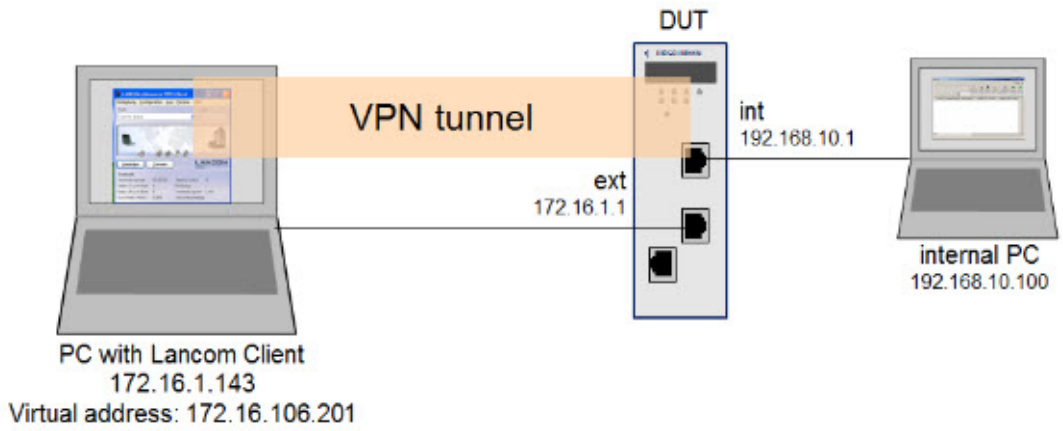
How to set up a VPN connection between EAGLE20 and the LANCOM Advanced VPN Client (NCP client) ?

- 2024-03-08 - Classic Firewalls

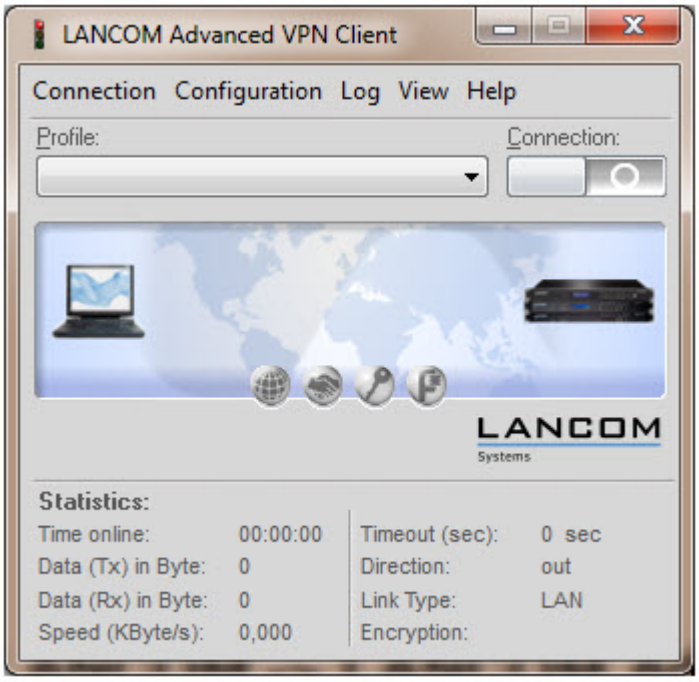
This lesson describes how to configure a VPN using Hirschmann EAGLE20 and the LANCOM Advanced VPN Client.

Used software versions:
EAGLE20 firmware v5.2.00
Lancom Advanced VPN Client v2.30 Build 146

Network Plan



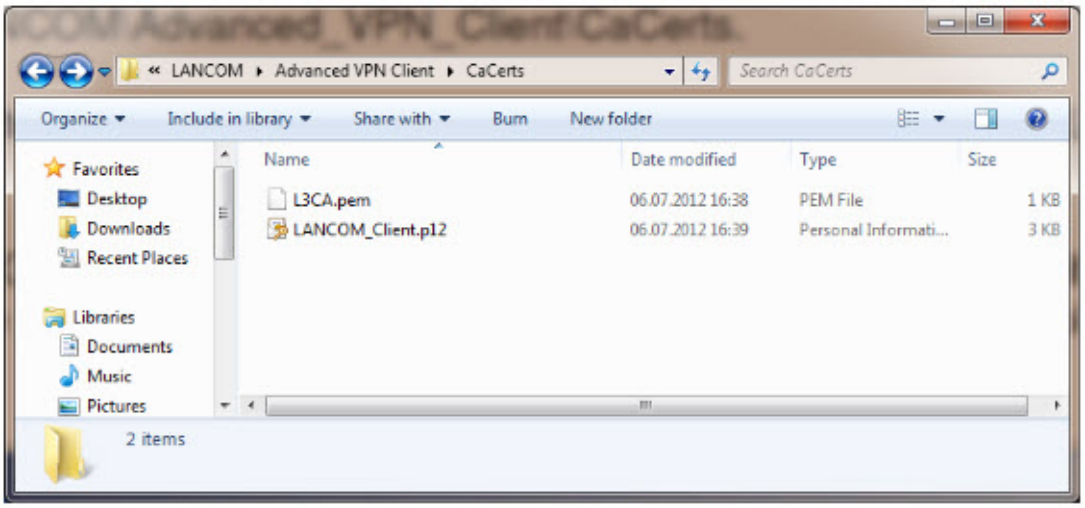
Install and start LANCOM Advanced VPN Client



The LANCOM Client with a 30 day evaluation period can be downloaded from http://www.lancom-systems.de

After installation start the LANCOM VPN Client.

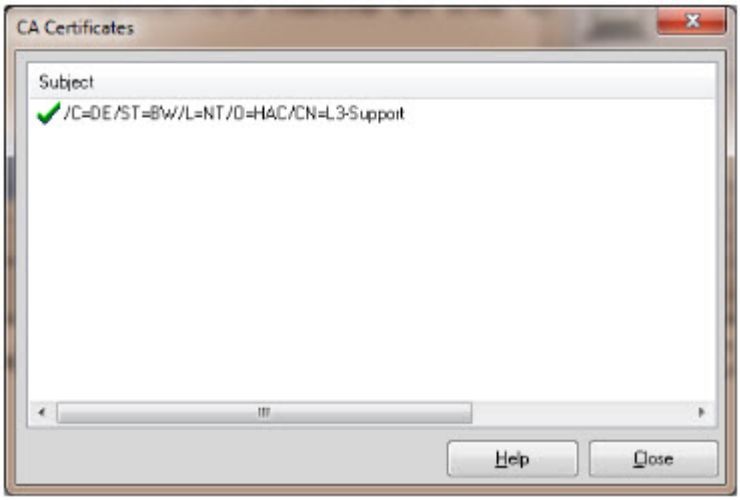
Import Certificates



Copy the PEM export of the CA (in our example L3CA.pem) and the PKCS#12 export of the LANCOM Client certificate (in our example LANCOM_client.p12) in the CaCerts directory: C:\Program Files (x86)\LANCOM\Advanced VPN Client\CaCerts

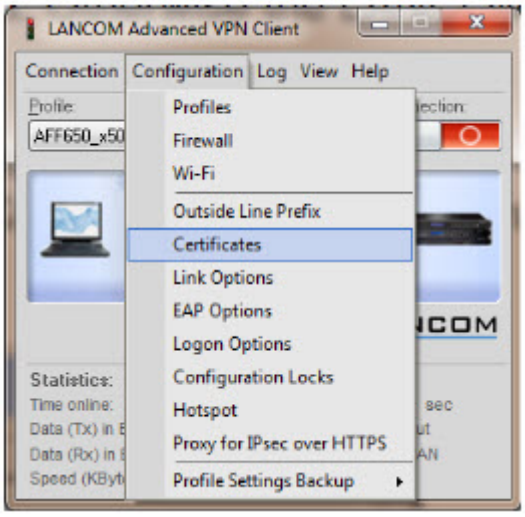
Note: The file extension of the CA export must be .pem otherwise the LANCOM Client will not find the CA.

CA Certificates



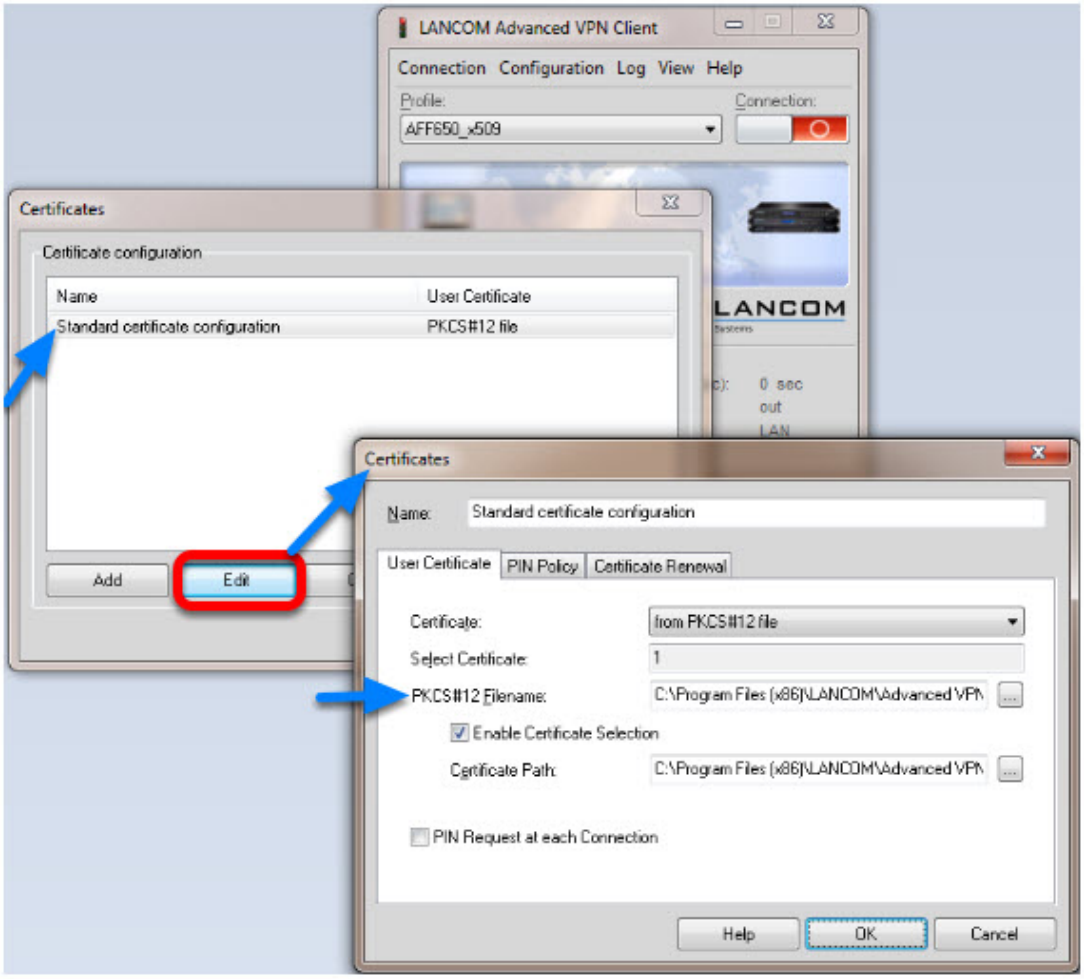
To verify if the LANCOM Client could load the CA, select Connection -> Certificates -> Display CA Certificates from the menu.
The distinguished name of the CA should be displayed, marked with a green checkmark.
Click Close.

