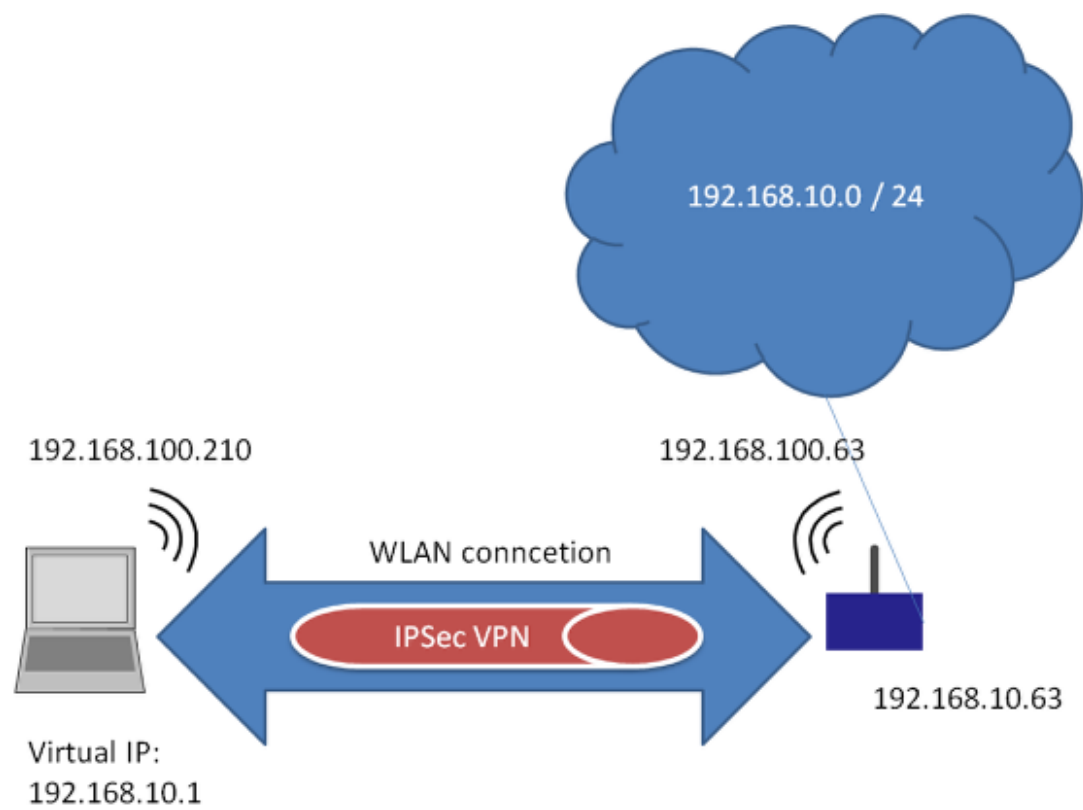


Howto configure a VPN between an OpenBAT and freeware Shrewsoft VPN Client (IPSec)

- 2018-02-21 - BAT, WLC (HiLCOS)

This lesson describes how to use a VPN between a OpenBAT and a WIN7 Shrewsoft Client over a WLAN connection

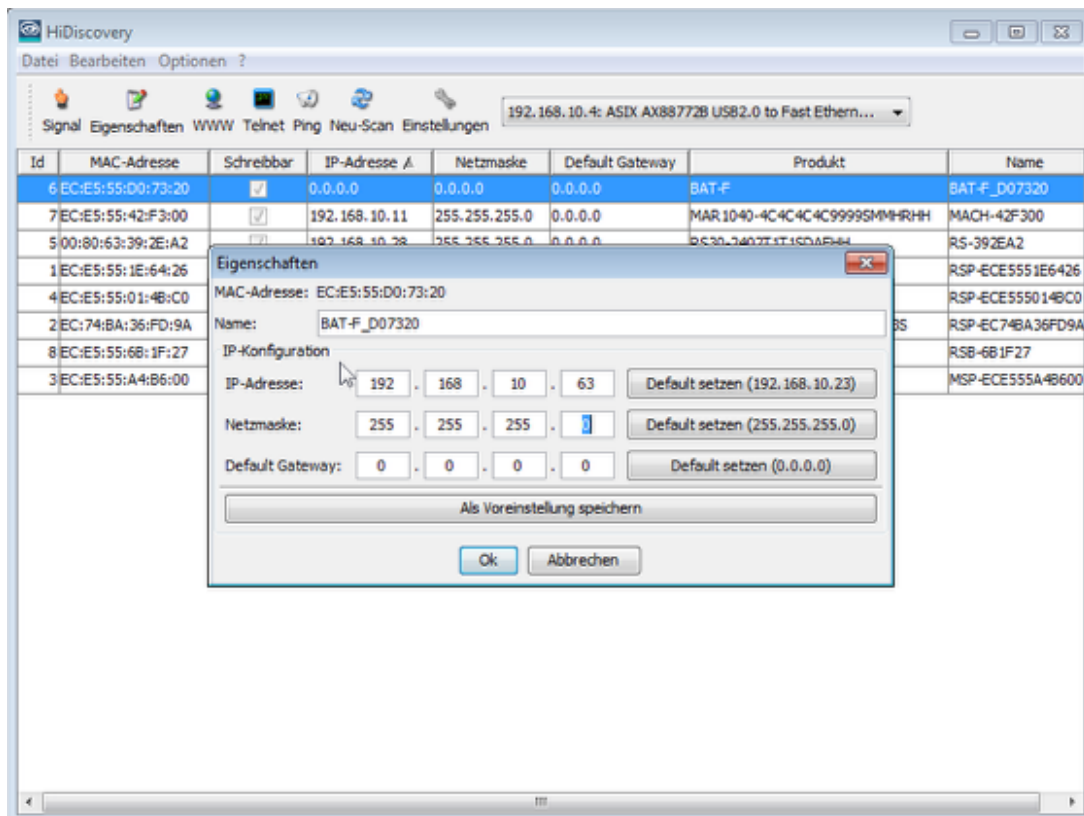
Network Topology



This is the network which will be configured in this Howto.

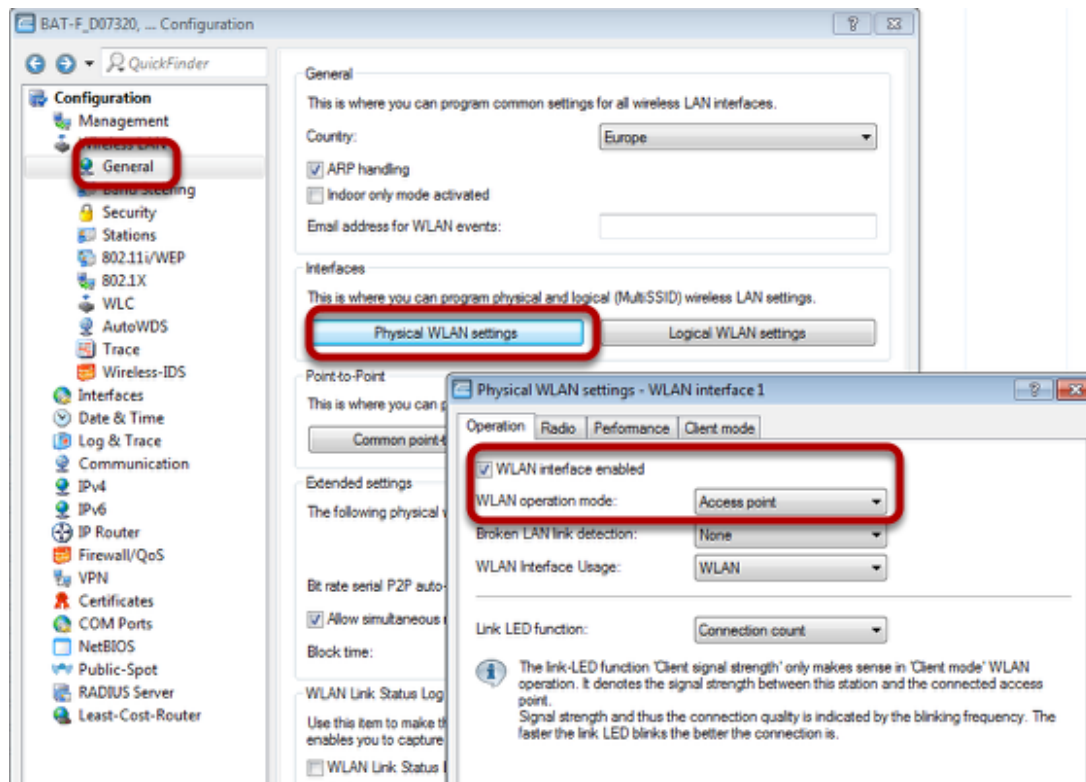
This configuration and this topology is an example only. It can be modified according to customers needs.

Assign IP-address



Use HiDiscovery to assign a IP-address to the BAT. The PC is locally connected.

Configure physical WLAN settings



Use Access-Point as WLAN operation mode. Optionally you can choose alternative Radio settings etc.

