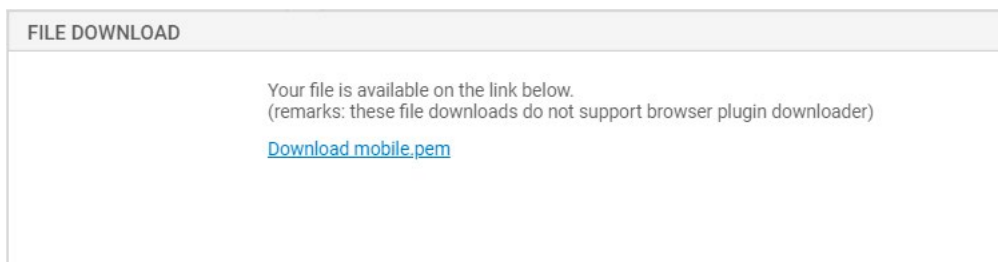
2. Download the User Identity. To do so, right-click the User Identity (e.g. mobile), and then select **Download > Identity > as P12 file**.



3. Enter a password to protect the P12 file.



4. Click **Download certificate (P12)**.



5. Click **Download User_Identity.pem** (in this case, mobile is the name of the user identity).



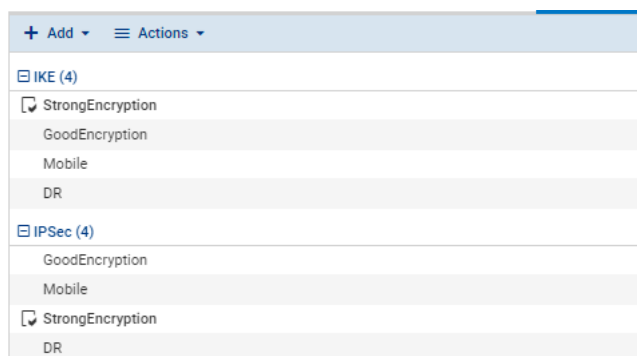
You will later need to import this P12 file into the VPN Client, using the password that you just set.

2.5 VPN encryption profiles

To generate the VPN encryption profiles, proceed as follows:

1. From the left menu, select **VPN / IPSEC VPN** and then **ENCRYPTION PROFILES**.

You should see the following screen:

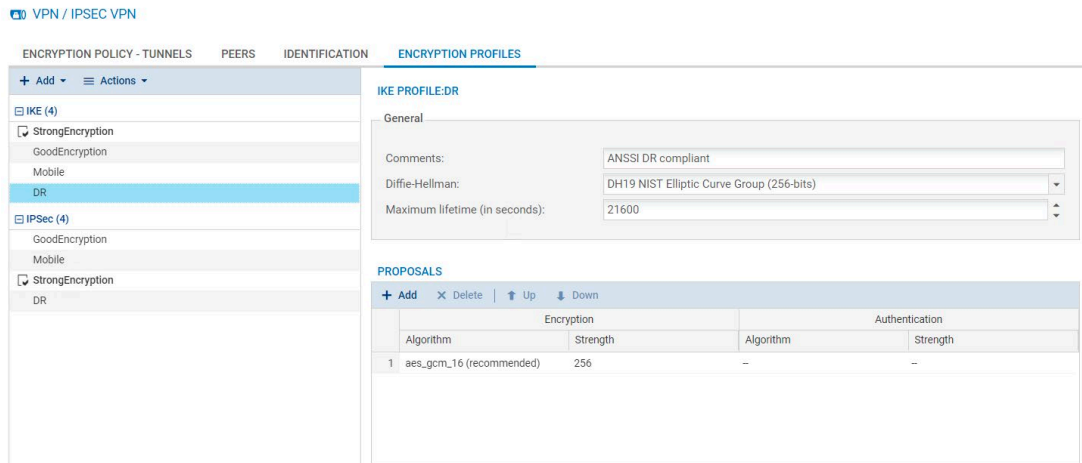


2. Proceed with generating the IKE and IPsec profiles as described below.

2.5.1 IKE profile

To generate the IKE profile, proceed as follows:

1. Under **IKE (4)**, select **DR**.
2. Configure the following parameters:
 - Diffie-Hellman: DH 19 NIST Elliptic Curve Group (256-bits)
 - Maximum lifetime (in seconds): 21600
 - Encryption proposal: aes_gcm_16 (Strength: 256)



The screenshot shows the configuration interface for the IKE profile. The left sidebar shows a tree view with 'IKE (4)' expanded and 'DR' selected. The main area is titled 'IKE PROFILE:DR' and contains the following configuration fields:

- General**
 - Comments: ANSSI DR compliant
 - Diffie-Hellman: DH19 NIST Elliptic Curve Group (256-bits)
 - Maximum lifetime (in seconds): 21600
- PROPOSALS**

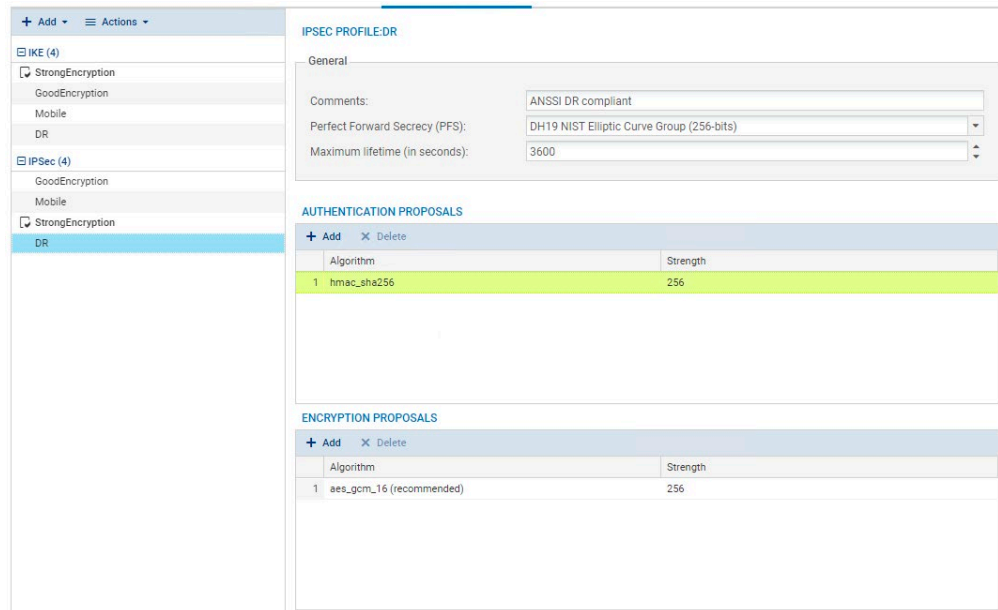
	Encryption		Authentication	
	Algorithm	Strength	Algorithm	Strength
1	aes_gcm_16 (recommended)	256	--	--