Certificates Configuration



Select Configuration -> Certificates from the menu.

Certificate Selection



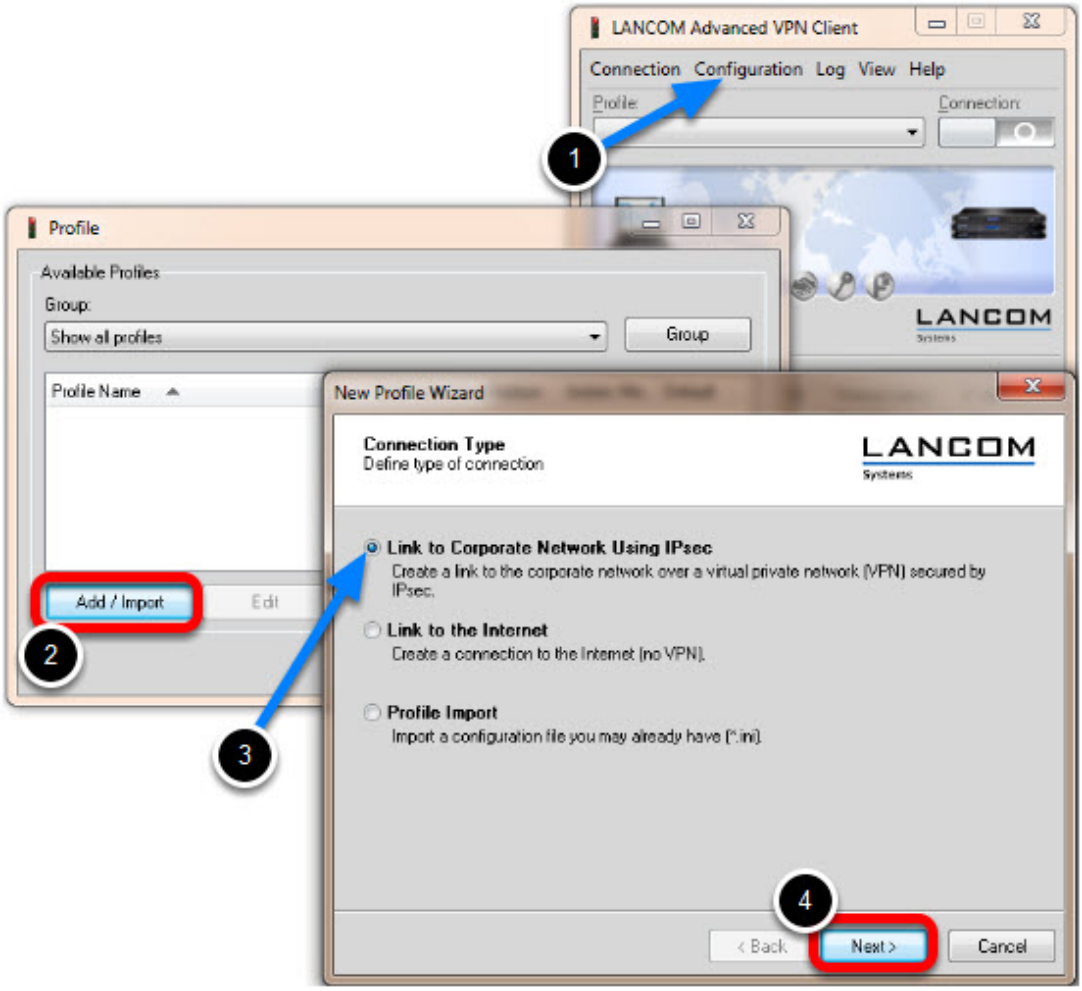
Highlight the Standard certificate configuration and click Edit.

Set the PKCS#12 Filename in our example C:\Program Files (x86)\LANCOM\Advanced VPN Client\CaCerts\LANCOM_Client.p12.

Click OK.

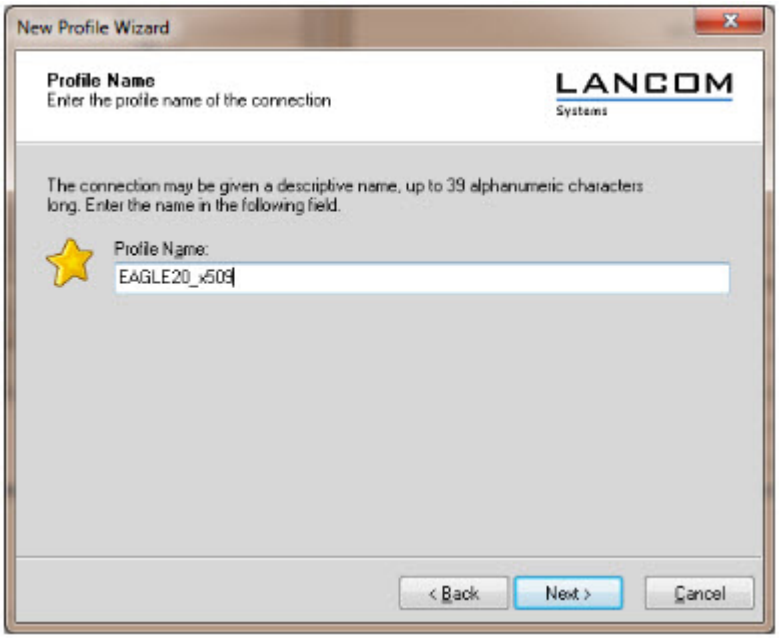
Close the Certificates configuration window.

Creating a new profile



1. Select from the menu Configuration -> Profiles
2. Click Add / Import to create a new profile
3. Select Link to Corporate Network Using IPsec
4. Click Next

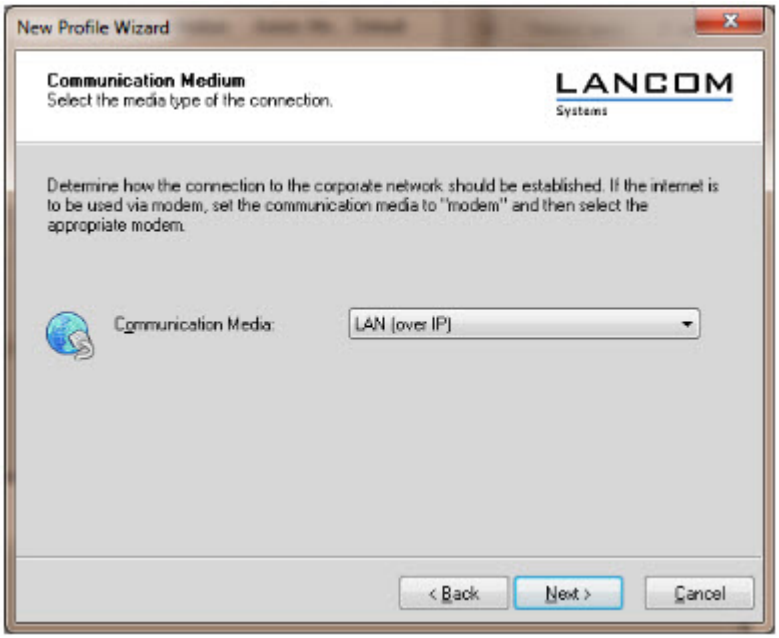
Profile Name



Enter a Profile Name

Click Next

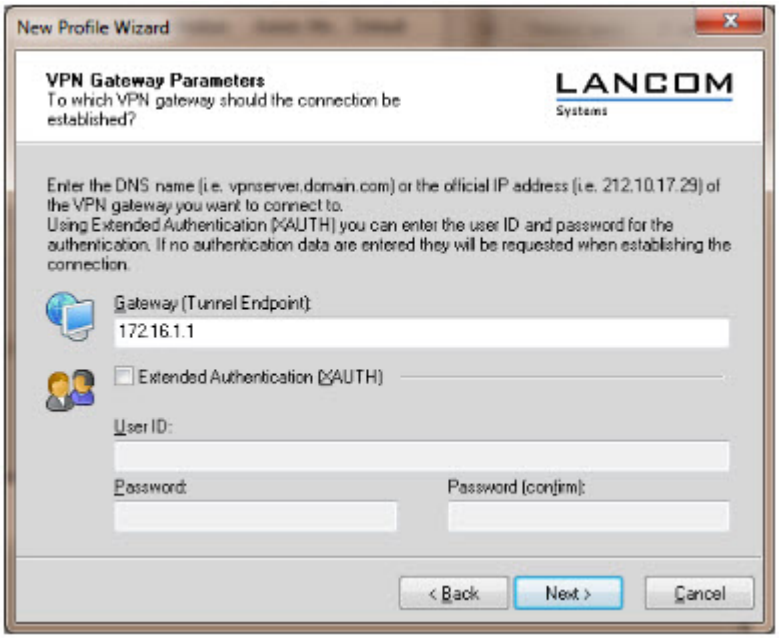
Communication Medium



Select LAN (over IP) as communication media

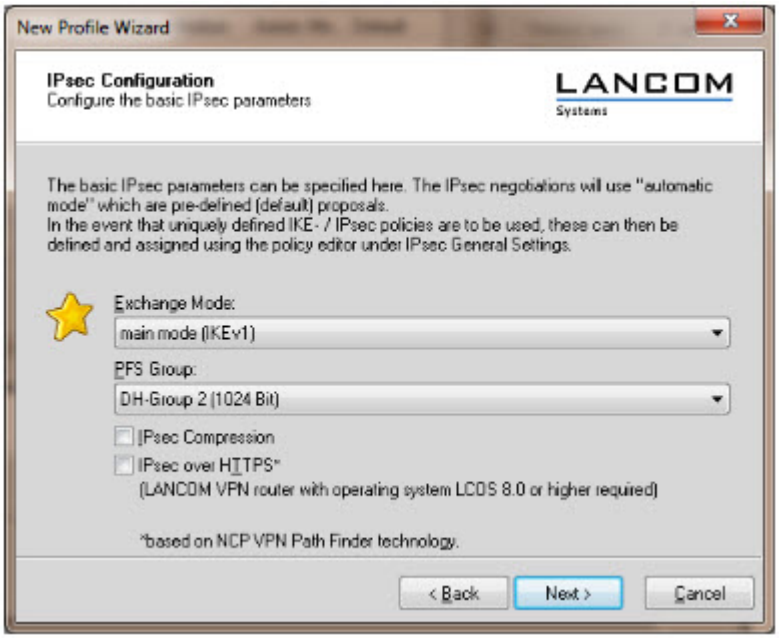
Click Next

VPN Gateway Parameters



Enter the **Gateway** to which the connection should be established. Could be an IP address or DynDNS name.