Configure Logical WLAN settings

IS

Physical WLAN settings Logical WLAN settings

Logical WLAN settings - WLAN interface 1 - Network 1

Network Transmission Alarms

Interface: WLAN interface 1 - Network 1

☒ WLAN network enabled

Network name (SSID):

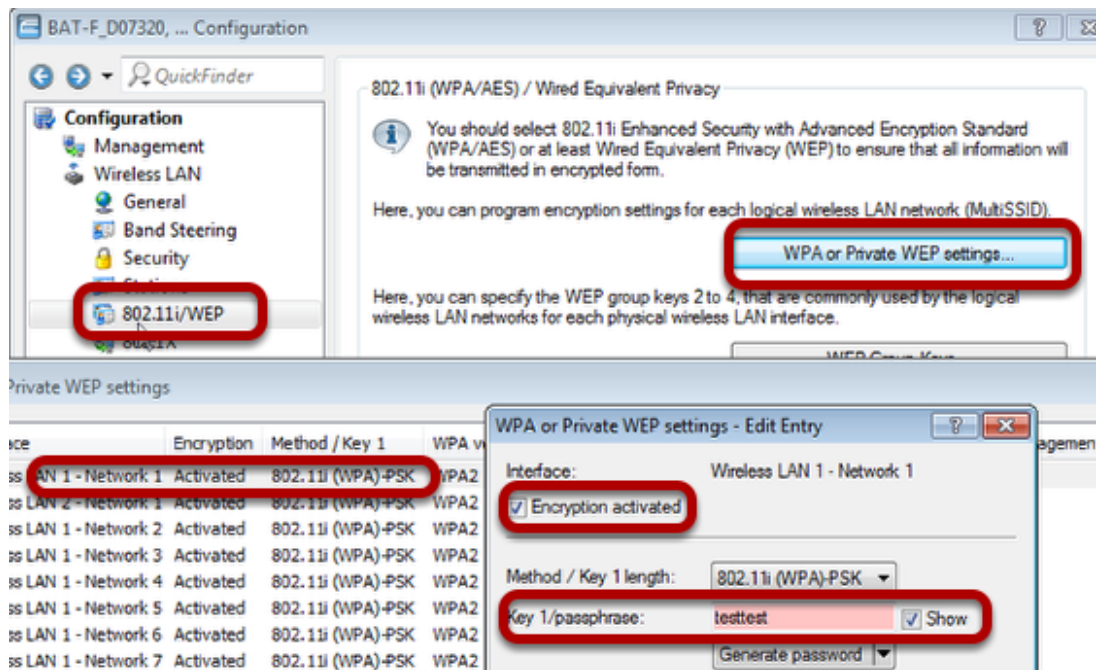
Suppress SSID broadcast:

☒ MAC filter enabled

Maximum count of clients:

Configure the SSID

Configure WPA PSK



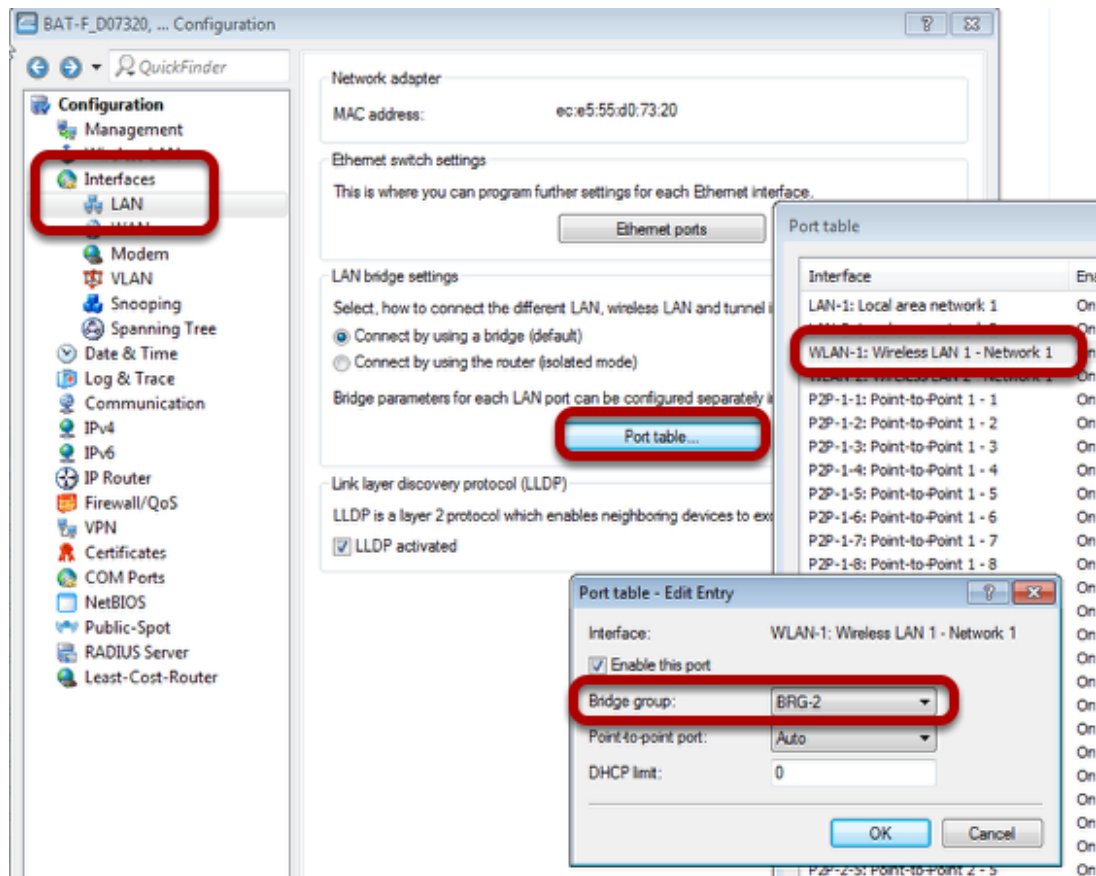
Proceed to menu "Wireless LAN - 802.11i/WEP"

Use button "WPA or Private WEP settings...". A new window will open

Doubleclick on first line

Make sure that "encryption activated" is checked and enter a passphrase

Use Routing: Define separate bridge group for WLAN



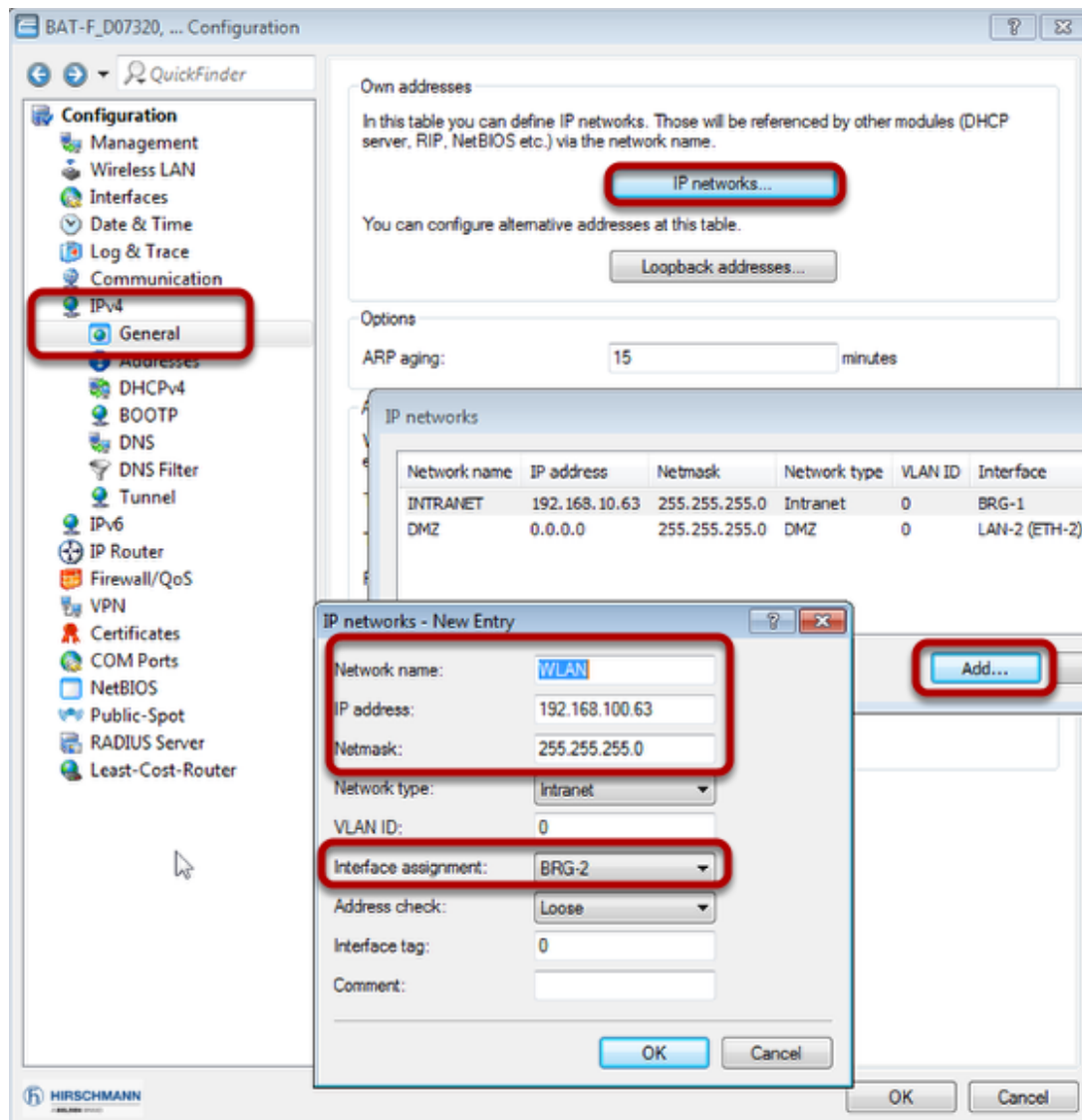
Proceed to menu "Interfaces - LAN"

Use button "Port table...". A new window will open.

Doubleclick on line "WLAN-1:..." A new window will open.