3. Click **APPLY**.
4. Click **SAVE**.
5. Click **YES, ACTIVATE NOW**.

2.5.2 IPsec profile

To generate the IPsec profile, proceed as follows:

1. Under **IPSec (4)** select **DR** and configure the following parameters:
 - Diffie-Hellman: DH 19 NIST Elliptic Curve Group (256-bits)
 - Maximum lifetime (in seconds): 3600
 - Authentication Proposals: Hmac_sha256 (256)
 - Encryption proposal: aes_gcm_16 (Strength: 256)

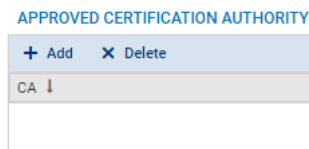


2. Click **APPLY**.
3. Click **SAVE**.
4. Click **YES, ACTIVATE NOW**.

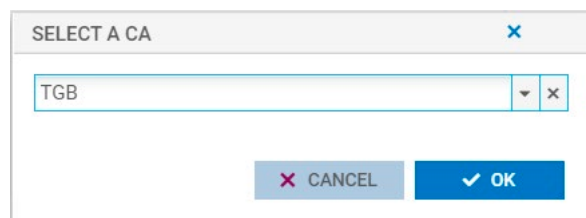
2.6 Identification

To add an identification, proceed as follows:

1. From the left menu, select **VPN / IPSEC VPN** and then **IDENTIFICATION**.
2. On the **APPROVED CERTIFICATION AUTHORITY** tab, click **+ Add**.

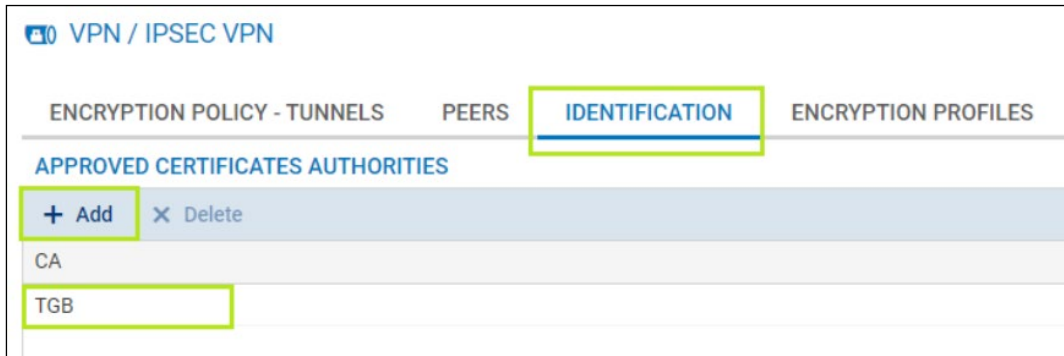


3. Select the CA that you created earlier (e.g. TGB) from the list.



4. Click **OK**.

You should now see the following screen:

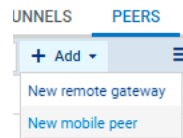


5. Click **APPLY**.

2.7 Peers

To create a peer, proceed as follows:

1. From the left menu, select **VPN / IPSEC VPN** and then **PEERS**.



2. Click **+ Add**.
3. Select **New mobile peer**.
4. In the **CREATE PEER MOBILE** window:
 - Enter a name (e.g. mobile_dr)
 - Select **IKE v2**.

CREATE PEER MOBILE

SELECTING THE GATEWAY - PEER CREATION WIZARD



Name:

IKE version:

5. Click » **NEXT**.

CREATE A MOBILE PEER

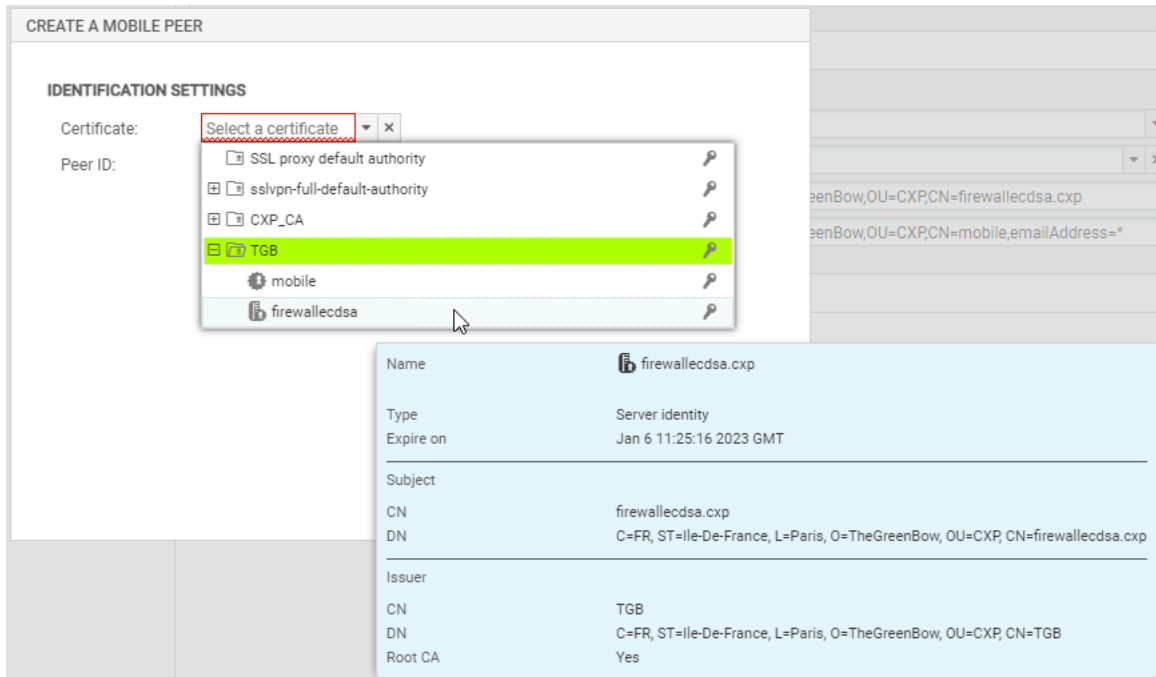
PEER IDENTIFICATION - PEER CREATION WIZARD

Authentication type:

- Certificate
- Certificate and Xauth (iPhone)

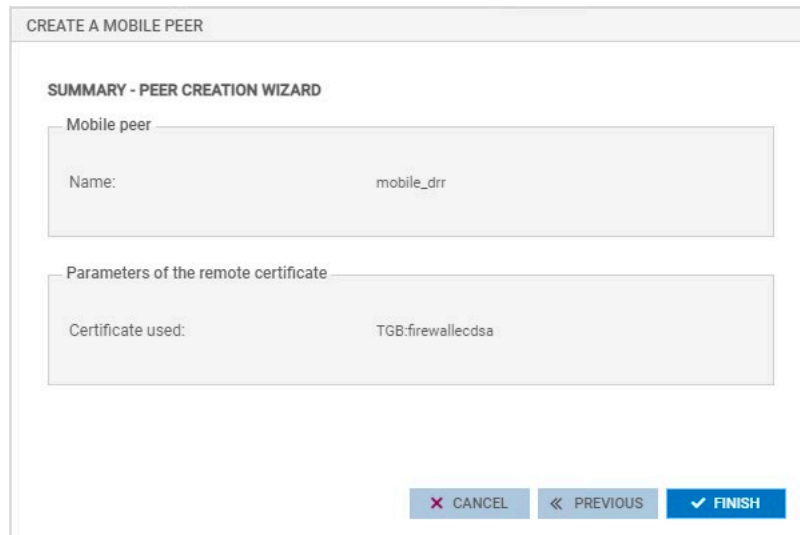
6. Click » **NEXT**.