IPsec Configuration

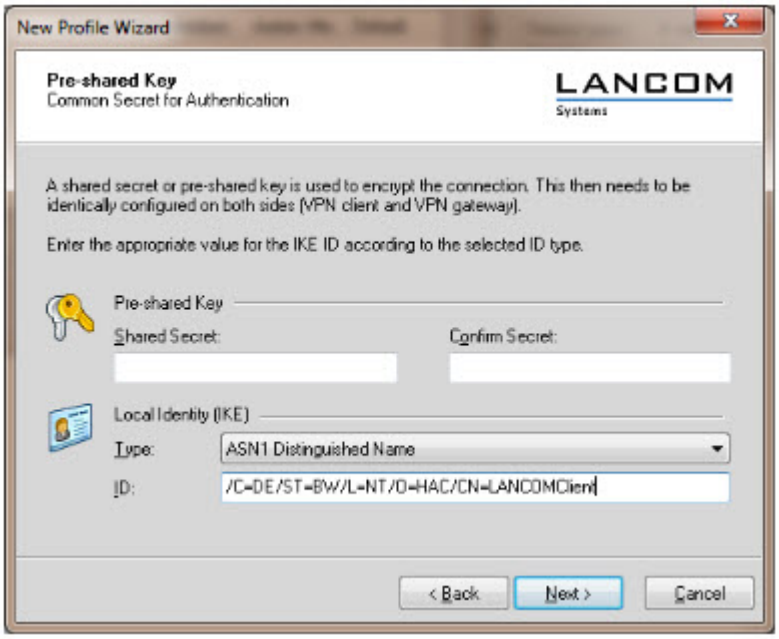


Set the **Exchange Mode** to **main mode (IKEv1)**

Set **PFS Group** to **DH-Group 2 (1024 Bit)**

Click **Next**

Local Identity (IKE)



Delete the pre-shared keys

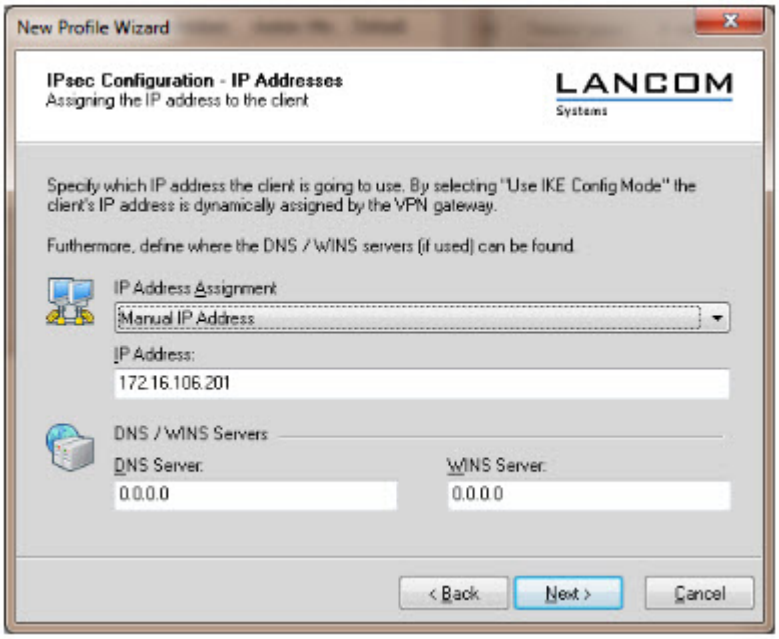
Set the Type to **ASN1 Distinguished Name**

Using the test certificates, copy the DN

/C=DE/ST=BW/L=NT/O=HAC/CN=LANCOMClient in the **ID** field

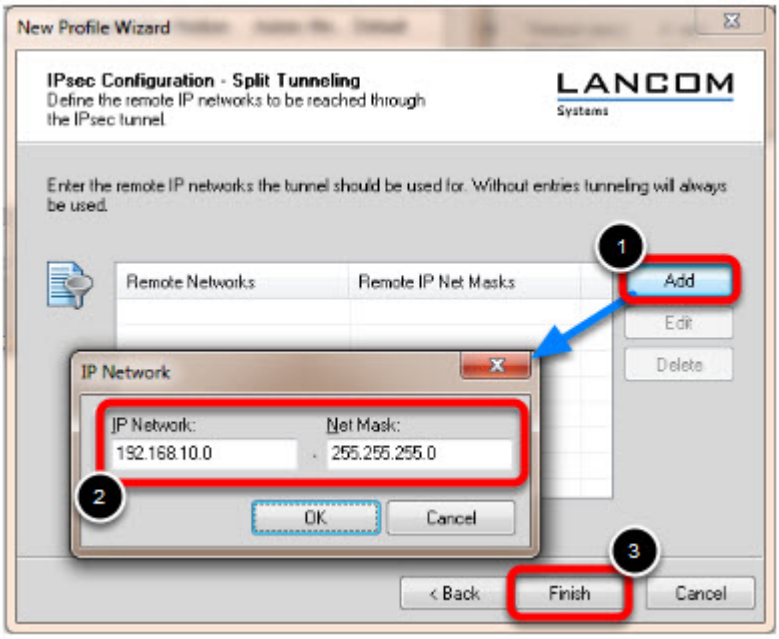
Click **Next**

IPsec Configuration - IP Addresses



Set the **IP Address Assignment** to **Manual IP Address.**

IPsec Configuration - Split Tunneling

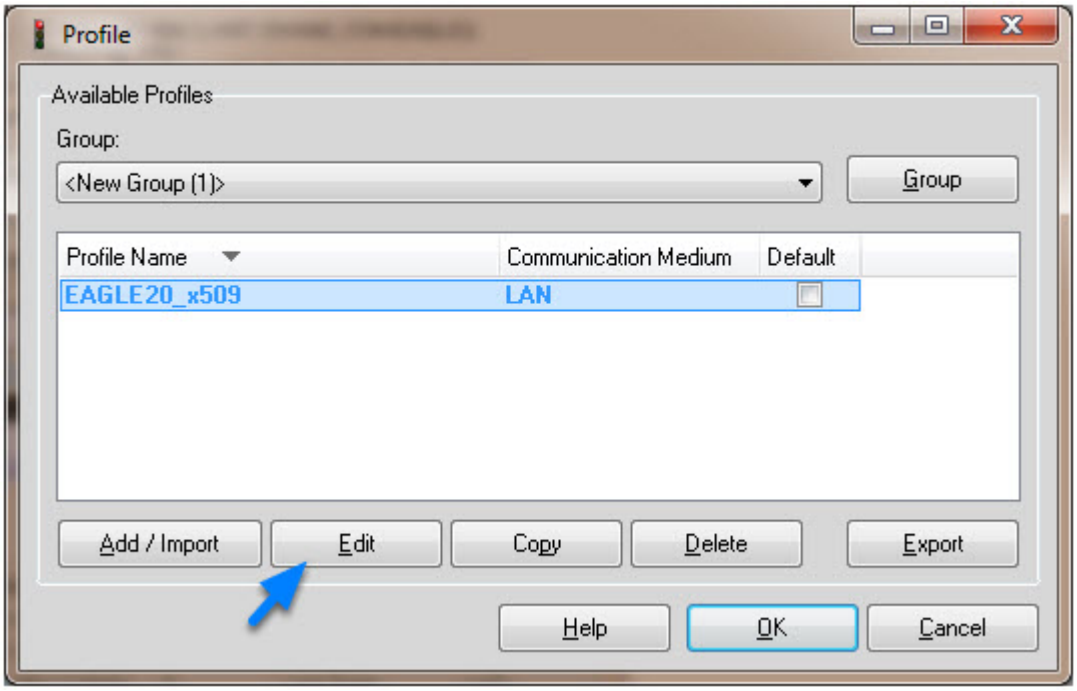


Define the remote IP network to be reached through the IPsec tunnel.

In our example 192.168.10.0/24.

Click Finish.

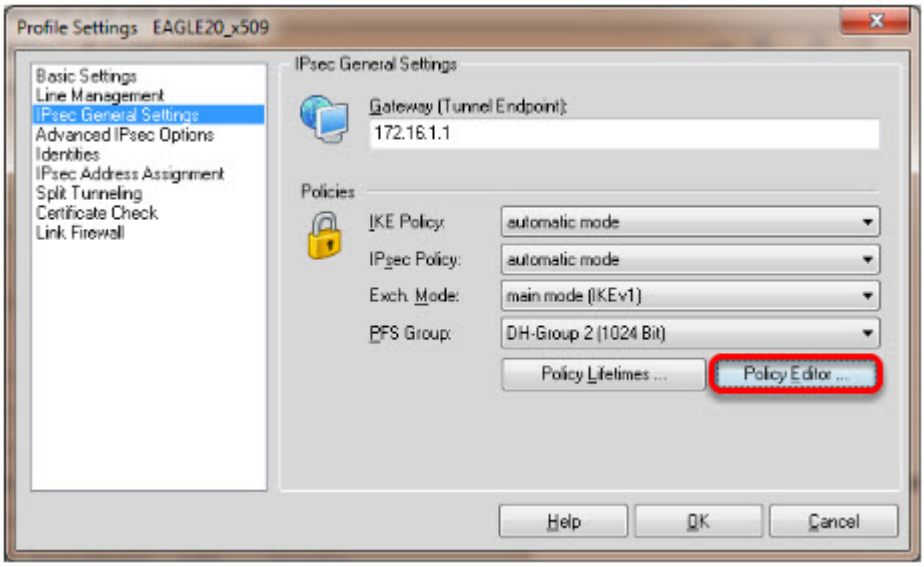
Profile Window



The new profile is created and displayed in the **Profile** window

Highlight the profile and click **Edit.**

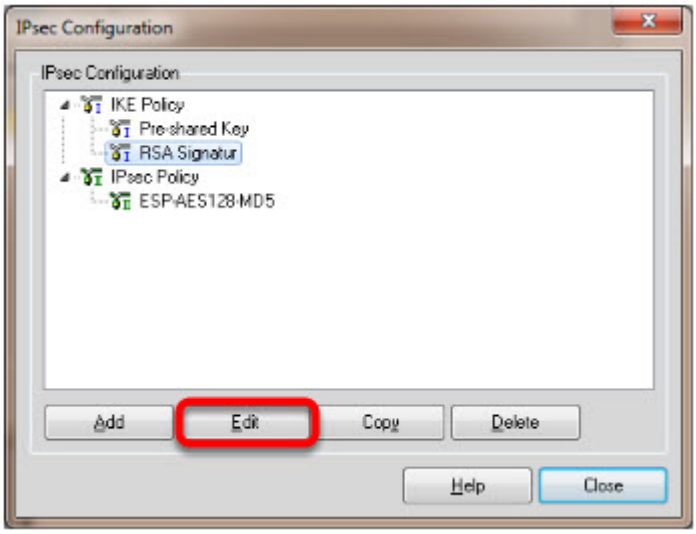
Profile Settings



Highlight **IPsec General Settings** in the left pane.