Choose "BRG-2" as Bridge group

Assign IP-address to BRG-2



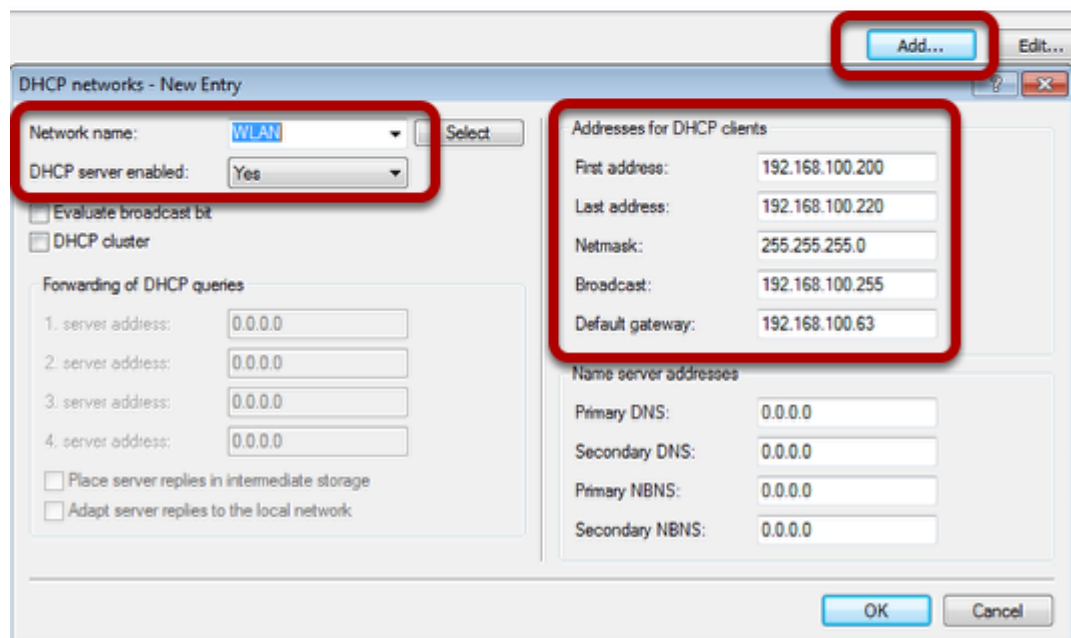
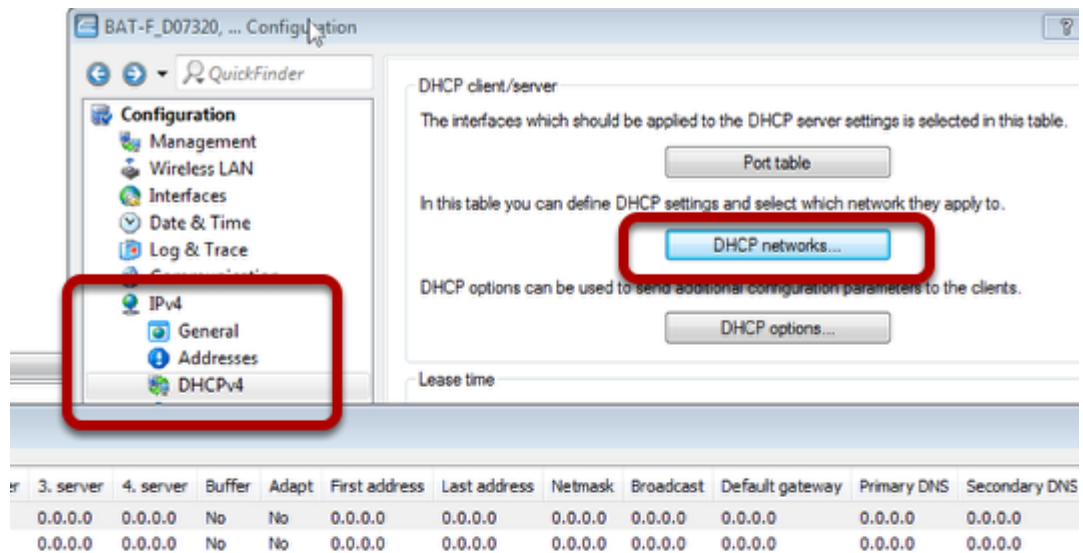
Proceed to menu "IPv4 - General"

Use button "IP networks...". A new window will open.

Use button "Add...". A new window will open.

Define IP parameters and make sure that BRG-2 is used.

Define DHCP for WLAN



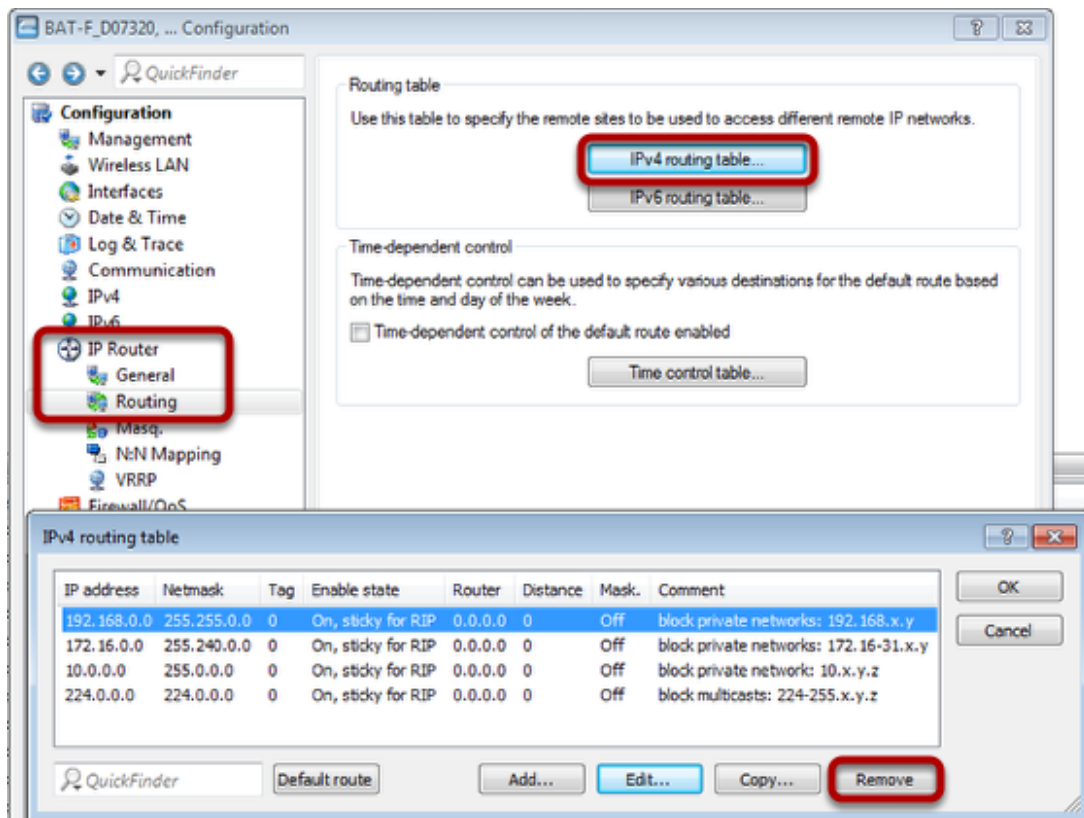
Proceed to menu "IPv4 - DHCPv4"

Use "DHCP networks...". A new window will open.

Use button "Add...". A new window will open.

Fill in relevant parameters.

Delete unused routes



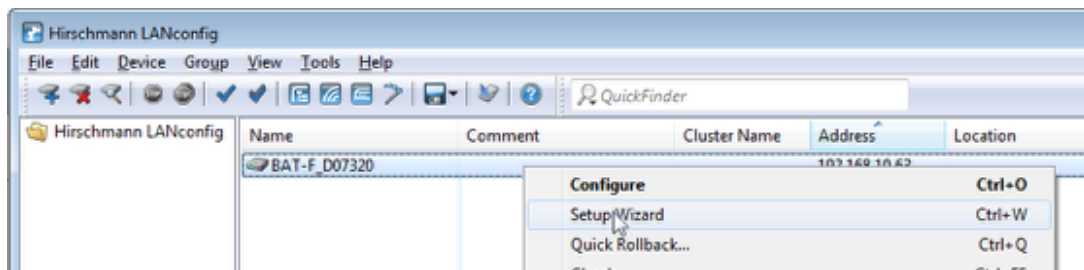
Proceed to menu "IP Router - Routing"

Use button "IPv4 routing table". A new window will open.

Delete all entries by clicking button "Remove" several times.