- In the next screen, select the Server Identity that you created earlier (e.g firewallecdsa).



Ignore the **PEER ID** field at this stage.

- Click » **NEXT**.



- Click **FINISH**.

You should see the following screen:

MOBILE_DR

General

Comment:

Remote gateway: Any

Local address: Any

IKE profile: DR

IKE version: IKEv2

Identification

Authentication method: Certificate

Certificate: firewallecdsa

Local ID: Enter an ID (optional)

Peer ID: Enter an ID

Advanced properties

Do not initiate the tunnel (Responder only)

IKE fragmentation

DPD: Passive

DSCP: 00 Best effort

10. Copy the **Issued** field from the Server Identity that you created under **CERTIFICATES AND PKI / CONFIGURATION** (see section 2.4.3 Creating a Server Identity) and paste it into the **Local ID** field.

For example:

```
C=FR, ST=Ile-De-France, L=Paris, O=TheGreenBow, OU=CXP, CN=firewallecdsa.cxp
```

11. Copy the **Issued** field from the User Identity that you created under **CERTIFICATES AND PKI / CONFIGURATION** (see section 2.4.2 Creating a User Identity) and paste it into the **Peer ID** field, making sure to replace the **CN** and **emailAddress** values with a wildcard (“*”).



Using wildcards will allow you to use the same configuration for all mobile users, each having a different Peer ID.

For instance, if the **Issued for** screen shows the following information:

Issued for	
Issuer:	C=FR,ST=Ile-De-France,L=Paris,O=TheGreenBow,OU=CXP,CN=mobile,emailAddress=mobile@thegreenbow.cxp
Common Name:	mobile
Organization Name:	TheGreenBow
Organization Unit Name:	CXP
Locality Name:	Paris
State Or Province Name:	Ile-De-France
Country Name:	FR
Email Address:	mobile@thegreenbow.cxp
Subject hash:	131d4541

Then the **Peer ID** field should contain the following value:

C=FR, ST=Ile-De-France, L=Paris, O=TheGreenBow, OU=CXP, CN=*, emailAddress=*

The screen should now appear as follows:

MOBILE_DR

General

Comment:

Remote gateway: Any

Local address: Any

IKE profile: DR

IKE version: IKEv2

Identification

Authentication method: Certificate

Certificate: firewallecdsa

Local ID: C=FR,ST=Ile-De-France,L=Paris,O=TheGreenBow,OU=CXP,CN=firewallecdsa.cxp

Peer ID: C=FR,ST=Ile-De-France,L=Paris,O=TheGreenBow,OU=CXP,CN=*,emailAddress=*

Advanced properties

Do not initiate the tunnel (Responder only)

IKE fragmentation

DPD: Passive

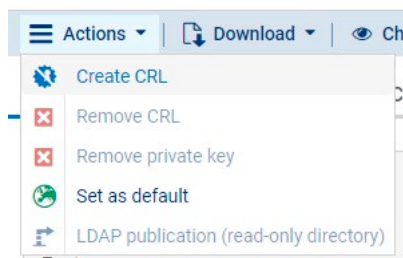
DSCP: 00 Best effort

12. Click **APPLY**.
13. Click **SAVE**.
14. Click **YES, ACTIVATE NOW**.

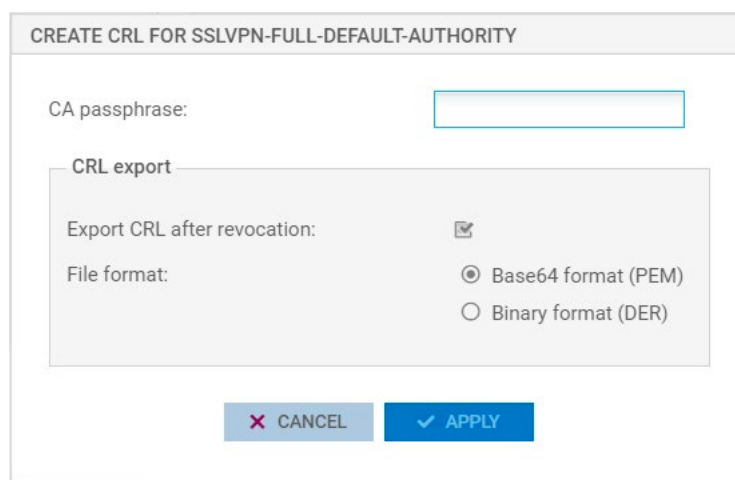
2.8 Creating a CRL

To create a CRL, proceed as follows:

1. From the left menu, select **OBJECTS / CERTIFICATES AND PKI**, click **Actions** and then select **Create CRL**.



2. Enter the **CA passphrase**.
3. Check **Export CRL after revocation** and select **Base64 format (PEM)**.

A screenshot of a dialog box titled 'CREATE CRL FOR SSLVPN-FULL-DEFAULT-AUTHORITY'. It contains a text input field for 'CA passphrase:'. Below it is a section titled 'CRL export' which includes a checkbox for 'Export CRL after revocation:' (checked) and radio buttons for 'File format:' with 'Base64 format (PEM)' selected and 'Binary format (DER)' unselected. At the bottom are 'CANCEL' and 'APPLY' buttons.

4. Click **APPLY**.
5. Download the generated CRL file (we will not use it in this document).

2.9 Configuring a mobile policy

To configure a mobile policy, proceed as follows:

1. From the **VPN / IPSEC VPN** menu, select the **Encryption Policy - Tunnels** tab.
2. Select **Mobile - Mobile Users** and then click **+ Add**.
3. Choose **New Config mode mobile policy**.