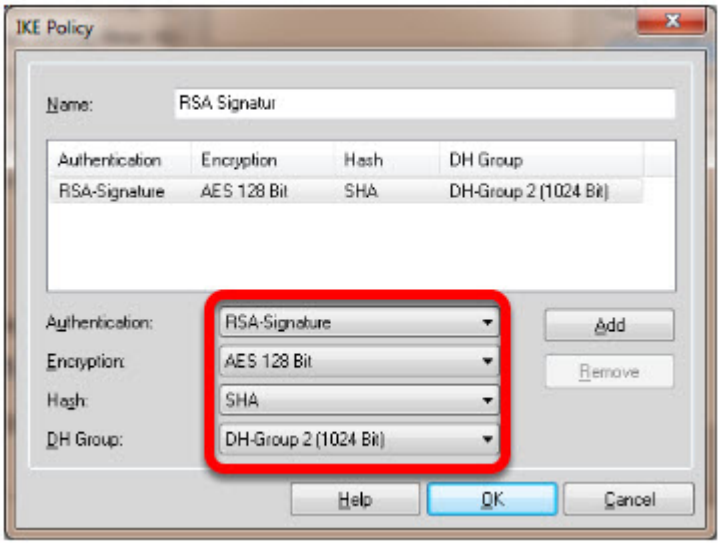
Click **Policy Editor**

IKE Policy Settings



Highlight **RSA Signature** in the IKE Policy

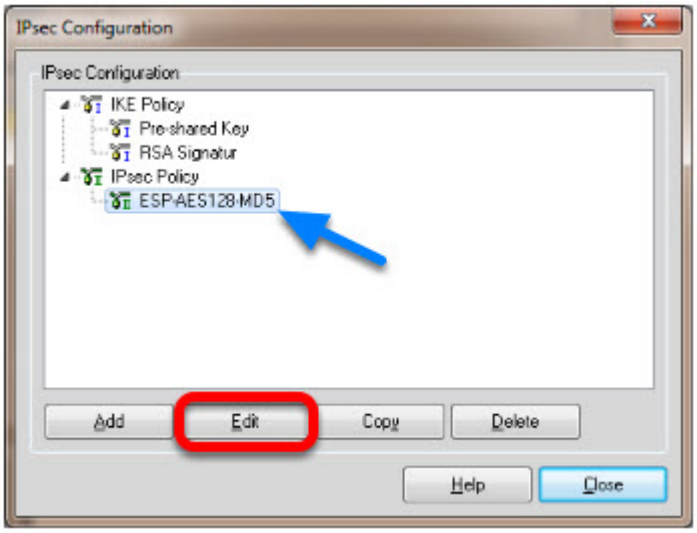
Click **Edit**



Set **Encryption** to **AES 128 Bit.**
Set **Hash** to **SHA.**
Set **DH Group** to **DH-Group 2 (1024 Bit)**

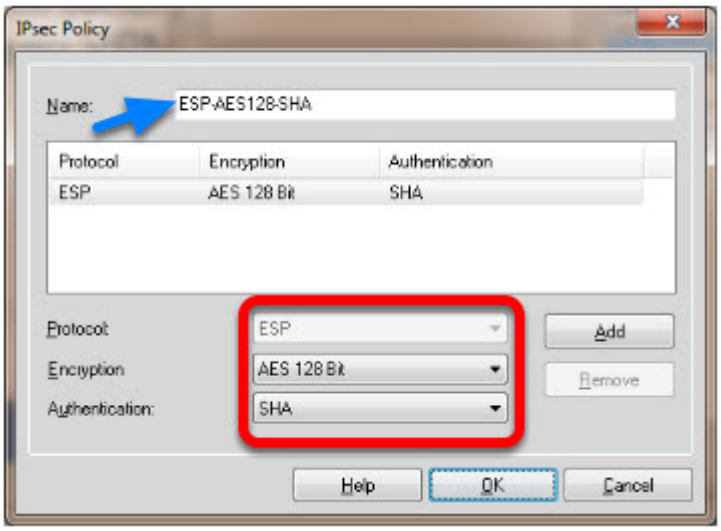
Note: The specified encryption and hash algorithms must correspond to the settings in the EAGLE

IPsec Policy Settings



Highlight the entry **ESP-AES128-MD5** in the **IPsec Policy** tree.

Click **Edit.**



Change the **Name** to **ESP-AES128-SHA.**

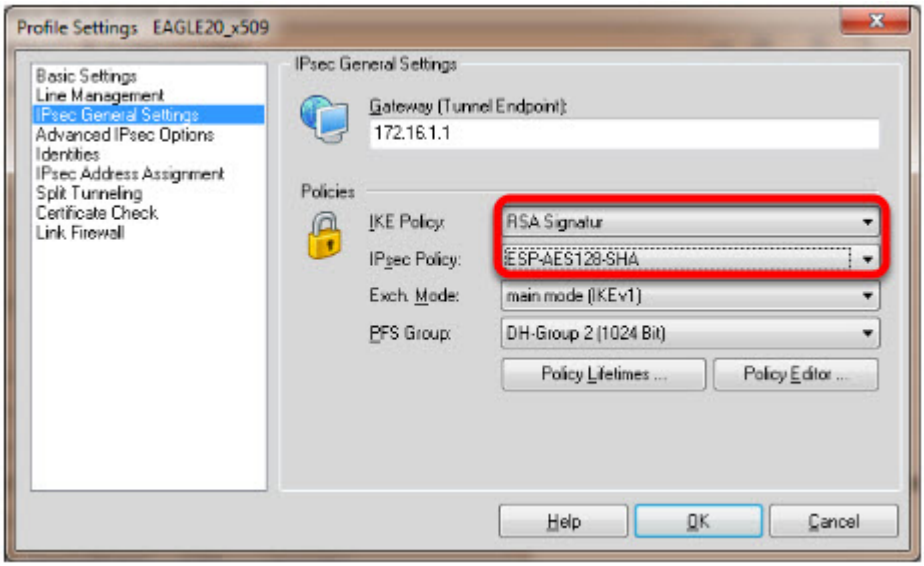
Set **Encryption to AES-128 Bit.**

Set **Authentication** to **SHA.**

Click **OK.**

Close the IPsec Configuration window.