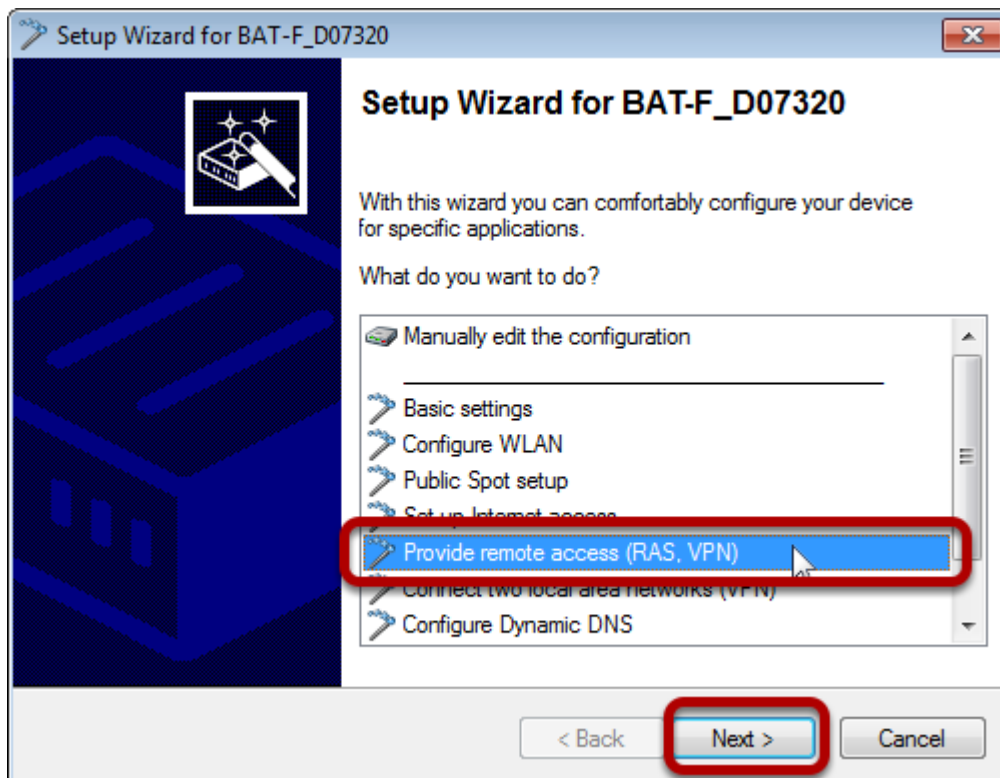
Now send the configuration to the OpenBAT by clicking "OK" in all dialogs.

OPEN Wizard

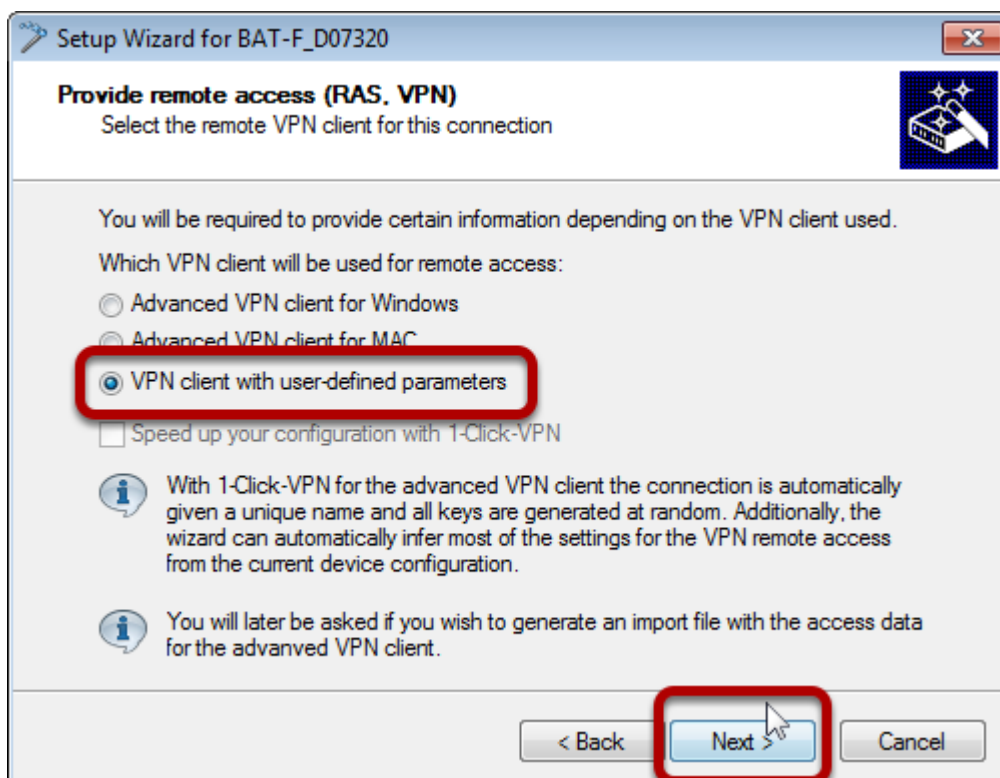


In LANconfig right-click on the device and choose SetupWizard

Use Wizard for VPN / Remote access



Choose relevant wizard and press "Next"



Choose "VPN client with user-defined parameters" and click "Next"

Setup Wizard for BAT-F_D07320

Provide remote access (RAS, VPN)
Settings for this connection's remote station

First, enter a name for this access:

VPN Name:

< Back **Next >** Cancel

Choose VPN Name and click "Next"

Setup Wizard for BAT-F_D07320

Provide remote access (RAS, VPN)
VPN Authentication and Exchange Mode Selection

Two kinds of VPN connection authentication are supported.
Select the used VPN connection authentication as well as the exchange mode:

☒ Preshared Key and Aggressive Mode
☐ Certificates (RSA Signature) and Main Mode

Preshared Key: ☒ Show

Generate password Quality

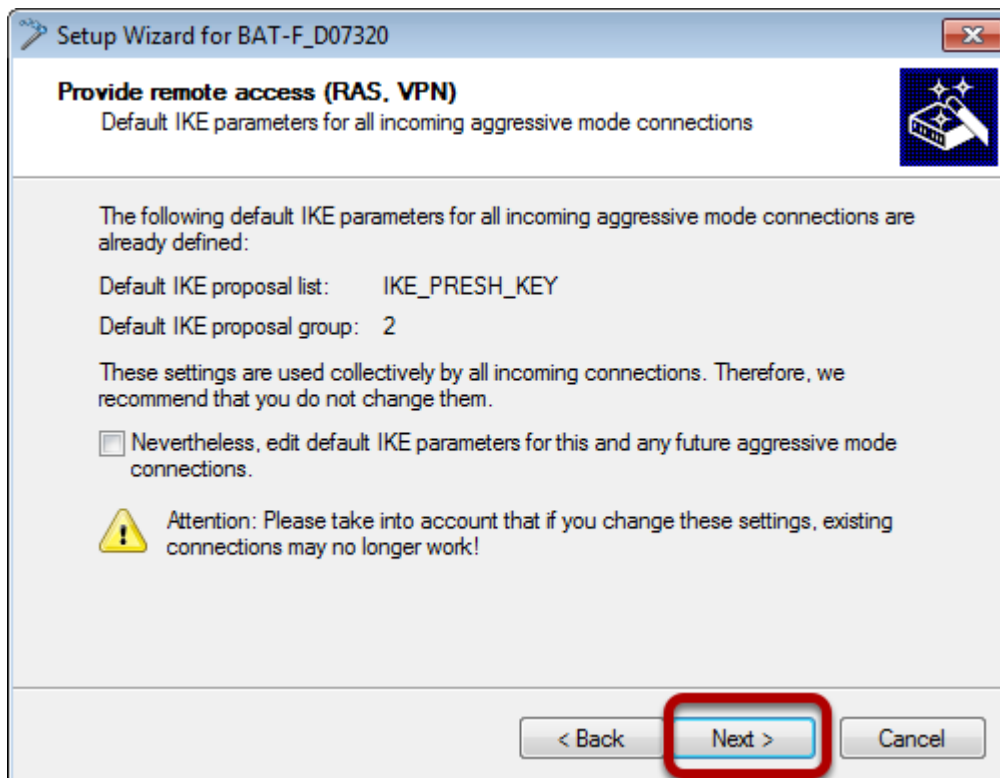
Information:
Please take into account that for RSA Signatures, digital certificates according to the X.509 standard are necessary for both this device and for the remote client. The device certificate must be uploaded via HTTP(S) before establishing the VPN connection. In addition, when using certificates, it is necessary for the device to have a valid system time.

< Back **Next >** Cancel

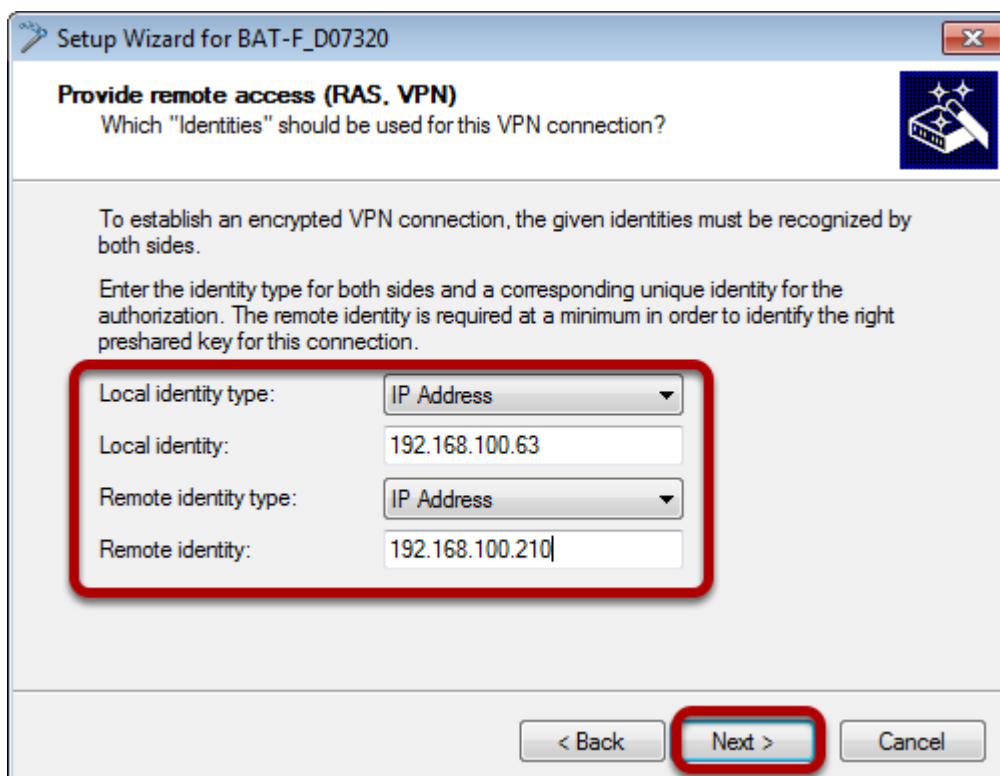
Choose "Preshared Key and Aggressive Mode"