VPN / IPSEC VPN

ENCRIPTION POLICY - TUNNELS PEERS IDENTIFICATION

IPsec 01 (01) Actions ⓘ

SITE TO SITE (GATEWAY-GATEWAY) MOBILE - MOBILE USERS

Enter a filter + Add X Delete ↑ Up

	Status
1	on

New standard mobile policy
New Config mode mobile policy
Separator (rule grouping)

4. On the following screen fill in the fields as follows:

- Local resources: Network_in
- Peer selection: mobile_dr
- Remote networks: Network_out

MOBILE IPSEC VPN POLICY WIZARD WITH CONFIG MODE

Only one local network can be defined for authenticated users to access through an IPsec tunnel
In Config mode, users present with an IP address from an address pool defined by the administrator for all remote users

Local resources: Network_in

Peer selection: mobile_dr

Remote networks: Network_out

X CANCEL ✓ FINISH

5. Click **FINISH**.

You should now see the following screen:

ENCRIPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

IPsec 01 (01) Actions ⓘ

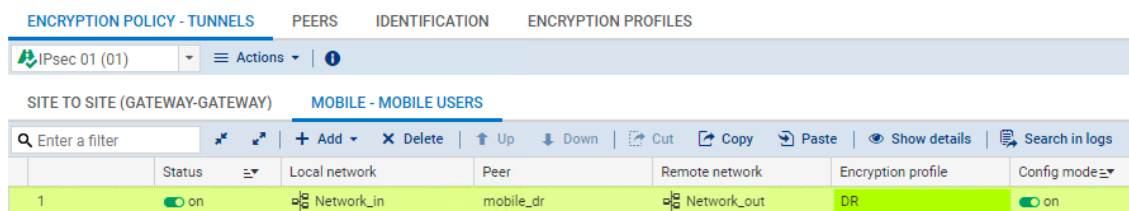
SITE TO SITE (GATEWAY-GATEWAY) MOBILE - MOBILE USERS

Enter a filter + Add X Delete ↑ Up ↓ Down Cut Copy Paste Show details Search in logs

	Status	Local network	Peer	Remote network	Encryption profile	Config mode
1	off	Network_in	mobile_dr	Network_out	StrongEncryption	on

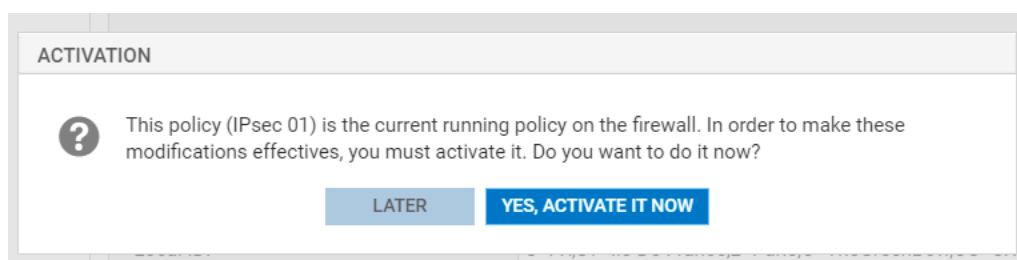
- 6. Switch the **Status** to **ON**.
- 7. Change **Encryption profile** to **DR**.

You should now see the following screen:



	Status	Local network	Peer	Remote network	Encryption profile	Config mode
1	on	Network_in	mobile_dr	Network_out	DR	on

8. Click **APPLY**.
9. Click **FINISH**.
10. Click **SAVE**.



11. Click **YES, ACTIVATE IT NOW**.

2.10 Filtering rules

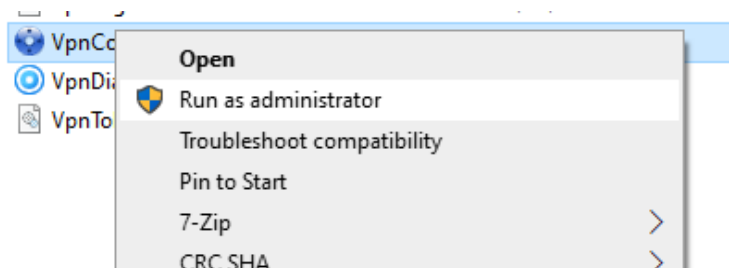
Where appropriate, integrate the filtering rules to allow IPsec traffic through the configured SNS network interfaces (refer to SNS documentation).

3 Configuring TheGreenBow VPN Client

This section describes the required configuration for TheGreenBow's Windows Enterprise VPN Client to connect to the SNS firewall configured according to the instructions set forth in the previous section.

3.1 Launching the VPN Client

By default, only administrators can access the Windows Enterprise VPN Client Configuration Panel. Therefore, right-click **vpnconf.exe** in the **File Explorer** and select **Run as administrator**.



3.2 Creating a new IKE Auth

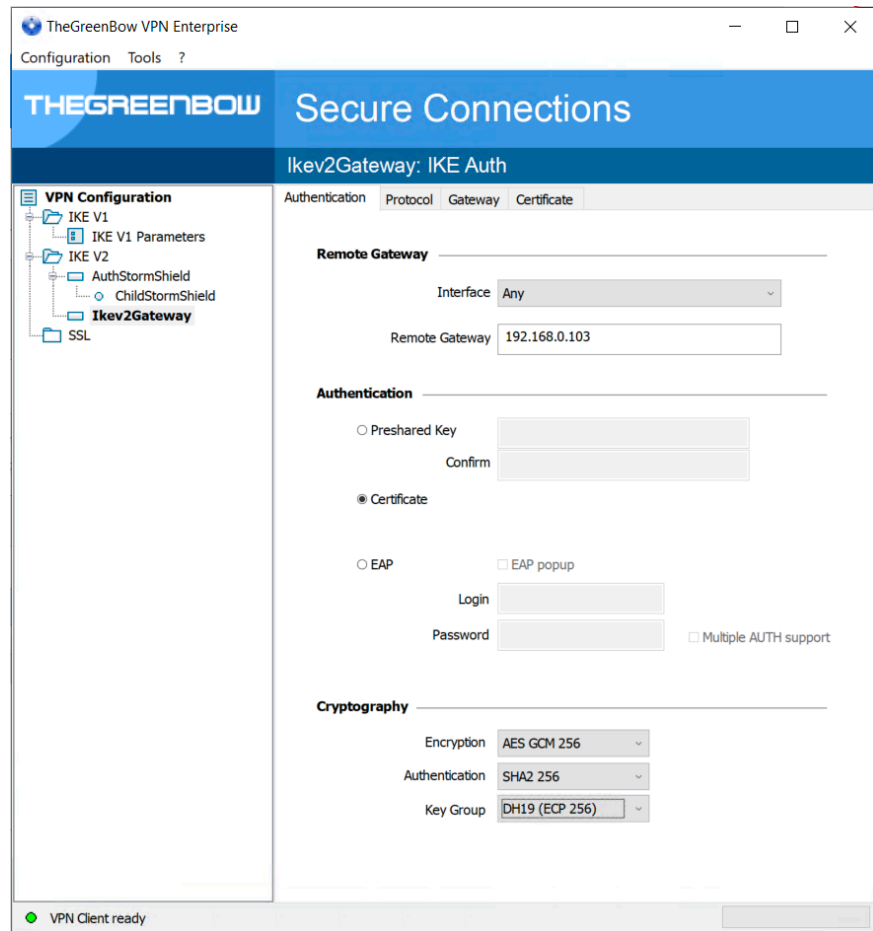
Configure TheGreenBow Windows Enterprise VPN Client as described below.