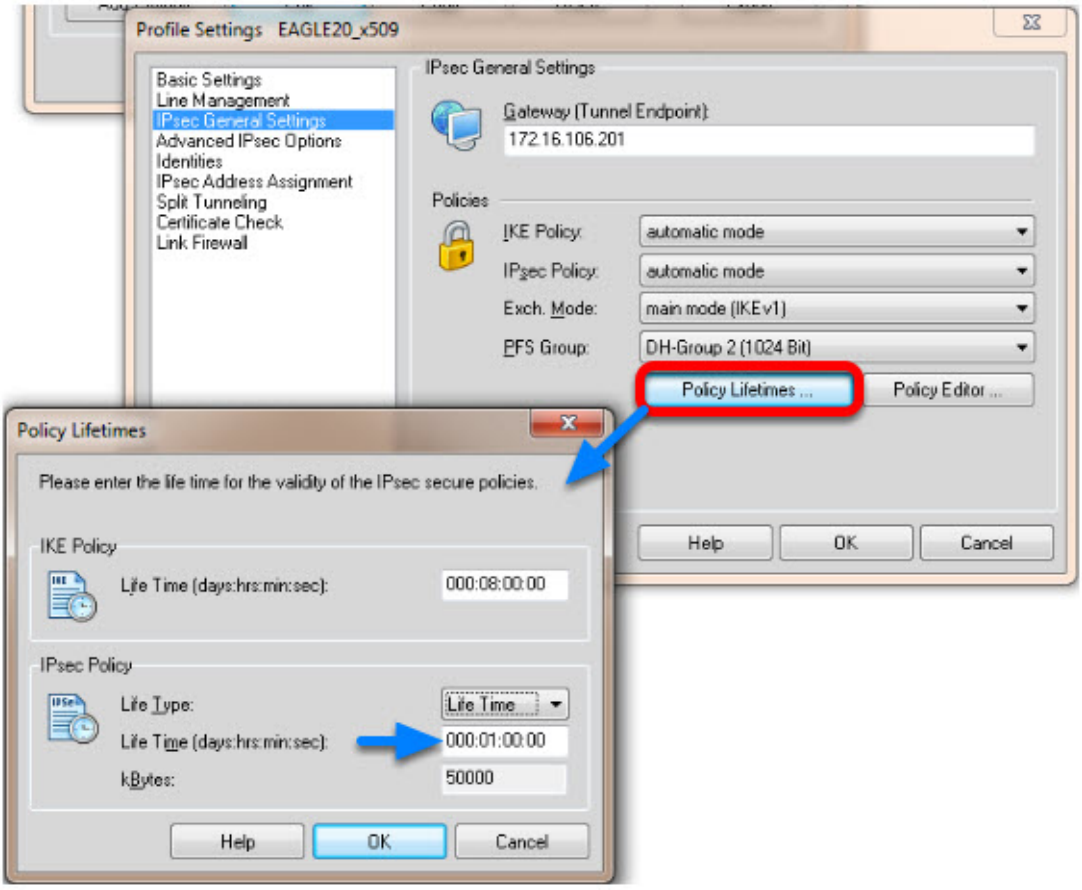
Select IKE and IPsec Policy



Set the IKE Policy to **RSA Signature**

Set the IPsec Policy to **ESP-AES 128-SHA**

Policy Lifetimes

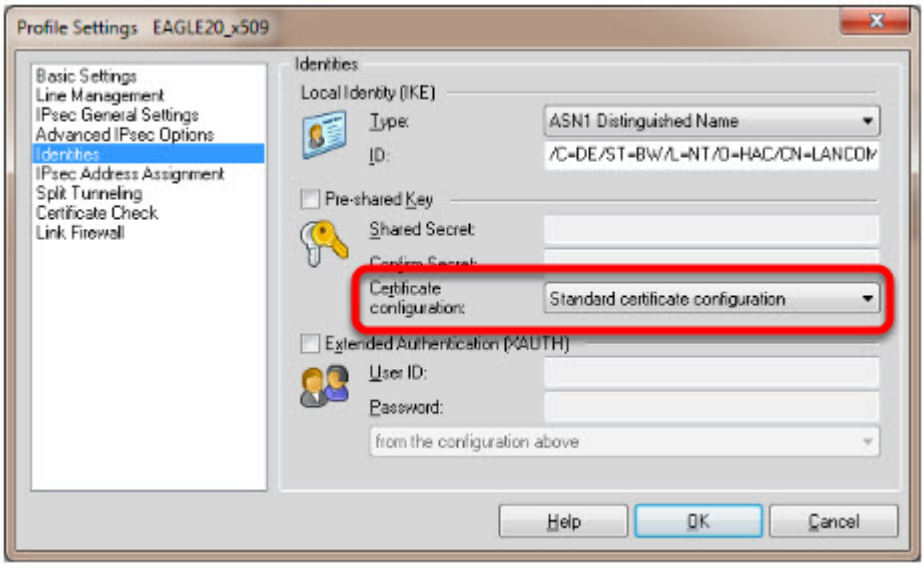


Click the button **Policy Lifetimes.**

Change the **IPsec Policy Life Time** to **1 hour.**

Click **OK.**

Profile Settings - Identities



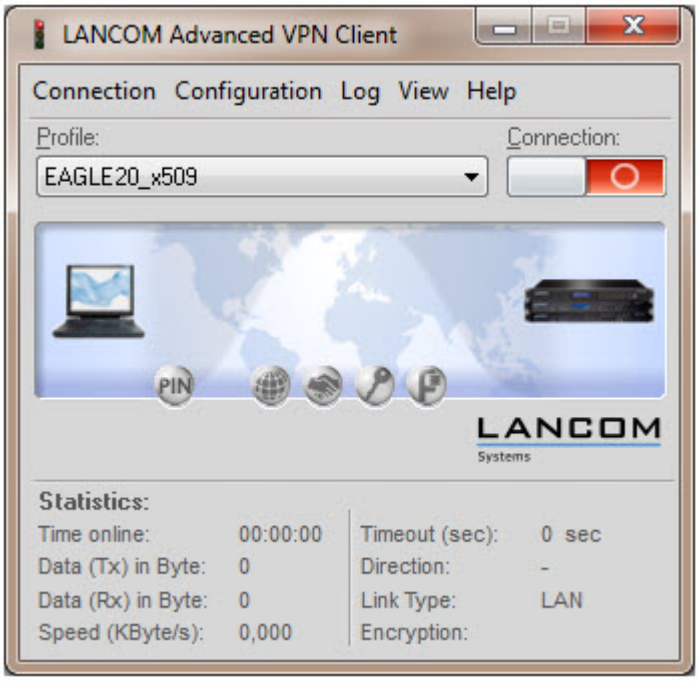
Navigate to **Identities.**

Select **Standard certificate configuration.**

Click **OK.**

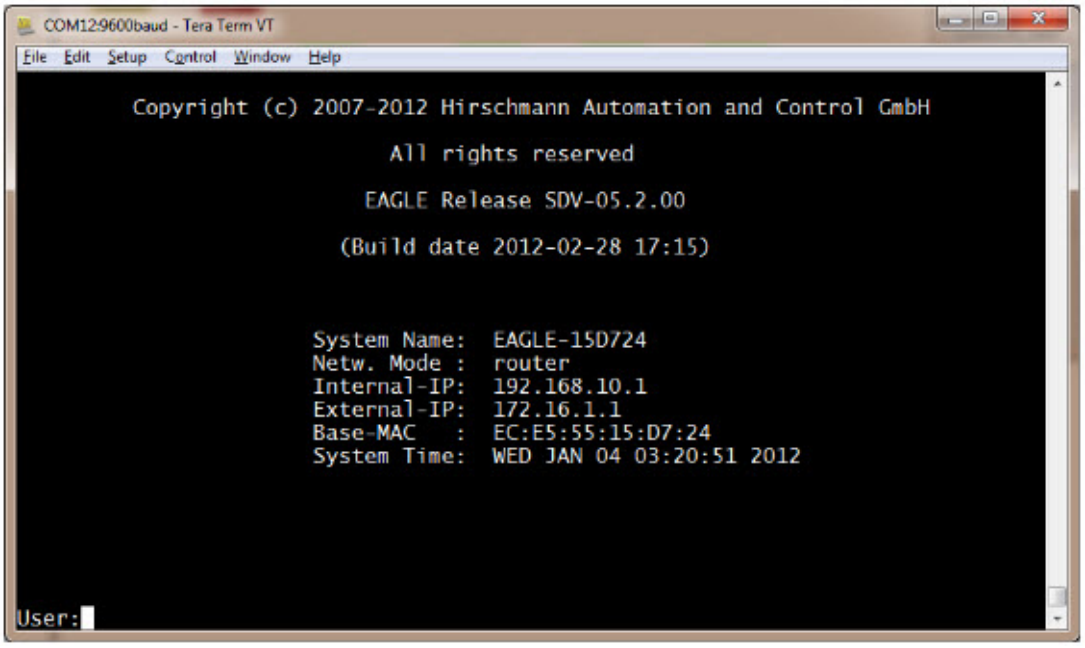
Click **Ok** to close the **Profile** Window.

LANCOM Client configured



The LANCOM Client configuration is finished

EAGLE20 Configuration



1. Switch the EAGLE20 into router mode
2. Set IP addresses of internal and external interface accordingly.

In our example: Internal Interface 192.168.10.1/24; External Interface: 172.16.1.1/24

Starting from a default configuration the CLI commands to configure the device via serial connection are:

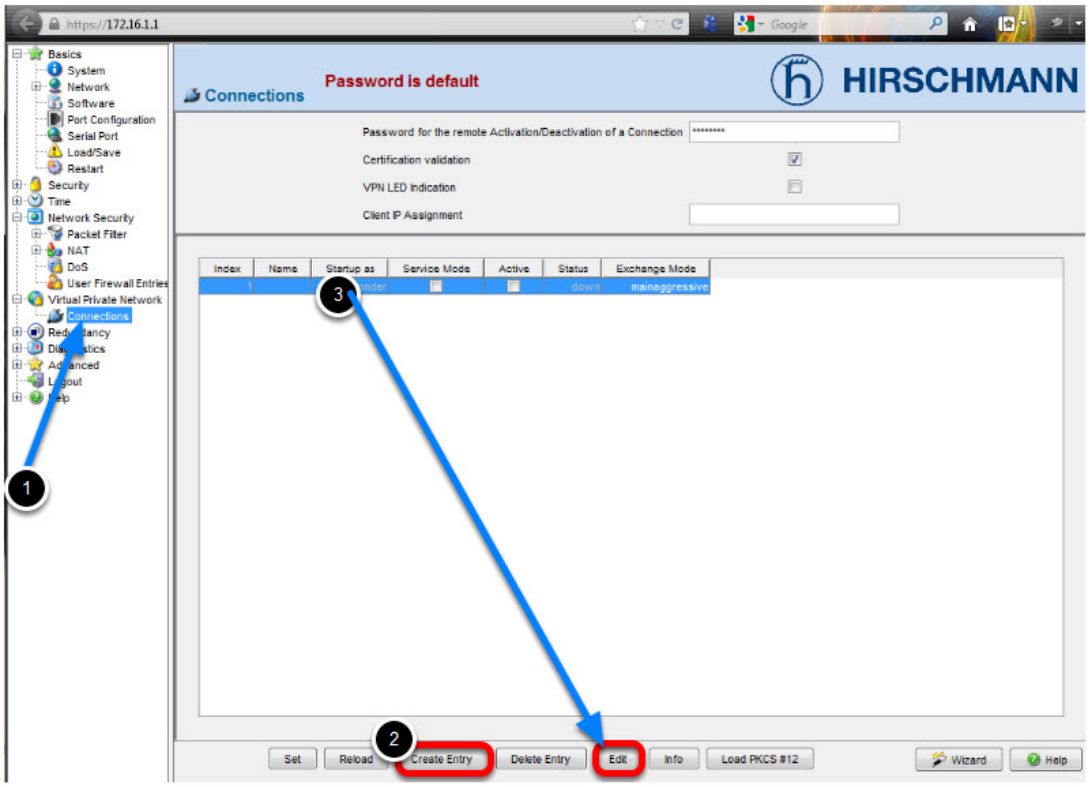
(Hirschmann Eagle) #network mode router

(Hirschmann Eagle) #network router param int ip-address 192.168.10.1

(Hirschmann Eagle) #network router param ext ip-address 172.16.1.1

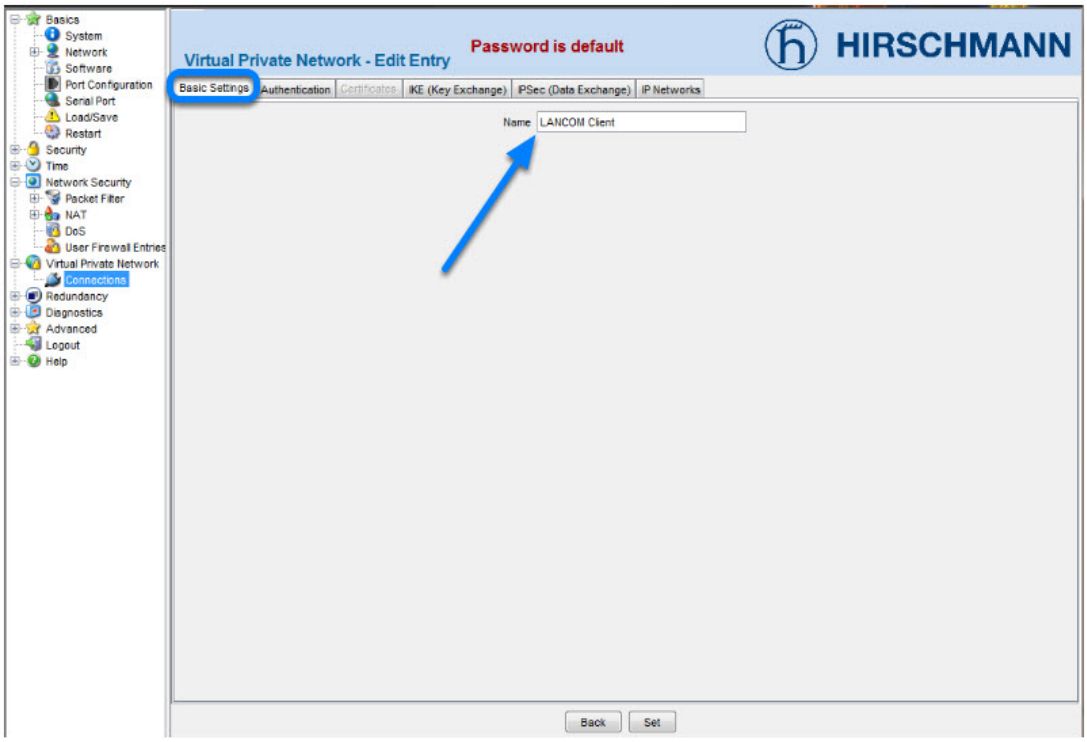
3. Login to the webinterface of the EAGLE20 from the internal network (192.168.10.0/24)