Choose a Preshared Key

Click "Next"

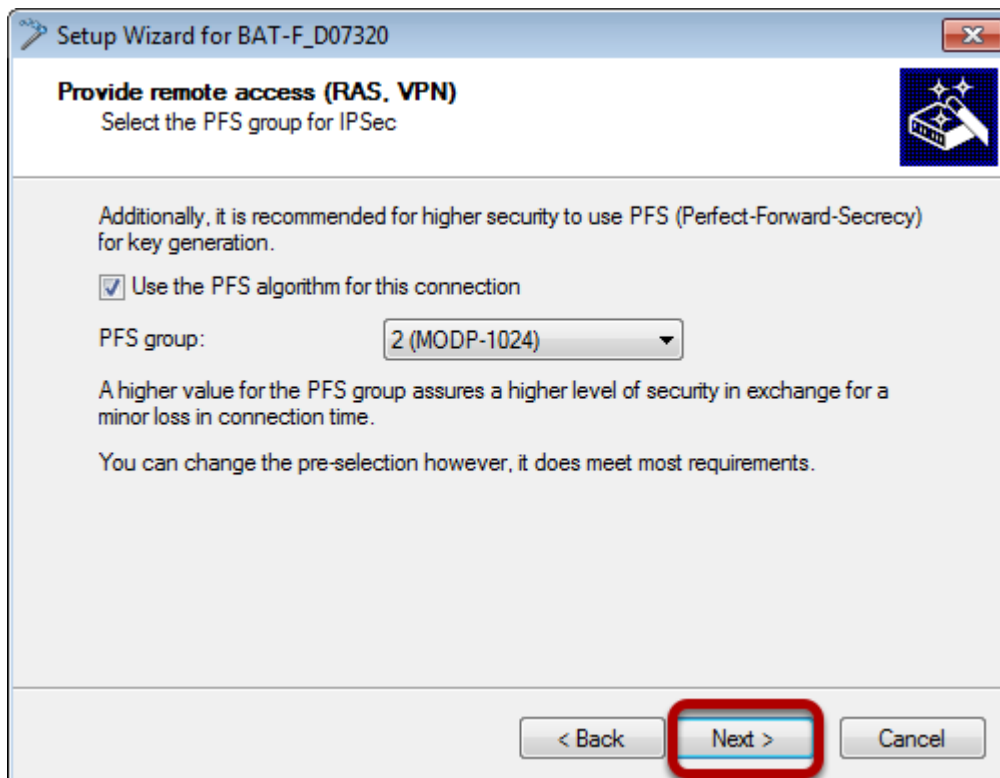


Use default settings and click "Next"

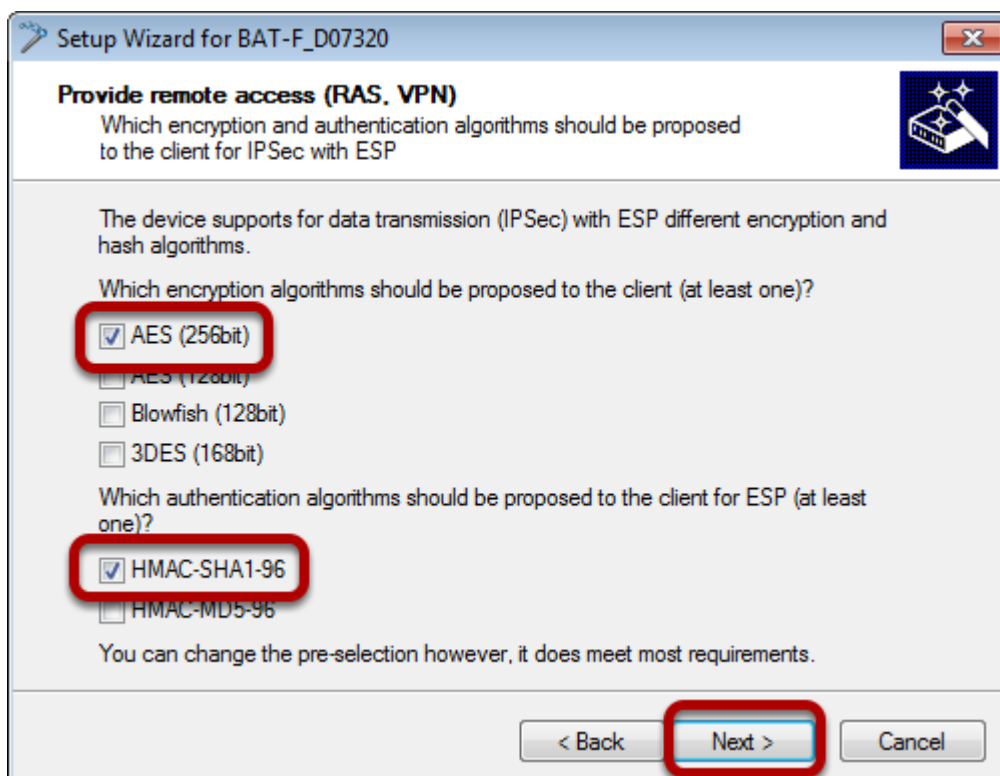


Choose "IP Address" as identifier (local and remote).

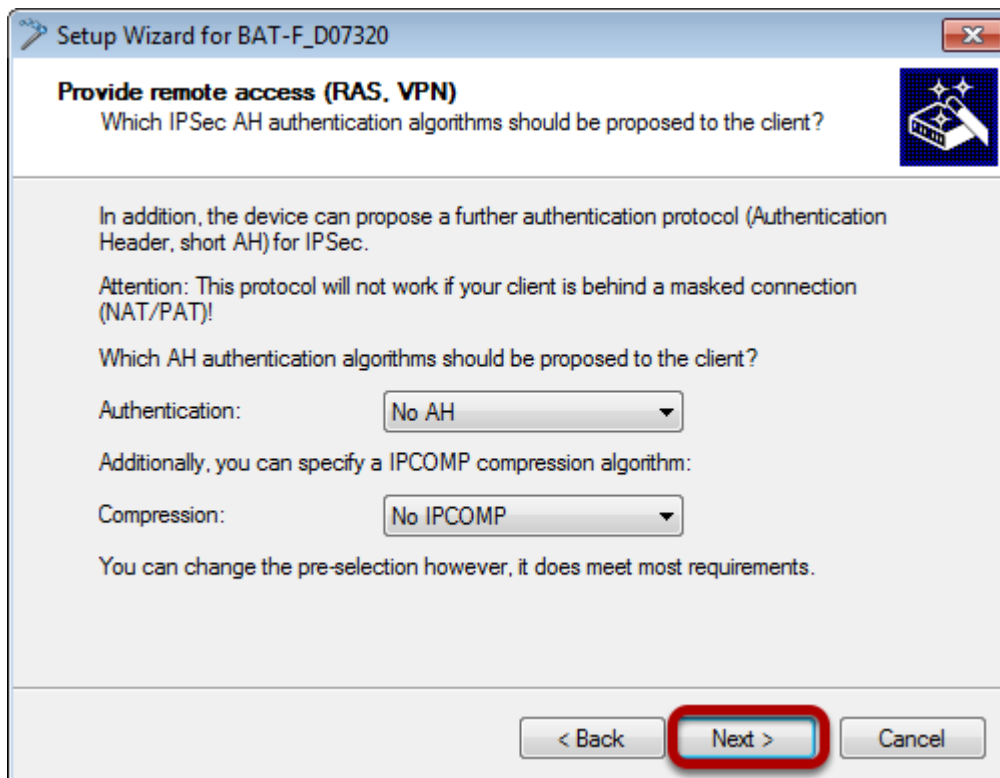
Enter IP-addresses. The remote IP address must be known. Probably you have to connect to the WLAN with your client first.



Use default settings and press "Next"



Choose "AES 8256bit)" and "HMAC-SHA1-96" and press "Next"



Setup Wizard for BAT-F_D07320

Provide remote access (RAS, VPN)
Which IPSec AH authentication algorithms should be proposed to the client?

In addition, the device can propose a further authentication protocol (Authentication Header, short AH) for IPSec.

Attention: This protocol will not work if your client is behind a masked connection (NAT/PAT)!

Which AH authentication algorithms should be proposed to the client?