Start by creating a new IKEv2 IKE Auth. To do so, right-click the IKE v2 branch of the VPN configuration tree and select **New IKE Auth**.

3.2.1 Authentication tab

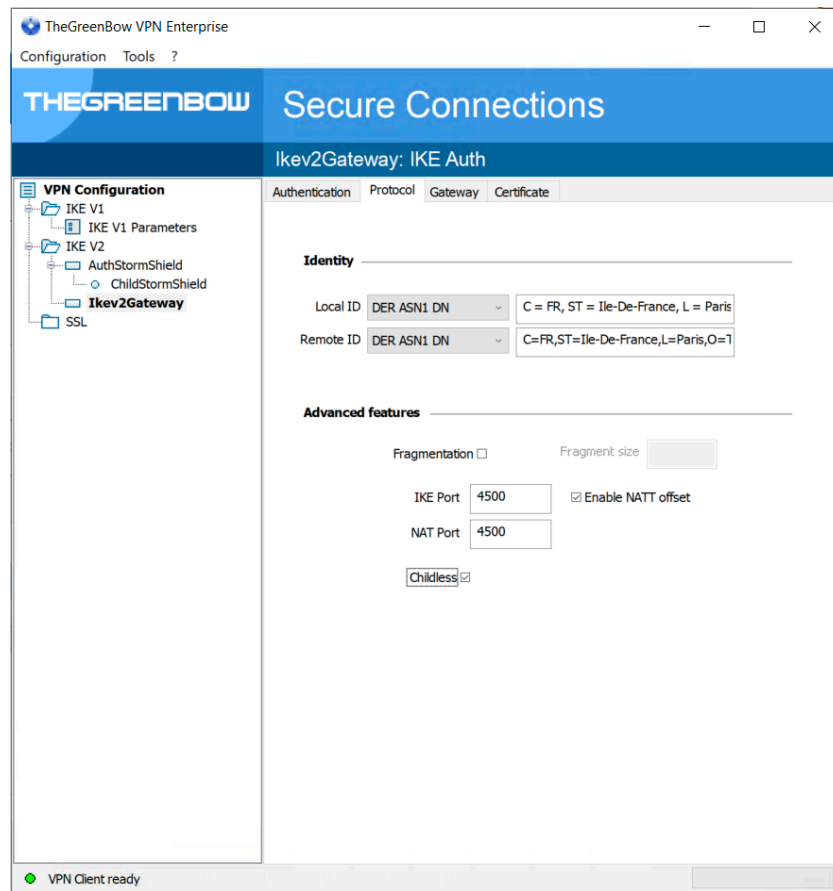
Select the **Authentication** tab and enter the following parameters:

- Interface: Any
- Remote Gateway: the IP address of the SNS gateway in your network.
- Authentication: certificate
- Cryptography:
 - Encryption: AES GCM 256
 - Authentication: SHA2 256
 - Key Group: DH19 (ECP 256)



3.2.2 Protocol tab

Set the following additional parameters in the **Protocol** tab:



The **Local ID** DER ASN1 DN will be automatically updated with the subject from the imported certificate (see below).

The **Remote ID** must be of type DER ASN1 DN and contain the same value as the **Local ID** field of the SNS (see step 10 in section 2.7 Peers), for example:

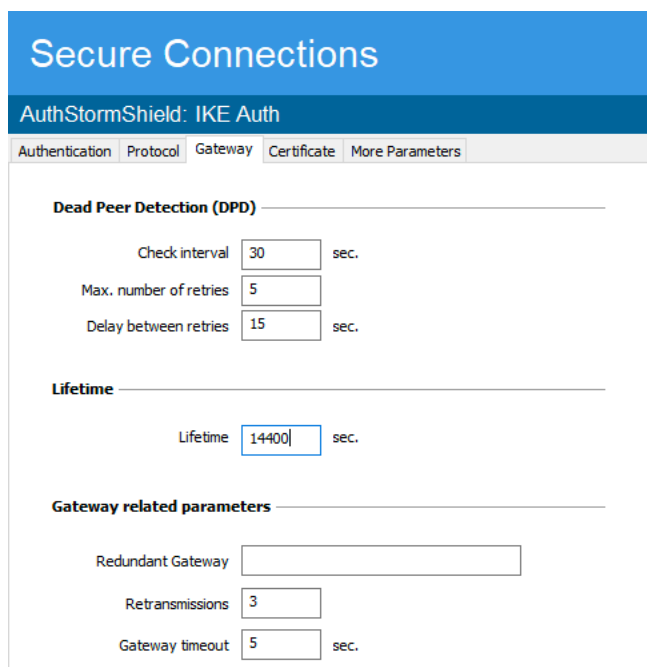
```
C=FR, ST=Ile-De-France, L=Paris, O=TheGreenBow, OU=CXP, CN=firewallecdsa.cxp
```

Under Advanced features, set the following parameters:

- IKE port: 4500
- Nat Port 4500
- Childless: selected

3.2.3 Gateway tab

You can keep the default parameters on the **Gateway** tab or change them according to your requirements.



Secure Connections

AuthStormShield: IKE Auth

Authentication Protocol **Gateway** Certificate More Parameters

Dead Peer Detection (DPD)

Check interval sec.

Max. number of retries

Delay between retries sec.

Lifetime

Lifetime sec.

Gateway related parameters

Redundant Gateway

Retransmissions

Gateway timeout sec.

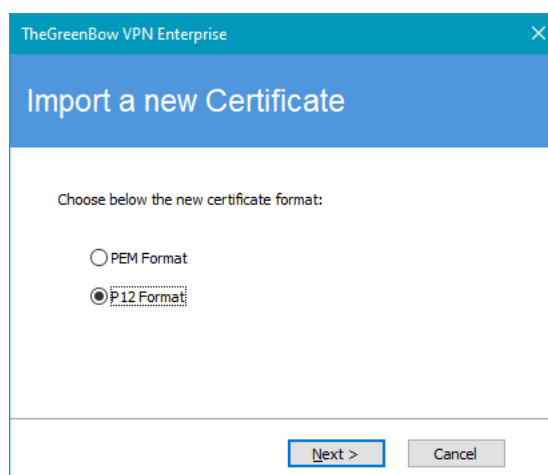


We recommend that you configure a lower lifetime value in the VPN Client than in the firewall, so that renegotiations are initiated by the VPN Client (in this case, we use 14400 for the VPN Client and 28800 for the firewall).