VPN Configuration Web Interface



1. Navigate in the web interface tree to **Virtual Private Network -> Connections**.
2. **Create** a new **Entry**.
3. Highlight the new entry and click **Edit**

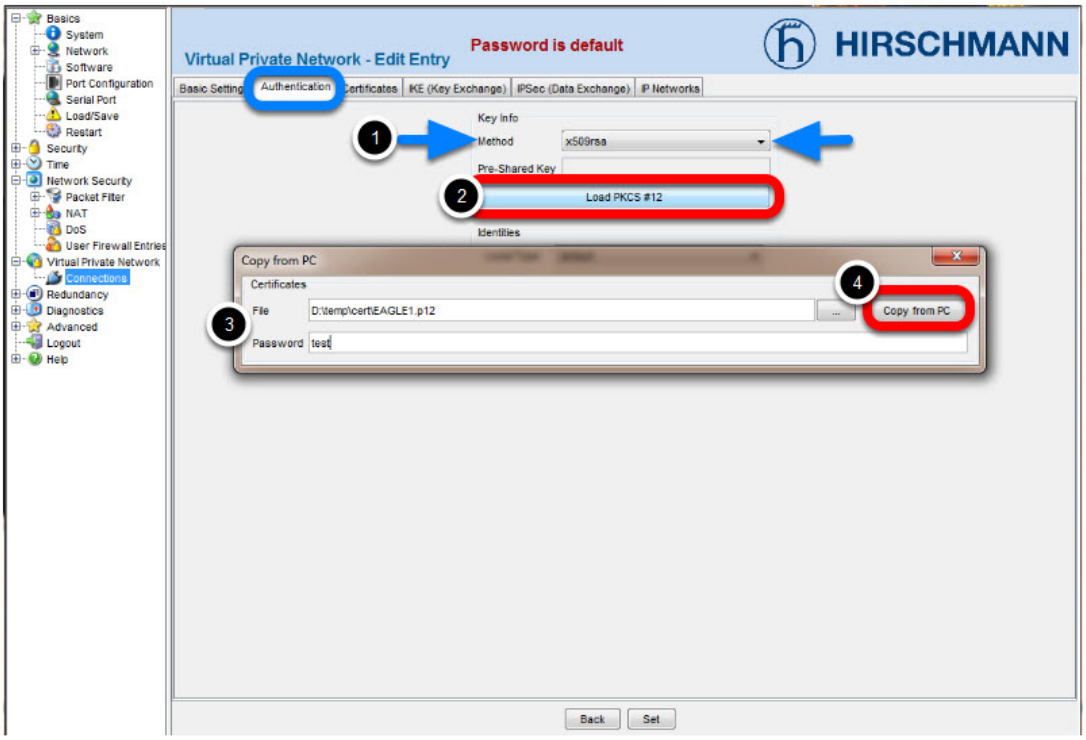
VPN - Basic Settings



Name the VPN connection.

Change to next tab **Authentication.**

VPN - Authentication - Import Certificate



1. Select **x509rsa**.

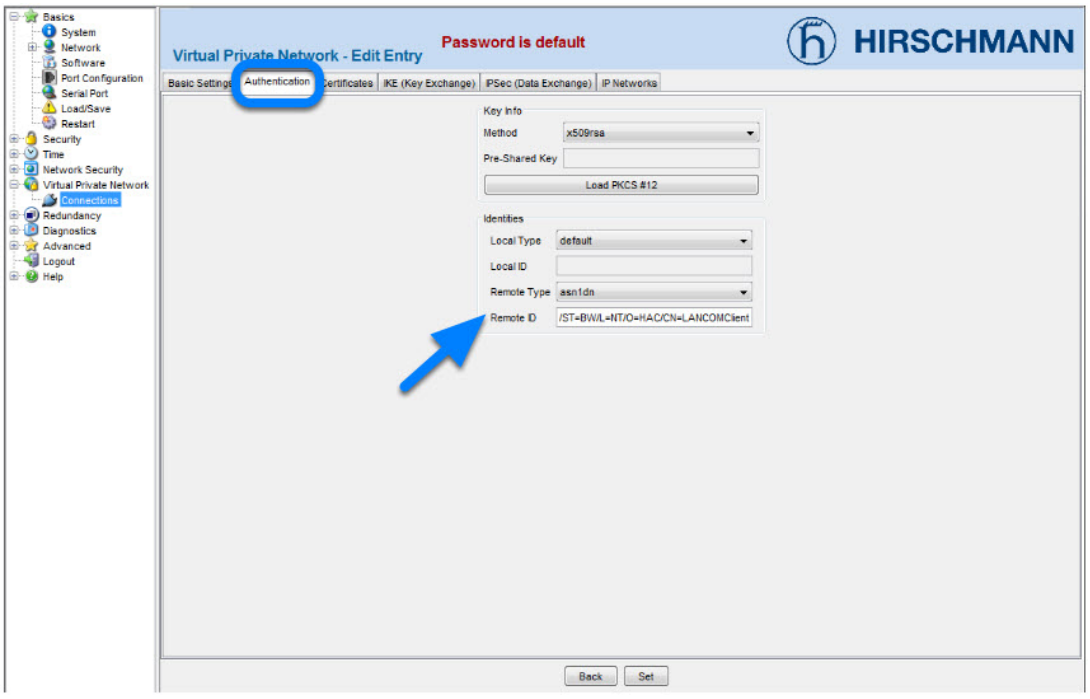
2. Click on **Load PKCS#12**

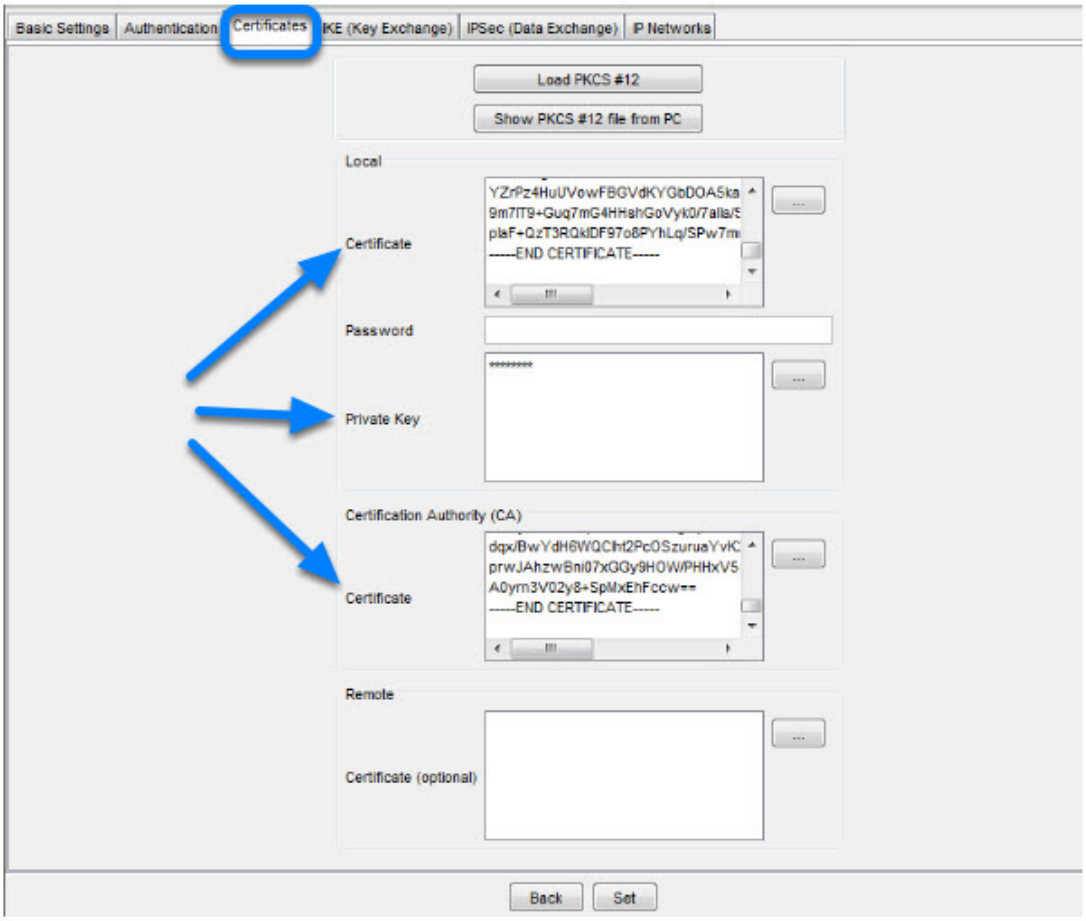
3. Specify location of the AFF certificate and password. The password of the test certificates is 'test'.
4. Click **Copy from PC**

Identities

Change the **Remote Type** to **asn1dn.**
Copy the distinguished name of the LANCOM Client certificatein the field **Remote ID.**
In our example /C=DE/ST=BW/L=NT/O=HAC/CN=LANCOMClient
Change to the next tab **Certificates.**