Authentication:

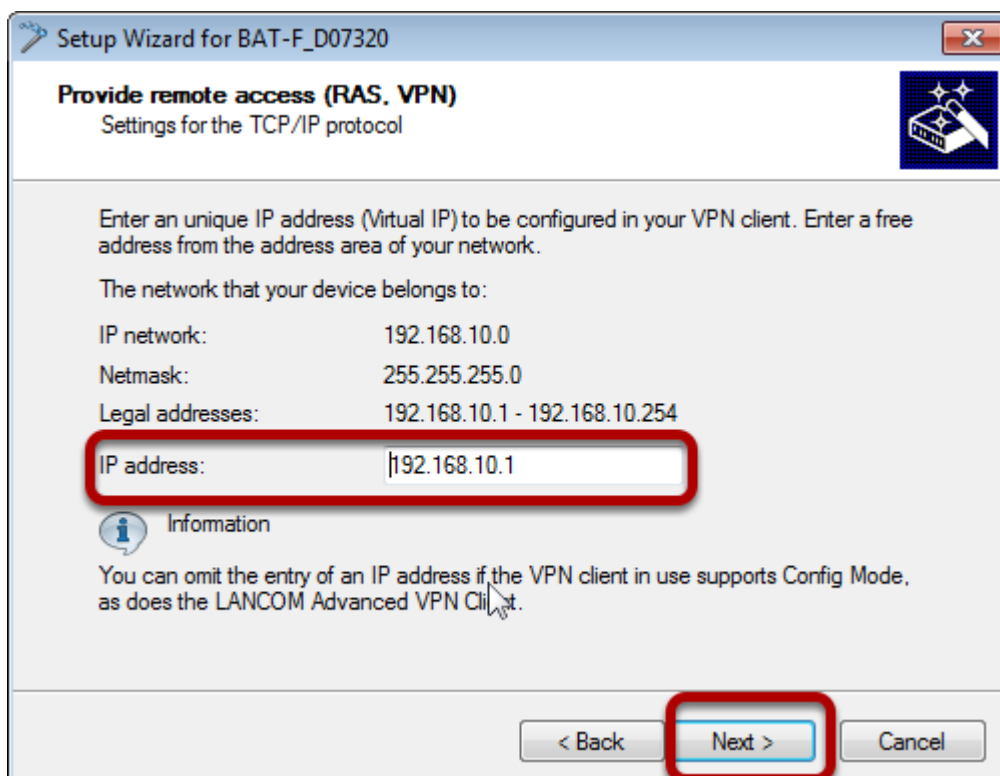
Additionally, you can specify a IPCOMP compression algorithm:

Compression:

You can change the pre-selection however, it does meet most requirements.

< Back **Next >** Cancel

Use default settings and press "Next"



Setup Wizard for BAT-F_D07320


Provide remote access (RAS, VPN)
Settings for the TCP/IP protocol

Enter an unique IP address (Virtual IP) to be configured in your VPN client. Enter a free address from the address area of your network.

The network that your device belongs to:

IP network:	192.168.10.0
Netmask:	255.255.255.0
Legal addresses:	192.168.10.1 - 192.168.10.254

IP address:

 **Information**

You can omit the entry of an IP address if the VPN client in use supports Config Mode, as does the LANCOM Advanced VPN Client.

< Back **Next >** Cancel

Choose a virtual IP address for the remote client in the local network. This will use proxy ARP automatically.

Press "Next"

Setup Wizard for BAT-F_D07320

Provide remote access (RAS, VPN)
Settings for the TCP/IP protocol

You may either allow all IP addresses to be reached by the VPN client (default) or you may limit the access to a specific IP network.

Which IP addresses should be reachable for the VPN client:

- ☒ Allow all IP addresses to be reachable for the VPN client
- ☐ The following IP network should be reachable for the VPN client:

IP network:

Netmask:

Please remember to configure this IP network on VPN client as well. If you neglect to configure the same network there, a VPN connection will not be able to be established.

Further networks and network relations or transmission properties can be configured in the corresponding new rule created on the firewall.

< Back **Next >** Cancel

Use default settings and press "Next"

Setup Wizard for BAT-F_D07320

Provide remote access (RAS, VPN)
Settings for the TCP/IP protocol

The NetBIOS protocol is used in some local networks to grant the individual stations mutual access to file and printer resources (For example, Microsoft Windows networks).

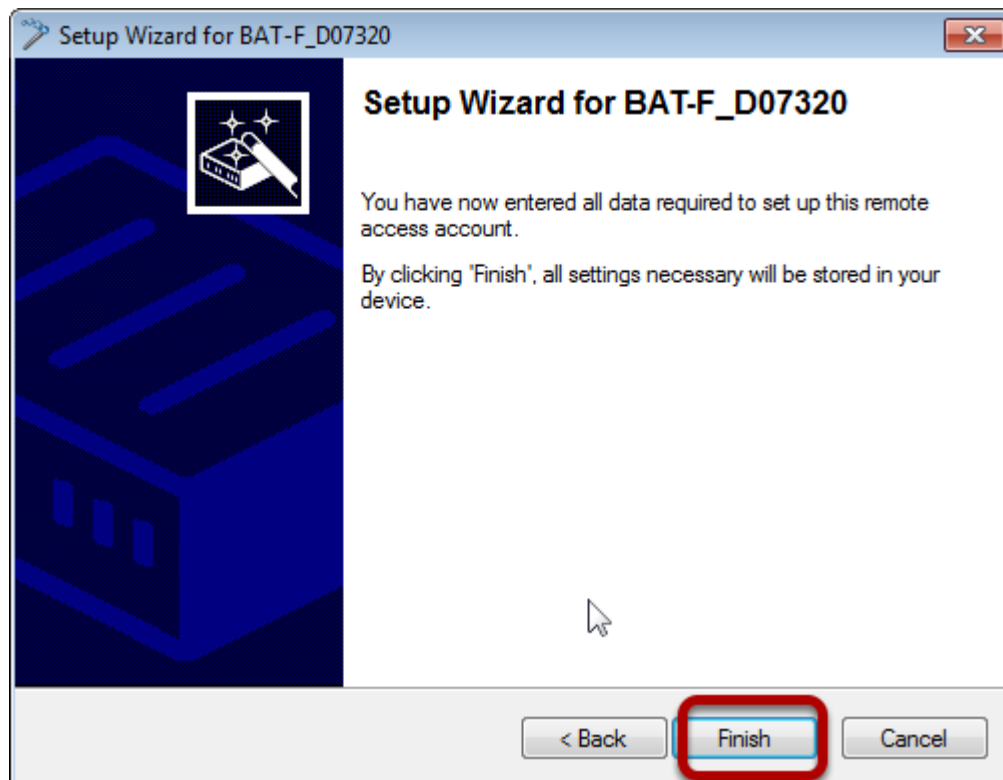
You can also grant dial-in access to user access to networks of this type.

☐ Activate NetBIOS over IP routing

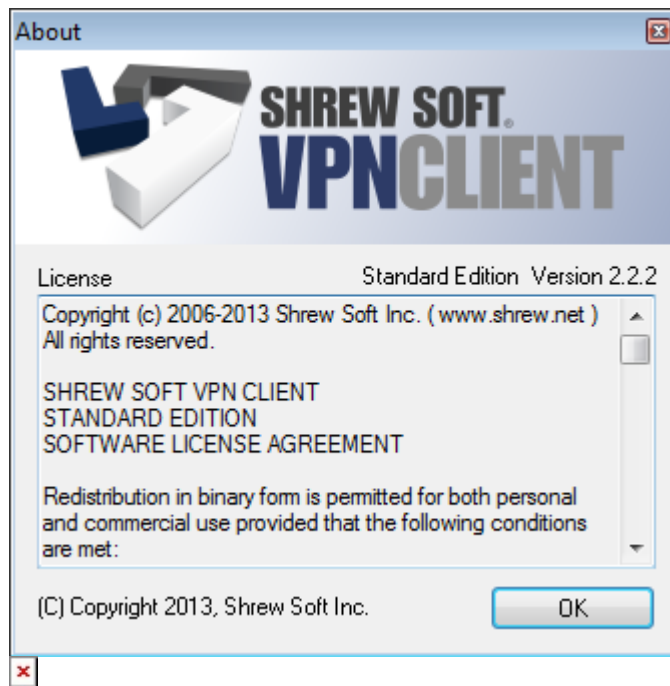
< Back **Next >** Cancel

Disable NetBIOS over IP routing

Press "Next"

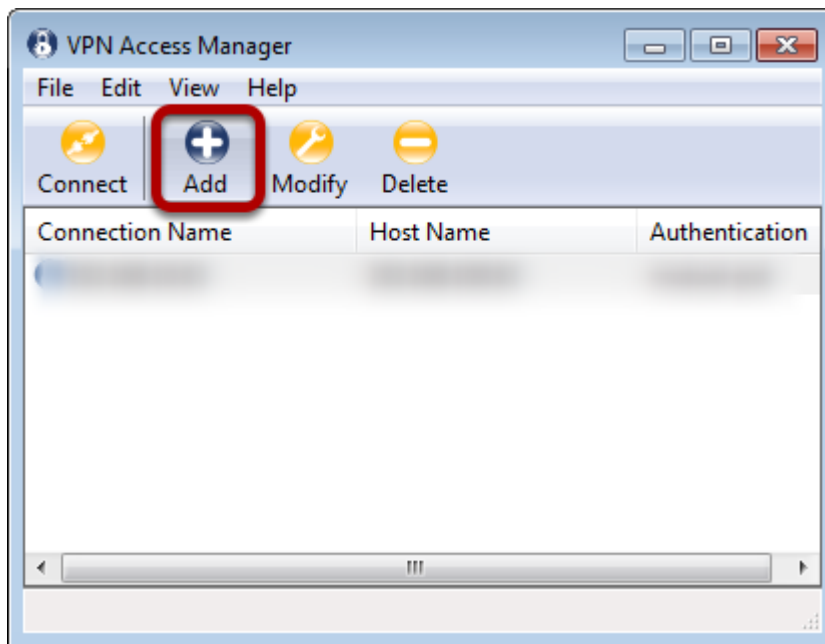


On Client side Shrewsoft VPN Clinet is used (freeware)