3.2.4 Certificate tab

To import the user certificate, proceed as follows:

1. Select the **Certificate** tab.
2. Click **Import Certificate...**



TheGreenBow VPN Enterprise

Import a new Certificate

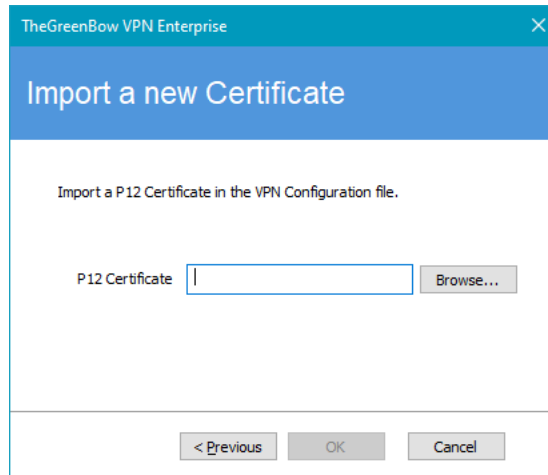
Choose below the new certificate format:

PEM Format

P12 Format

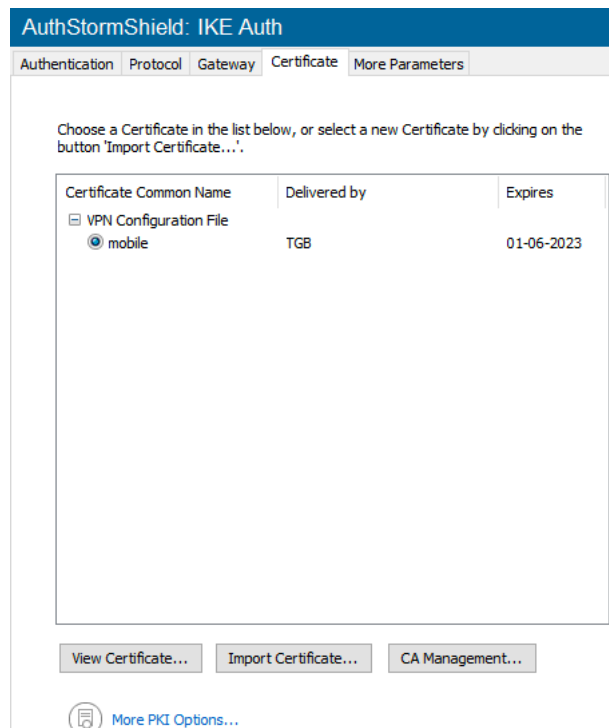
Next > Cancel

3. Select **P12 Format**.
4. Click **Next >**.



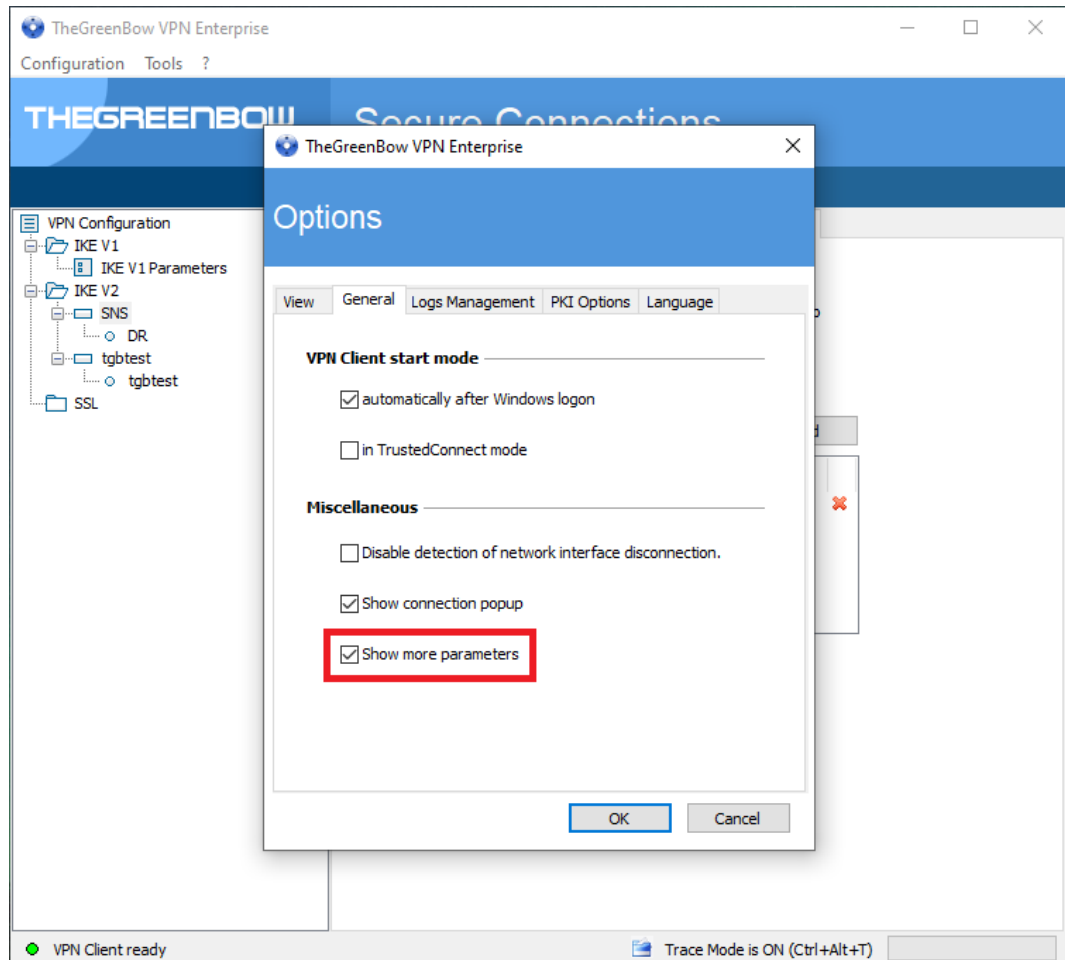
5. Click **Browse...**
6. Select the User Identity that you have previously downloaded from the SNS firewall (e.g. Mobilep12.pem).
7. Enter the password when prompted.
8. Click **OK**.