VPN - Certificates

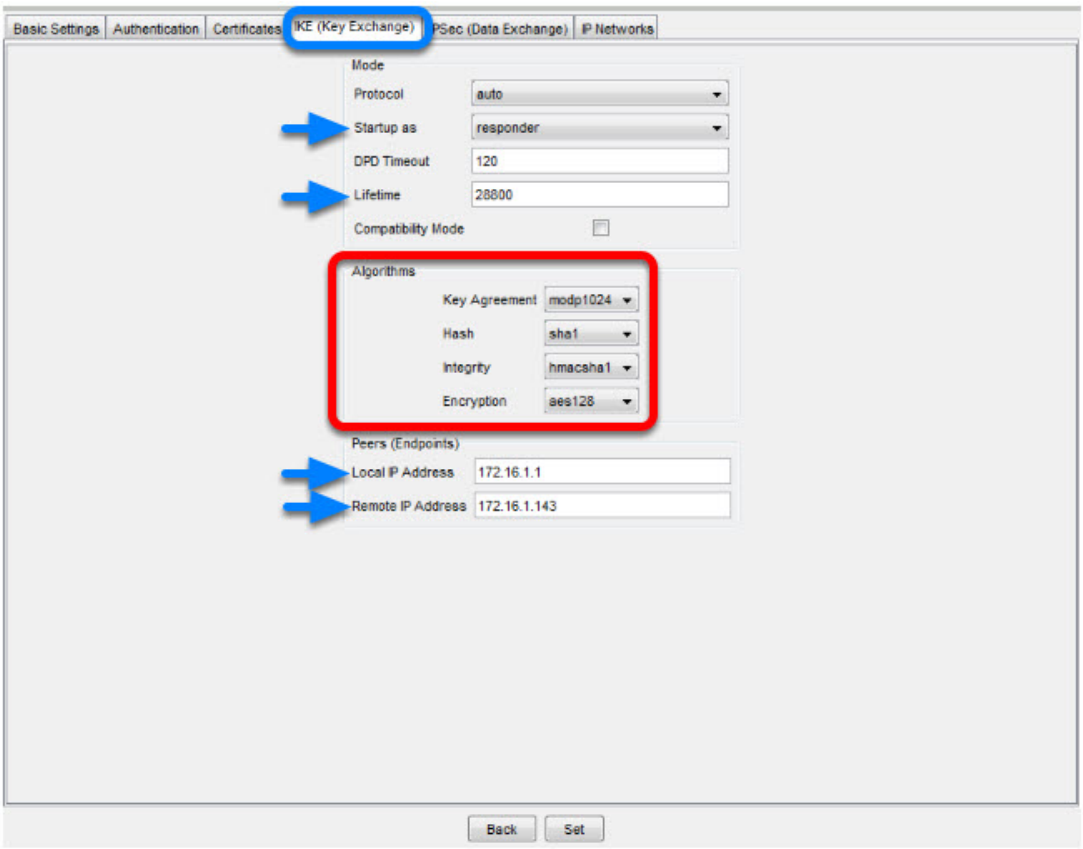




After successfully imported the certificate in the previous step you'll get the content of the PKCS#12 file displayed here.

Change to the next tab **IKE (Key Exchange)**

VPN - IKE (Key Exchange)



1. Set **Startup as** to **responder.**
2. The **Lifetime** should correspond to the LANCOM Client settings (8 hours) but is entered here in seconds.
3. Set the encryption **algorithms** accordingly in our example:

Key Agreement: **modp1024**

Hash: **sha1**

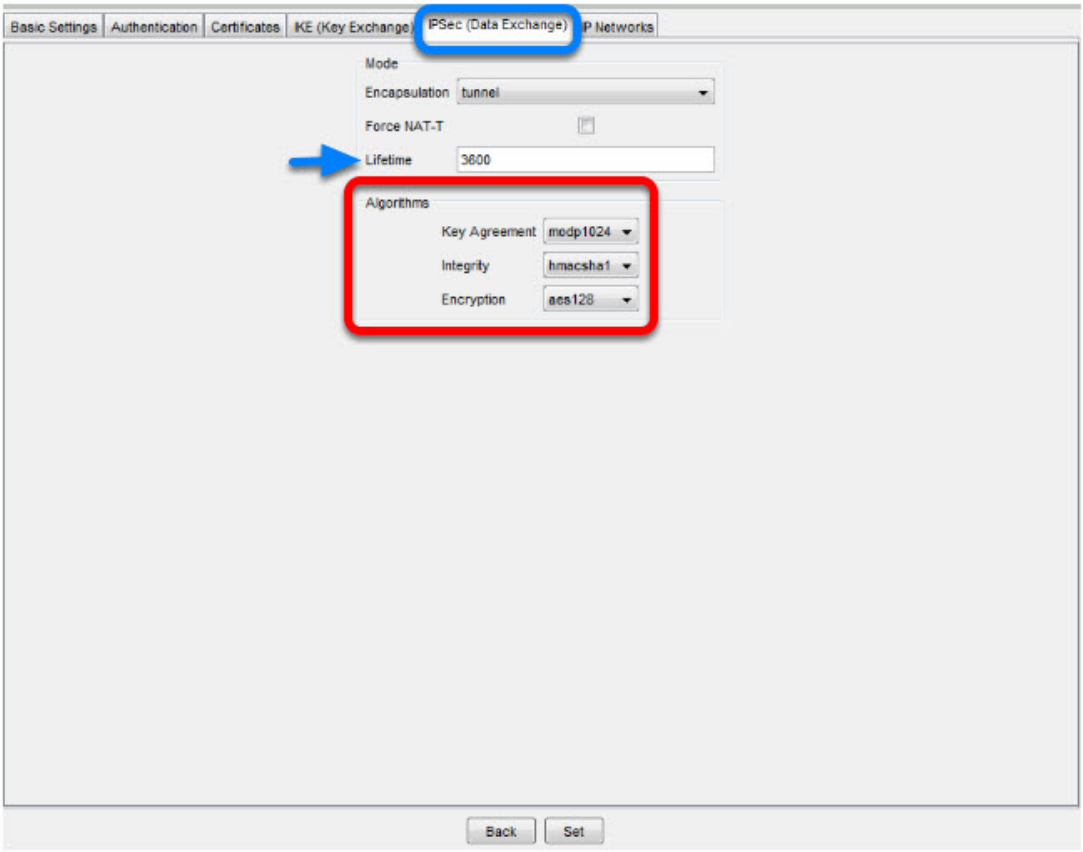
Integrity: **hmacsha1**

Encryption: **aes128**

4. Set the **Local IP Address** to **172.16.1.1**
5. Set the **Remote IP Address** to **172.16.1.143**

Change to the next tab **IPsec (Data Exchange)**

VPN - IPsec (Data Exchange)



The **Lifetime** in seconds should correspond with the settings of the LANCOM Client (1 hour)

Set the encryption **algorithms** accordingly.

In our example:

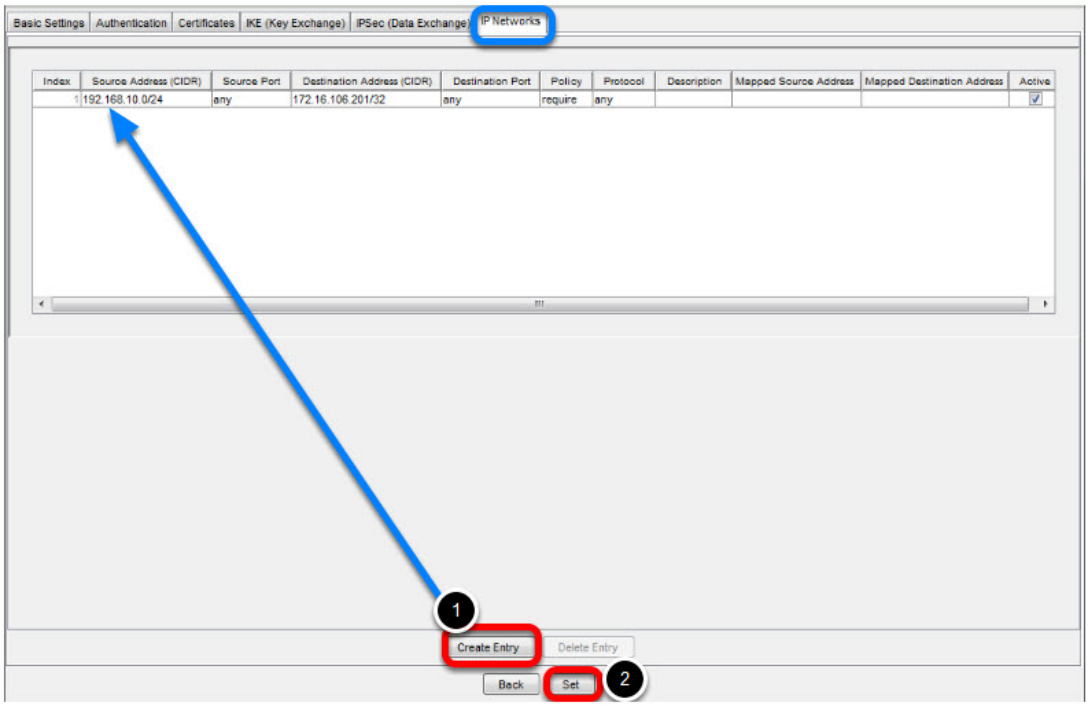
Key Agreement: **modp1024**

Integrity: **hmacsha1**

Encryption: **aes128**

Change to the next tab **IP Networks**

VPN - IP Networks



1. **Create** a new **Entry**

Enter the following values:

Source Address: 192.168.10.0/24 (internal network EAGLE20)

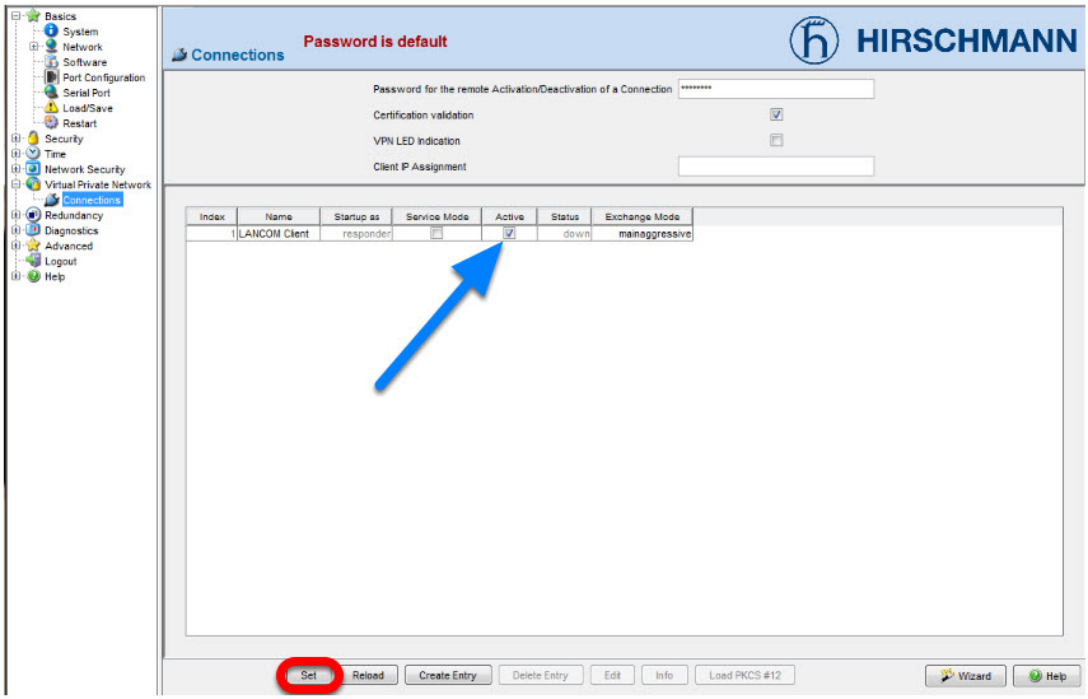
Destination Address: 172.16.106.201/32 (virtual Address of LANCOM Client)

