

VPN with LANCOM Advanced VPN Client

- 2018-02-22 - HiSecOS

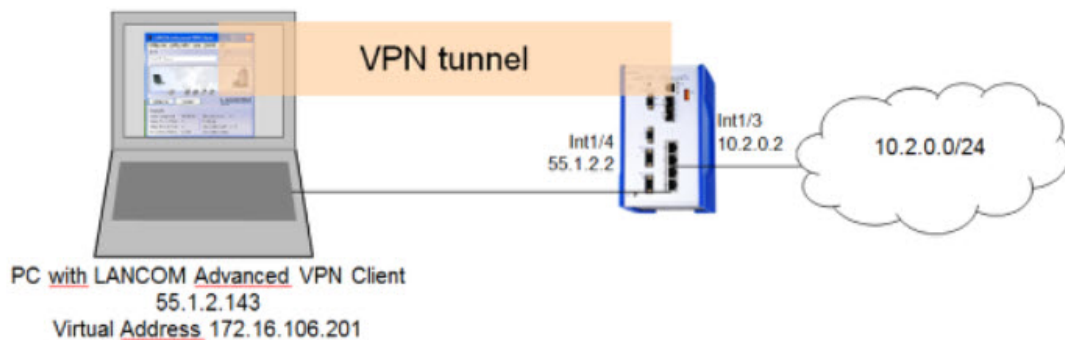
This lesson describes how to configure a VPN using Hirschmann EAGLE20/30 and the LANCOM Advanced VPN Client using x.509 certificates.

Software versions used:

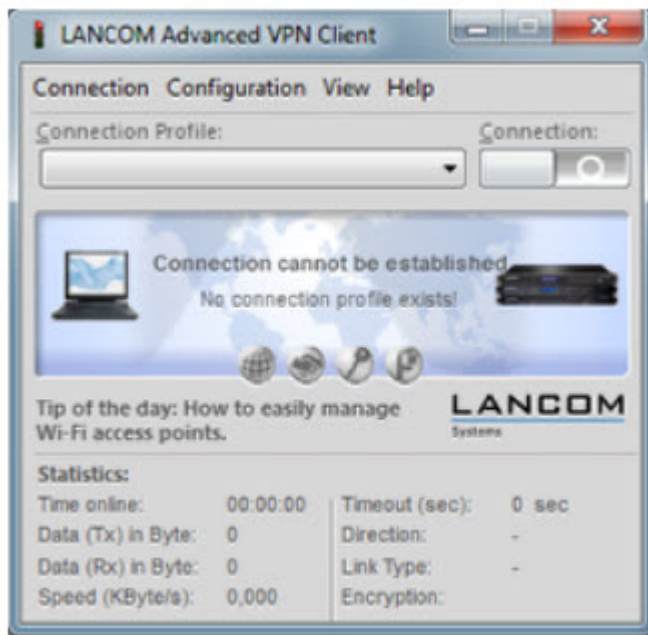
EAGLE20/30 firmware v02.0.01

Lancom Advanced VPN Client v3.00 Build 21499

Network plan



Install and start LANCOM Advanced VPN Client

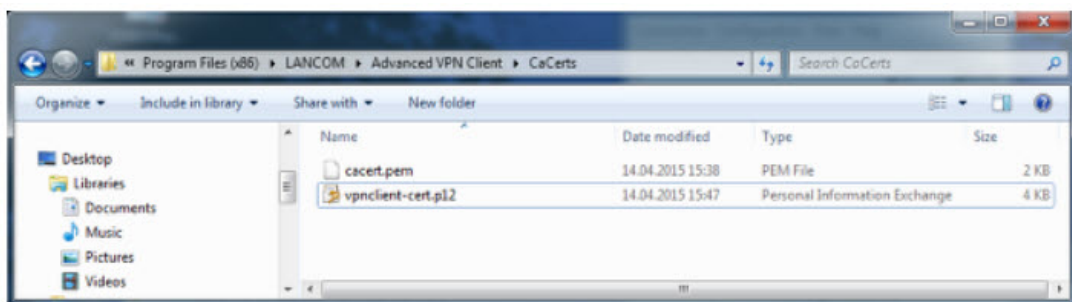


The LANCOM Client with a 30 day evaluation period can be downloaded from

<http://www.lancom-systems.de>

After installation start the LANCOM VPN Client.

Import Certificates

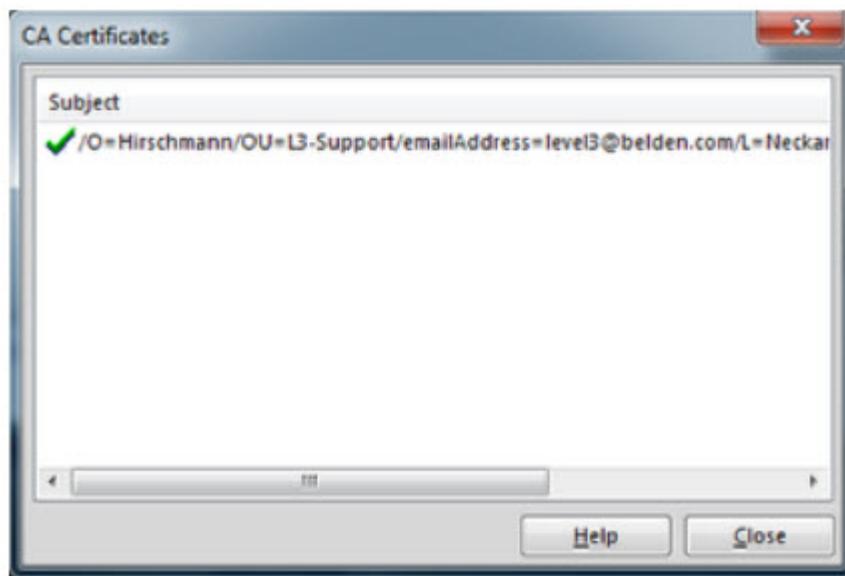


Copy the PEM export of the CA (in our example **cacert.pem**) and the PKCS#12 export of the LANCOM Client certificate (in our example **vpnclient-cert.p12**) in the CaCerts directory:

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.