You should now see the following screen:

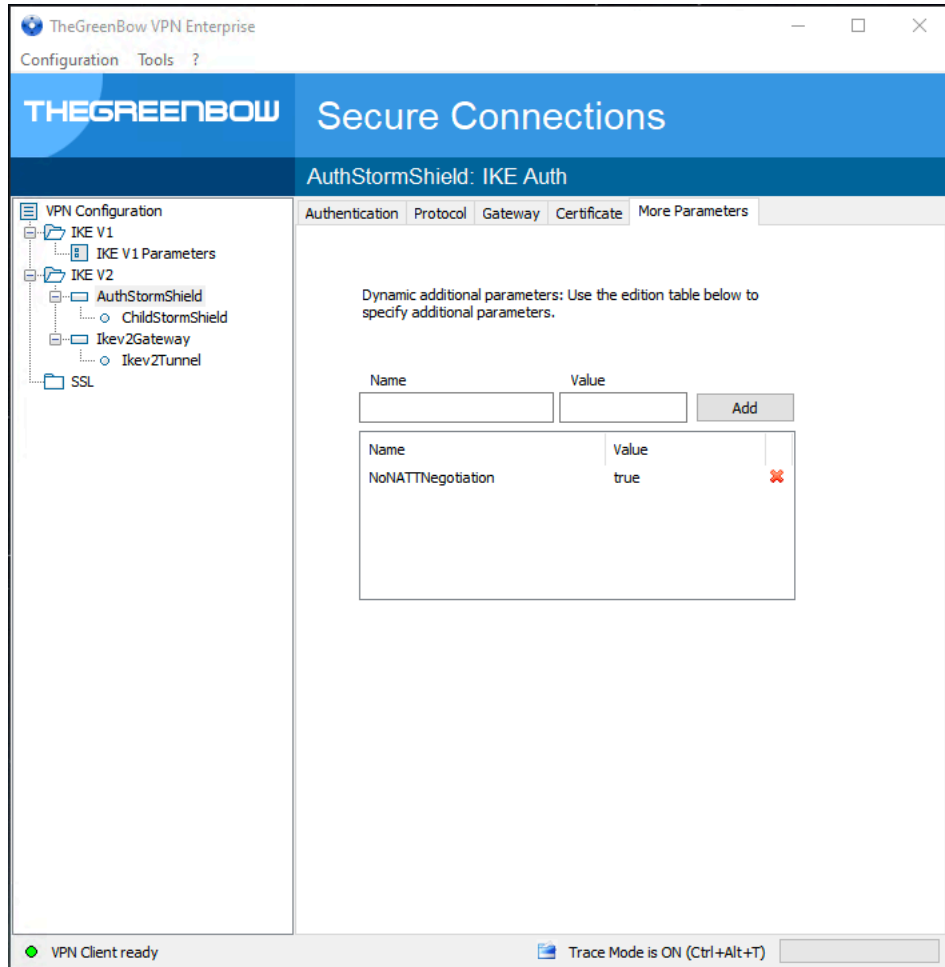


3.2.5 More Parameters tab

To show the **More Parameters** tab, from the **Tools** menu, choose **Options**, and then select the **General** tab and then check the **Show more parameters** box.



On the **More Parameters** tab, add a dynamic parameter named **NoNATTNegotiation** with its value set to `true`.



This parameter prevents the VPN client from negotiating NAT-T with the firewall, which is prohibited in DR mode.

3.3 Creating a new Child SA

To configure TheGreenBow Windows Enterprise VPN Client for a Child SA, proceed as shown in the following screenshot:

The screenshot shows the 'Secure Connections' configuration window for 'ChildStormShield: Child SA'. The window has tabs for 'Child SA', 'Advanced', 'Automation', 'Remote Sharing', 'More Parameters', 'IPV4', and 'IPV6'. The 'IPV4' tab is selected. The configuration is divided into three sections: 'Traffic selectors', 'Cryptography', and 'Lifetime'.
- **Traffic selectors:** 'VPN Client address' is 0.0.0.0, 'Address type' is 'Subnet address', 'Remote LAN address' is 0.0.0.0, and 'Subnet mask' is 0.0.0.0. The checkbox 'Request configuration from the gateway' is checked.
- **Cryptography:** 'Encryption' is 'AES GCM 256', 'Integrity' is 'Auto', 'Diffie-Hellman' is 'DH19 (ECP 256)', and 'Extended Sequence Number' is 'Auto'.
- **Lifetime:** 'Child SA Lifetime' is 1800 sec.

1. Check **Request configuration from the gateway**.
2. Under **Cryptography**, select the following values:
 - Encryption: AES GCM 256
 - Integrity: Auto
 - Diffie-Hellman: DH19 (ECP 256)
 - Extended Sequence Number: Auto
3. Under **Lifetime**, enter 1800 in the **Child SA Lifetime** field.



We recommend that you configure a lower lifetime value in the VPN Client than in the firewall, so that renegotiations are initiated by the VPN Client.

3.4 Saving the configuration

In TheGreenBow Windows Enterprise VPN Client, from the **Configuration** menu, select **Save** to account for all the changes you have made to your VPN configuration.



3.5 Opening the VPN connection

Once both the Stormshield firewall and TheGreenBow Windows Enterprise VPN Client have been configured as described above, you are ready to open VPN connections.

Double-click your Child SA tunnel name or click **Open** in the **Connection Panel** to open a tunnel.

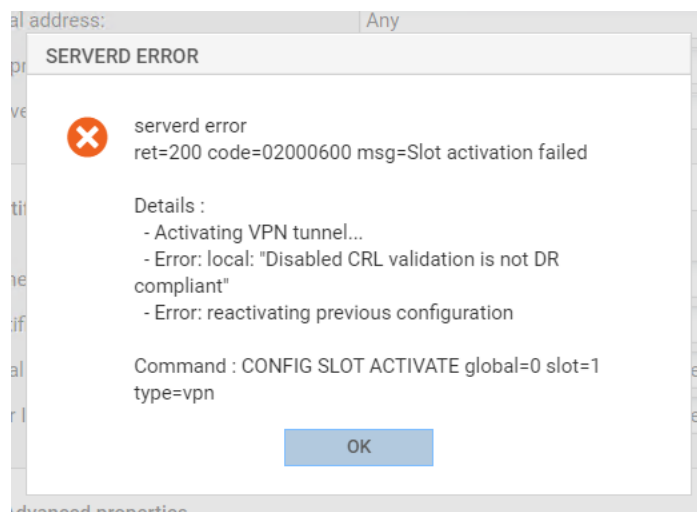
A green icon appears next to the Child SA when the connection is established successfully.

4 Troubleshooting

4.1 SNS firewall

4.1.1 Disabled CRL validation is not DR compliant

If you encounter the “Disabled CRL validation is not DR compliant” error on the SNS firewall, you must first determine the active VPN slot and then enable CRL validation.