Policy: **require** (traffic is not routed if tunnel is down)

2. Click **Set** to write the changes on all tabs in the device

Click **Back**

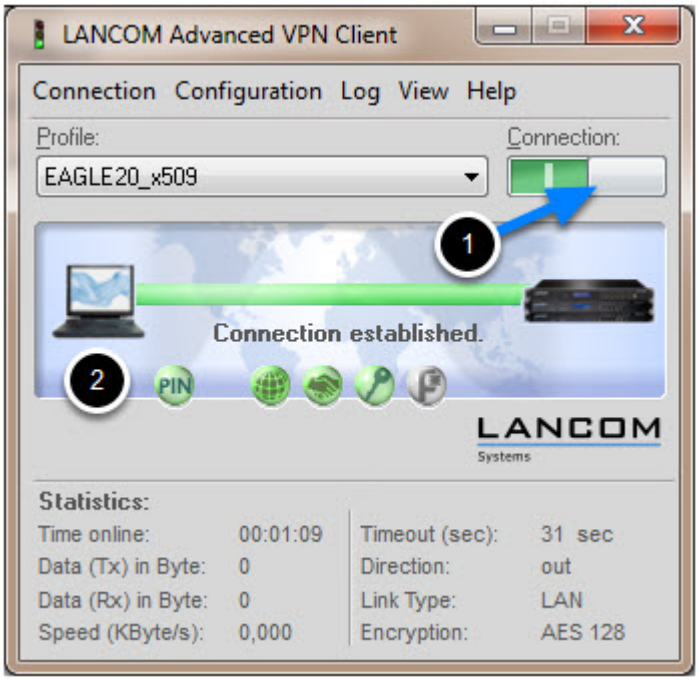
Activate VPN Connection



Activate the created VPN connection.

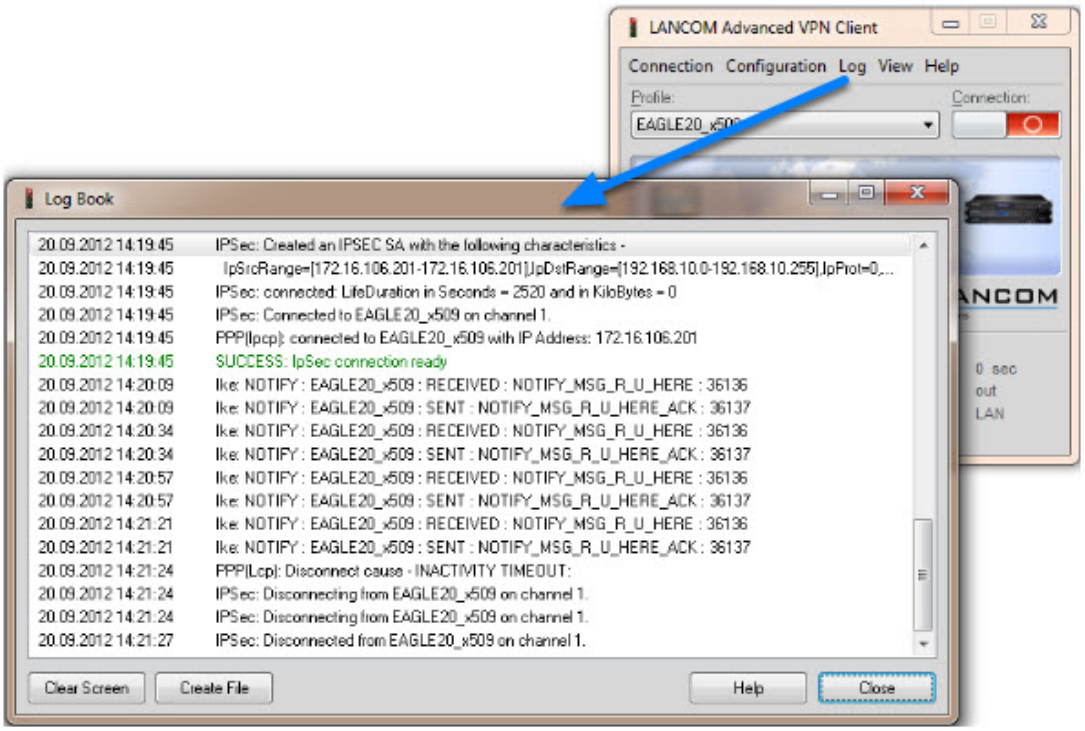
Click **Set**

Initialize Tunnel Setup



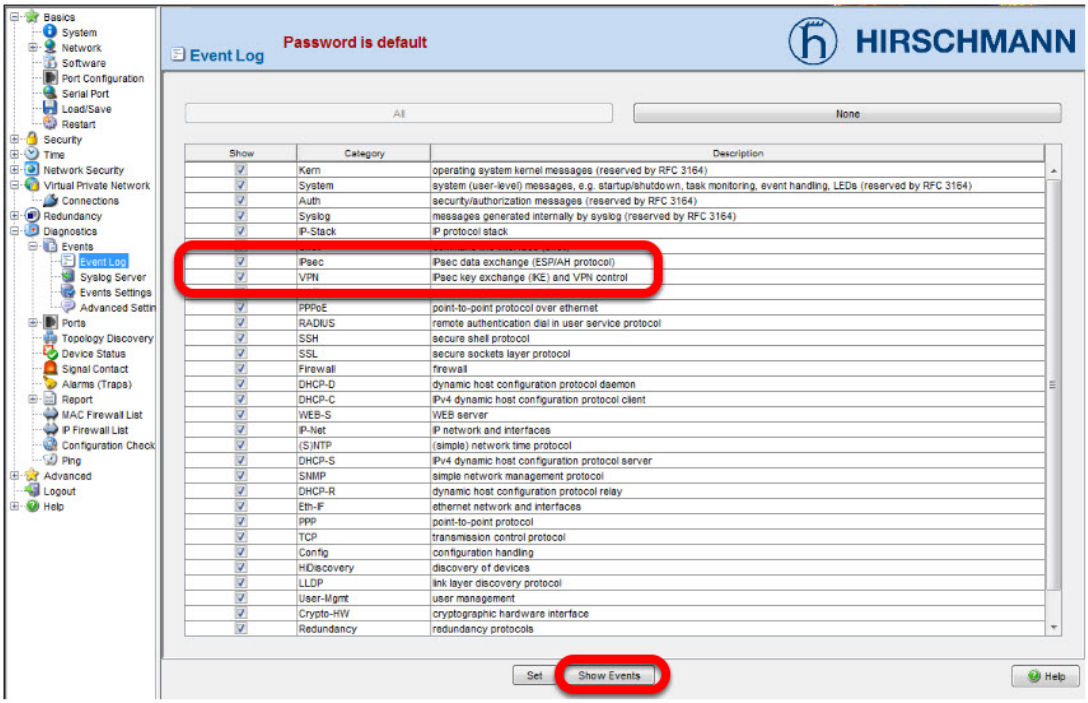
1. Move the Connection slide to the right to initialize the tunnel setup.
You will get prompted to enter the certificate's pin. In our example 'test'
2. The connection should be established successfully.

LANCOM Advanced VPN Client - Log



Select Log -> Logbook

EAGLE20 - Logfile



In the EAGLE20 web interface navigate to **Diagnostics -> Events -> Event Log.**
Make sure that **all** events or at least the **category IPsec** and **VPN VPN** is checked, then click **Show Events**

EAGLE20 Event Log

Event Log

Hirschmann EAGLE Security Device

System software: **EAGLE SDV-05.2.00 2012-02-28 17:15 RAM: SDV-05.2.00 2012-02-28 17:15 BAK: SDV-05.1.00 2011-06-07 11:27**
Network operation mode: **Router Mode**
Network internal interface IP address: **192.168.10.1** MAC address: **ec:e5:55:15:d7:24**
Network external interface IP address: **172.16.1.1** MAC address: **ec:e5:55:15:d7:25**
System name: **EAGLE-15D724**
System uptime: **0 days 0 hours 16 minutes 26 seconds**
System local time: **2012-09-20 14:33:43**

Entrynumber: Time [Taskname, Severity, Facility, Errorcode] Eventinformation

1: 2012-09-20 14:21:43 [tSnmpTrapTask, NOTICE, SNMP, 0x01FB0036] SNMP trap - send vpnDown trap done.

2: 2012-09-20 14:21:43 [tVpnMain, NOTICE, VPN, 0x020000A3] VPN connection 1 is 'DOWN'

3: 2012-09-20 14:21:40 [tHmLog, NOTICE, Syslog, 0x01F60003] There were 1 additional message(s) of the last entry

4: 2012-09-20 14:21:16 [tHmLog, NOTICE, Syslog, 0x01F60003] There were 1 additional message(s) of the last entry

5: 2012-09-20 14:20:52 [tHmLog, NOTICE, Syslog, 0x01F60003] There were 1 additional message(s) of the last entry

6: 2012-09-20 14:20:08 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "VPN-1 received notification R-U-THERE-ACK"

7: 2012-09-20 14:19:45 [tSnmpTrapTask, NOTICE, SNMP, 0x01FB0035] SNMP trap - send vpnUp trap done.

8: 2012-09-20 14:19:45 [tVpnMain, NOTICE, VPN, 0x020000A2] VPN connection 1 is 'UP'

9: 2012-09-20 14:19:44 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "VPN-1 quick mode exchange done in 235 ms (peer: 172.16.1.143, message ID: 44889b98)"

10: 2012-09-20 14:19:44 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "New exchange started (QUICK_MODE with Message ID: 1149803416)"

11: 2012-09-20 14:19:44 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "VPN-1 Main mode exchange done in 520 ms (peer: 172.16.1.143, Message ID: 0)"

12: 2012-09-20 14:19:44 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "VPN-1 received notification INITIAL-CONTACT"

13: 2012-09-20 14:19:43 [ipcom_syslogd, NOTICE, VPN, 0x01F60001] OS-Log "New exchange started (ID_PROT with Message ID: 0)"

14: 2012-09-20 14:19:37 [tSnmpd, NOTICE, VPN, 0x0200000C] VPN connection 1 activated successfully

Back Reload Search Save