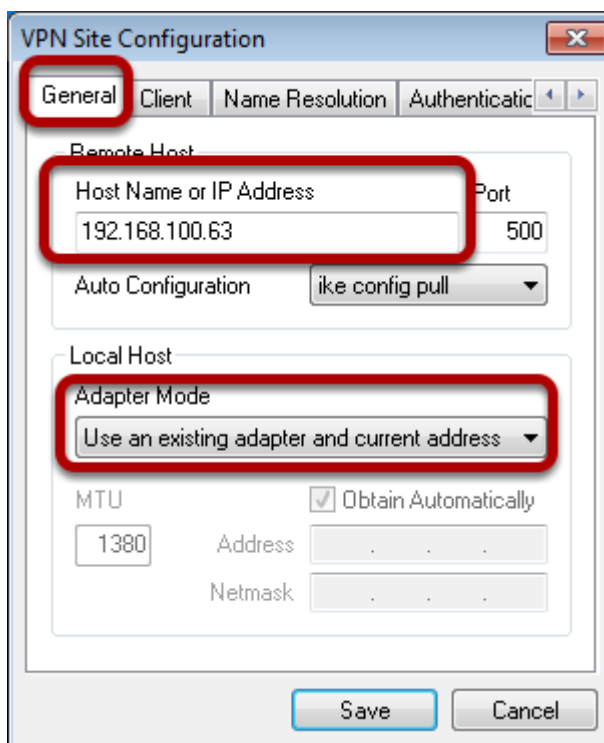


Install Shrewsoft VPN Client and start "VPN Access Manager"

Define new VPN

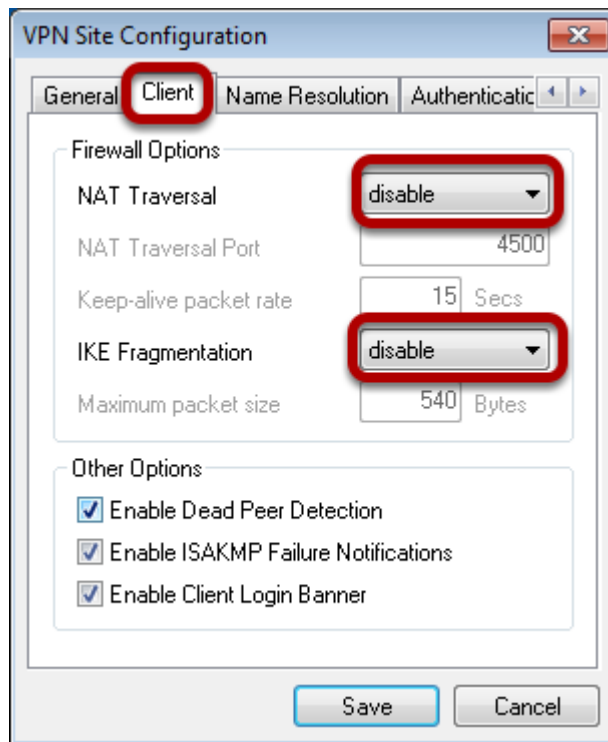


Click "Add". A new window will open.

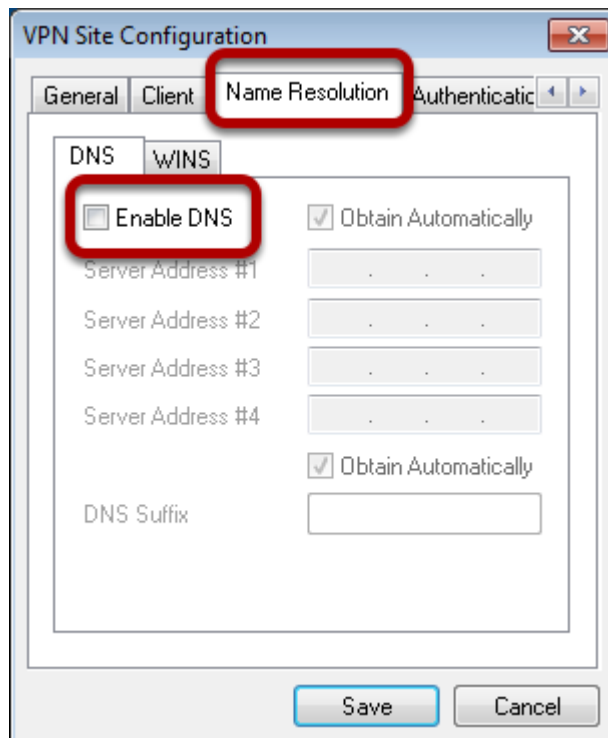


Enter the IP-address of the VPN Gateway (OpenBAT)

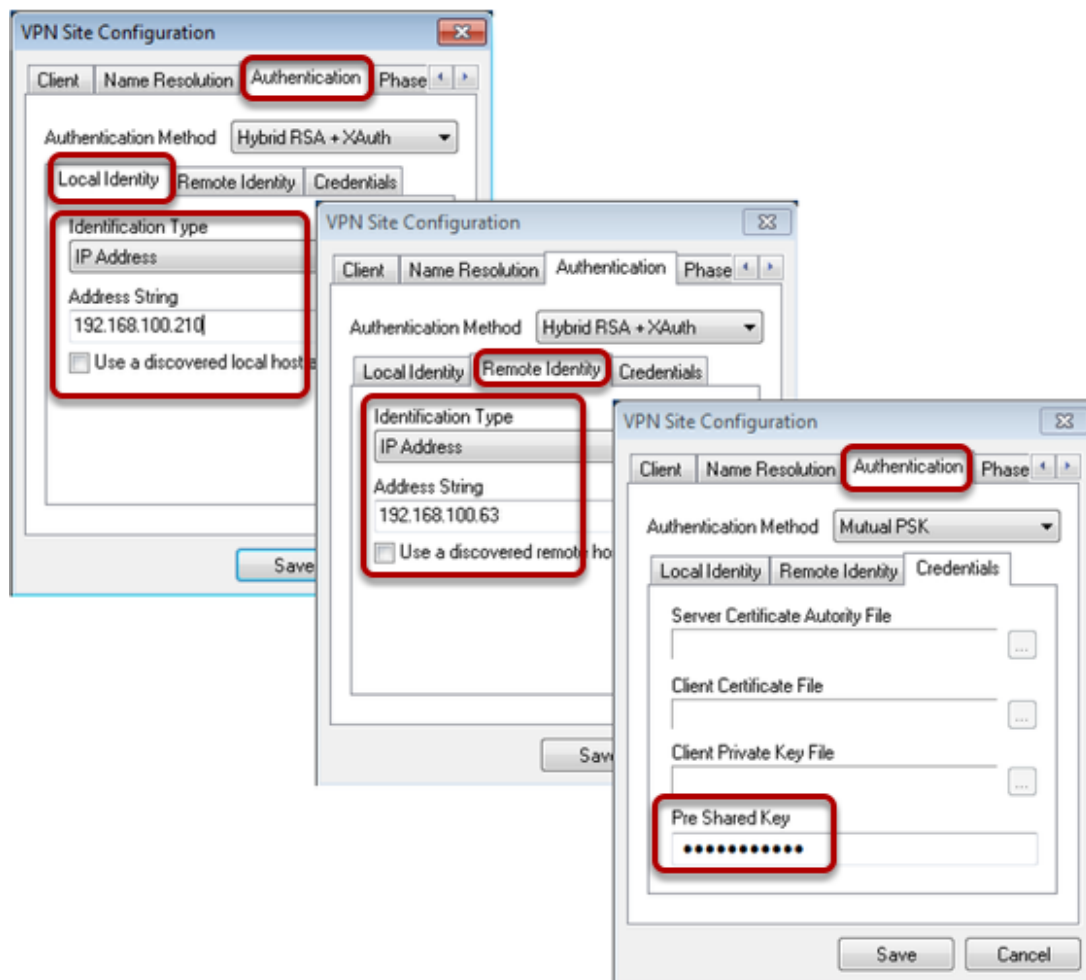
Choose "Use existing adapter and current address" as "Adapter Mode"



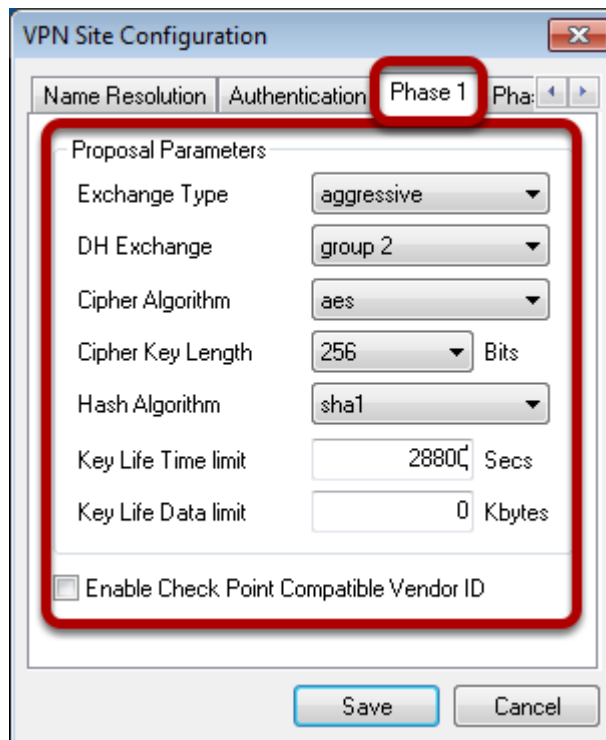
In "Client" tab disable nat-T and Fragmentation.