4.1.1.1 Determining the active VPN slot

To determine the active VPN slot, proceed as follows:

1. Connect to the firewall via SSH.
2. Run the following command:

```
slotinfo
```

The command returns the active VPN slot. In this case, 02:

```
SNI40-MED-SNI40A38A1465E5>slotinfo
globalfilter: active=00 name="" sync=1
globalvpn: active=00 name="" sync=1
filter: active=05 name="Filter 05" sync=1
vpn: active=02 name="IPsec 02" sync=1
```



4.1.1.2 Enabling CRL validation

There are two ways to enable CRL validation:

- Method 1: using the `CONFIG IPSEC UPDATE` command
- Method 2: editing the firewall configuration file in a text editor

4.1.1.2.1 Method 1

To enable CRL validation using the `CONFIG IPSEC UPDATE` command, proceed as follows:

1. If you are no longer connected to the firewall, connect to the firewall via SSH.
2. Run the following commands successively:

```
CONFIG IPSEC UPDATE slot=02 CRLRequired=1  
CONFIG IPSEC ACTIVATE
```



Make sure to replace `02` with the result from the `slotinfo` command.

4.1.1.2.2 Method 2

To enable CRL validation by editing the firewall configuration file in a text editor, proceed as follows:

1. Use your favorite text editor (e.g. `vi` or `Joe`) to edit the firewall configuration file by running the following command:

```
Joe /Firewall/ConfigFiles/VPN/02
```



Make sure to replace `02` with the result from the `slotinfo` command.

2. In the text editor, set `CRLRequired` to 1.
3. Save the file (e.g. `Ctrl+Alt+K` in `Joe`).
4. Run the following command to disable and then re-enable the VPN configuration:

```
envpn 00 && envpn 02
```



Make sure to replace `02` with the result from the `slotinfo` command.

CRL validation is now enabled. You should no longer get the “Disabled CRL validation is not DR compliant” error.

4.1.1.3 Checking whether CRL validation is enabled

If you simply want to check whether CRL validation is enabled, once you have determined the active VPN slot as described in section 4.1.1.1 Determining the active VPN slot above, proceed as follows:

1. If you are no longer connected to the firewall, connect to the firewall via SSH.
2. Run the following command :

```
cat /Firewall/ConfigFiles/VPN/02 | grep CRL
```



Make sure to replace 02 with the result from the `slotinfo` command.

```
SNI40-MED-SNI40A38A1465E5>cat /Firewall/ConfigFiles/VPN/02 | grep CRL
CRLRequired=0 # Set to 1 to block the tunnel negotiation when the CRL is missing.
```

If `CRLRequired` is equal to 0, CRL validation is disabled. You must enable CRL validation to use the firewall in DR mode. To do so, refer to section 4.1.1.2 Enabling CRL validation above.

4.2 VPN Client

If the VPN connection cannot be established, check the Console log in TheGreenBow VPN Client to see whether some of the messages displayed match one of the messages described in the following sections.

4.2.1 NO_PROPOSAL_CHOSEN

If you encounter a `NO_PROPOSAL_CHOSEN` error, you might have wrongly configured the Phase 1 [IKE Auth]. Make sure the encryption algorithms are the same at both ends of the VPN connection.

```
20XX0913 16:08:53:387 TIKEV2_Tunnel SEND IKE_SA_INIT
[HDR] [SA] [NONCE] [N(NAT_DETECTION_SOURCE_IP)] [N(NAT_DETECTION_DESTINATION_IP)]
[KE] [VID] [N(FRAGMENTATION_SUPPORTED)]
20XX0913 16:08:53:419 TIKEV2_Tunnel RECV IKE_SA_INIT
[HDR] [N(NO_PROPOSAL_CHOSEN)]
```

4.2.2 AUTHENTICATION_FAILED

If you encounter an `AUTHENTICATION_FAILED` error, this means that the certificate sent by the VPN Client does not match what the firewall is

expecting. Make sure the VPN Client's user certificate is correctly configured on the firewall.

```
20XX0913 16:15:22:032 TIKEV2_Tunnel RECV IKE_AUTH
[HDR] [N(AUTHENTICATION_FAILED)]
20XX0913 16:15:22:032 TIKEV2_Tunnel Remote endpoint sends error
AUTHENTICATION_FAILED
```

4.2.3 No user certificate available for the connection

Make sure the user certificate has been correctly imported to the VPN Client.

```
20XX0913 16:18:07:491 TIKEV2_Tunnel RECV IKE_SA_INIT
[HDR] [SA] [KE] [NONCE] [N(NAT_DETECTION_SOURCE_IP)] [N(NAT_DETECTION_DESTINATION_IP)] [CERTREQ] [N(FRAGMENTATION_SUPPORTED)] [N(MULTIPLE_AUTH_SUPPORTED)]
20XX0913 16:18:07:491 TIKEV2_Tunnel IKE SA I-SPI 8D4467C52C91C316 R-SPI
9DF0F0E4A91F8867
20XX0913 16:18:07:491 TIKEV2_Tunnel No user certificate available for the
connexion
20XX0913 16:18:07:491 TIKEV2_Tunnel Connection aborted.
```

4.2.4 Remote IDr rejected

The Remote ID type or value sent by the firewall does not match what the VPN Client is expecting (see **Protocol** tab). Configure the Remote ID type and value in the VPN Client according to the firewall's Local ID.

```
20180913 16:24:32:087 TIKEV2_Tunnel ID types do not match. Expecting
ID_RFC822_ADDR. Receiving ID_DER_ASN1_DN
20180913 16:24:32:087 TIKEV2_Tunnel Remote IDr rejected
```

4.2.5 FAILED_CP_REQUIRED

If you encounter a FAILED_CP_REQUIRED error, it means that the firewall is configured to use CP (Configuration Payload) mode, but not the VPN Client. In TheGreenBow Windows Enterprise VPN Client, go to **Traffic selectors** and enable **Request configuration from the gateway**.

```
20XX0913 16:29:46:780 TIKEV2_Tunnel RECV IKE_AUTH
[HDR] [IDr] [CERT] [AUTH] [N(AUTH_LIFETIME)] [N(FAILED_CP_REQUIRED)] [N(TS_UNACCEPTABLE)]
20180913 16:29:46:780 TIKEV2_Tunnel Remote endpoint sends error
FAILED_CP_REQUIRED
20XX0913 16:29:46:780 TIKEV2_Tunnel Remote endpoint is expecting a
configuration request from the client
```

5 Contact

5.1 Information

All the information on TheGreenBow products is available on our website: <https://thegreenbow.com/>.

5.2 Sales

Phone: +33.1.43.12.39.30

E-mail: sales@thegreenbow.com

5.3 Support

There are several pages related to the software's technical support on our website:

Online help

<https://www.thegreenbow.com/en/support/online-support/>

FAQ

<https://www.thegreenbow.com/en/frequently-asked-questions/>

Contact form

Technical support can be reached using the form on our website at the following address: <https://www.thegreenbow.com/en/support/online-support/technical-support/>.

Protect your connections
in any situation

14, rue Auber
75009 Paris - France
sales@thegreenbow.com

www.thegreenbow.com