Disable DNS



For authentication use "IP-Address" as identifier and enter the addresses .
In the "Credentials" tab enter the "Pre Shared Key" (vpnpassword)

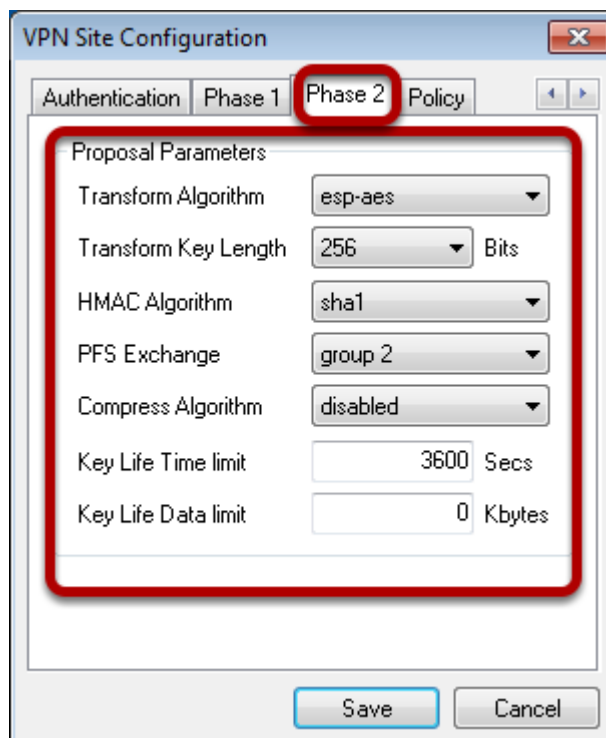


The image shows the 'VPN Site Configuration' dialog box with the 'Phase 1' tab selected. A red rectangle highlights the 'Proposal Parameters' section. The parameters are as follows:

Parameter	Value
Exchange Type	aggressive
DH Exchange	group 2
Cipher Algorithm	aes
Cipher Key Length	256 Bits
Hash Algorithm	sha1
Key Life Time limit	28800 Secs
Key Life Data limit	0 Kbytes

Below the parameters is an unchecked checkbox labeled 'Enable Check Point Compatible Vendor ID'. At the bottom are 'Save' and 'Cancel' buttons.

For phase1 use relevant parameters

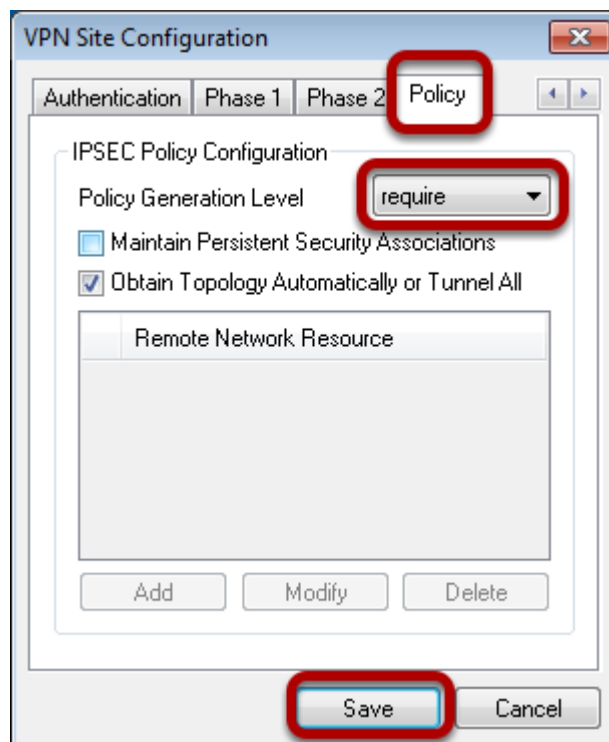


The image shows the 'VPN Site Configuration' dialog box with the 'Phase 2' tab selected. A red rectangle highlights the 'Proposal Parameters' section. The parameters are as follows:

Parameter	Value
Transform Algorithm	esp-aes
Transform Key Length	256 Bits
HMAC Algorithm	sha1
PFS Exchange	group 2
Compress Algorithm	disabled
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes

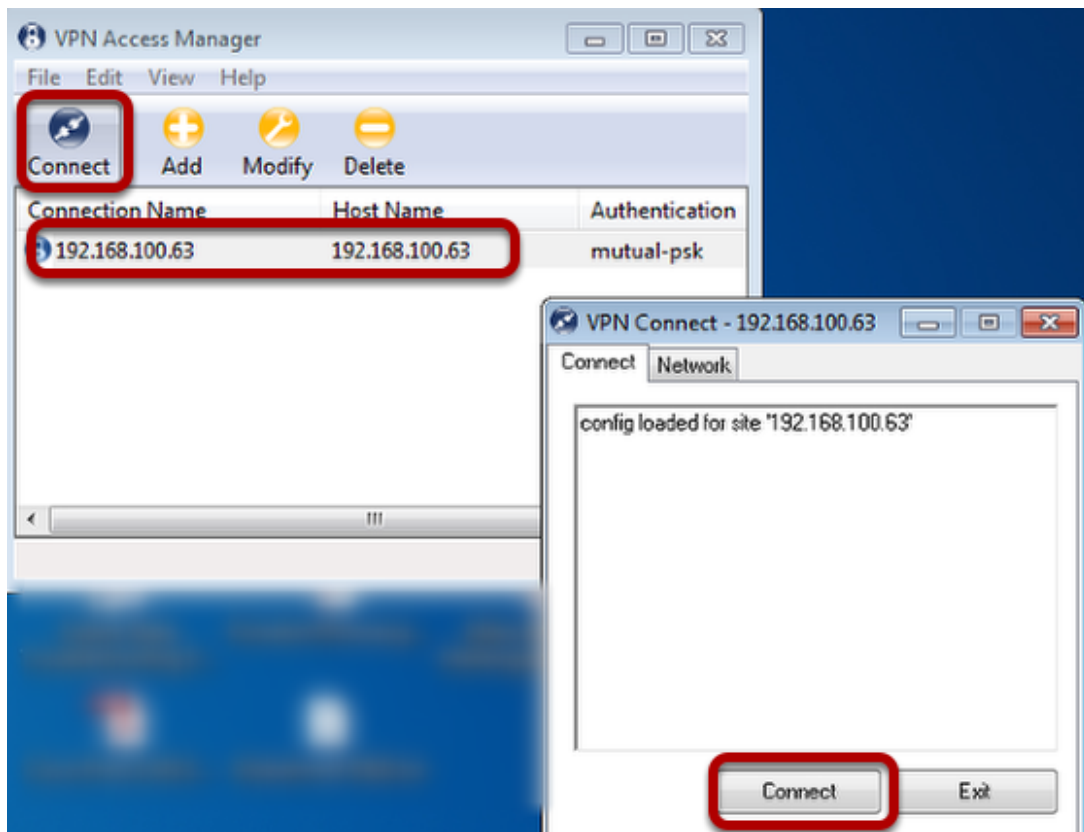
At the bottom are 'Save' and 'Cancel' buttons.

For phase2 use relevant parameters



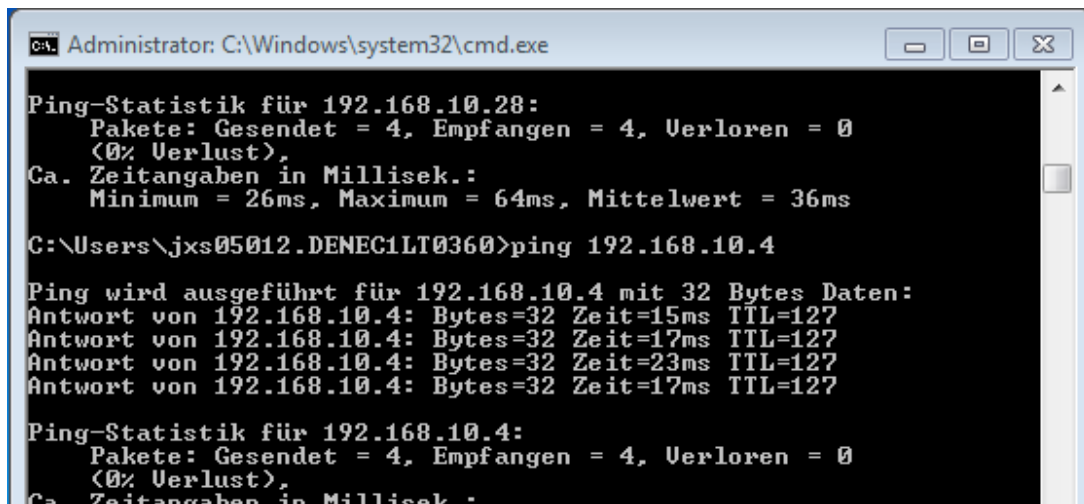
In "Policy" tab user "require" as "Policy Generation Level"
Press button "Save"

Start VPN



Mark the new created Vpn and press "Connect". A new window will open.
Press "Connect".

Test VPN



```
Administrator: C:\Windows\system32\cmd.exe

Ping-Statistik für 192.168.10.28:
  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
  Ca. Zeitangaben in Millisek.:
    Minimum = 26ms, Maximum = 64ms, Mittelwert = 36ms

C:\Users\jxs05012.DENEC1LT0360>ping 192.168.10.4

Ping wird ausgeführt für 192.168.10.4 mit 32 Bytes Daten:
Antwort von 192.168.10.4: Bytes=32 Zeit=15ms TTL=127
Antwort von 192.168.10.4: Bytes=32 Zeit=17ms TTL=127
Antwort von 192.168.10.4: Bytes=32 Zeit=23ms TTL=127
Antwort von 192.168.10.4: Bytes=32 Zeit=17ms TTL=127

Ping-Statistik für 192.168.10.4:
  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
  Ca. Zeitangaben in Millisek.:
```

Open a DOS window and ping an IP-address of the remote network.