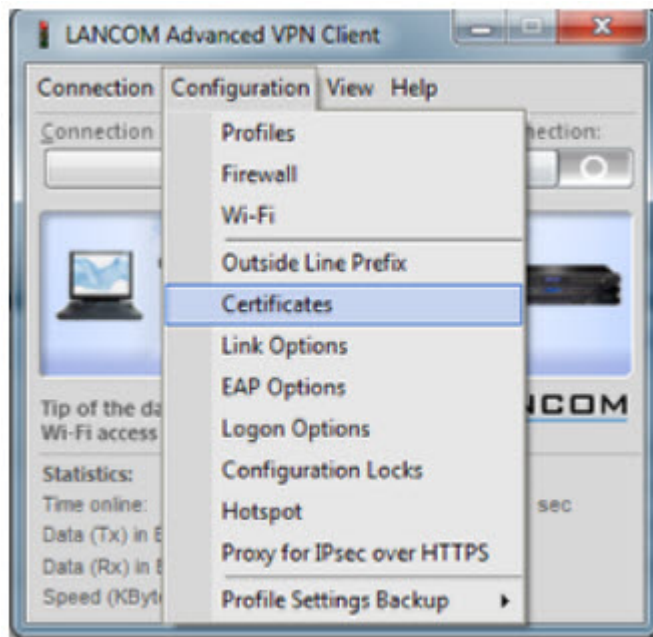
CA Certificates



To verify if the LANCOM Client could load the CA, select **Connection -> Certificates -> Display CA Certificates** from the menu.

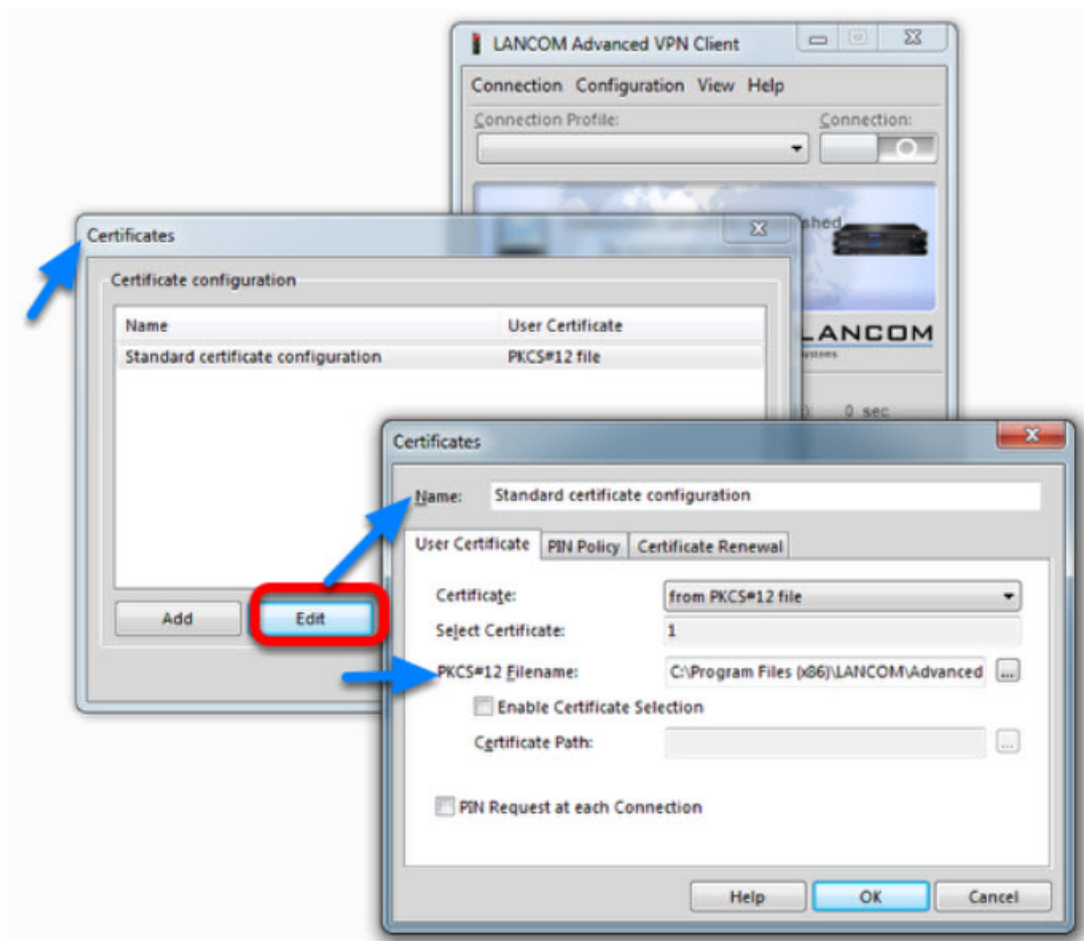
The distinguished name of the CA should be displayed, marked with a green checkmark. Click **Close**.

Certificates Configuration



Select **Configuration -> Certificates** from the menu.

Certificate Selection



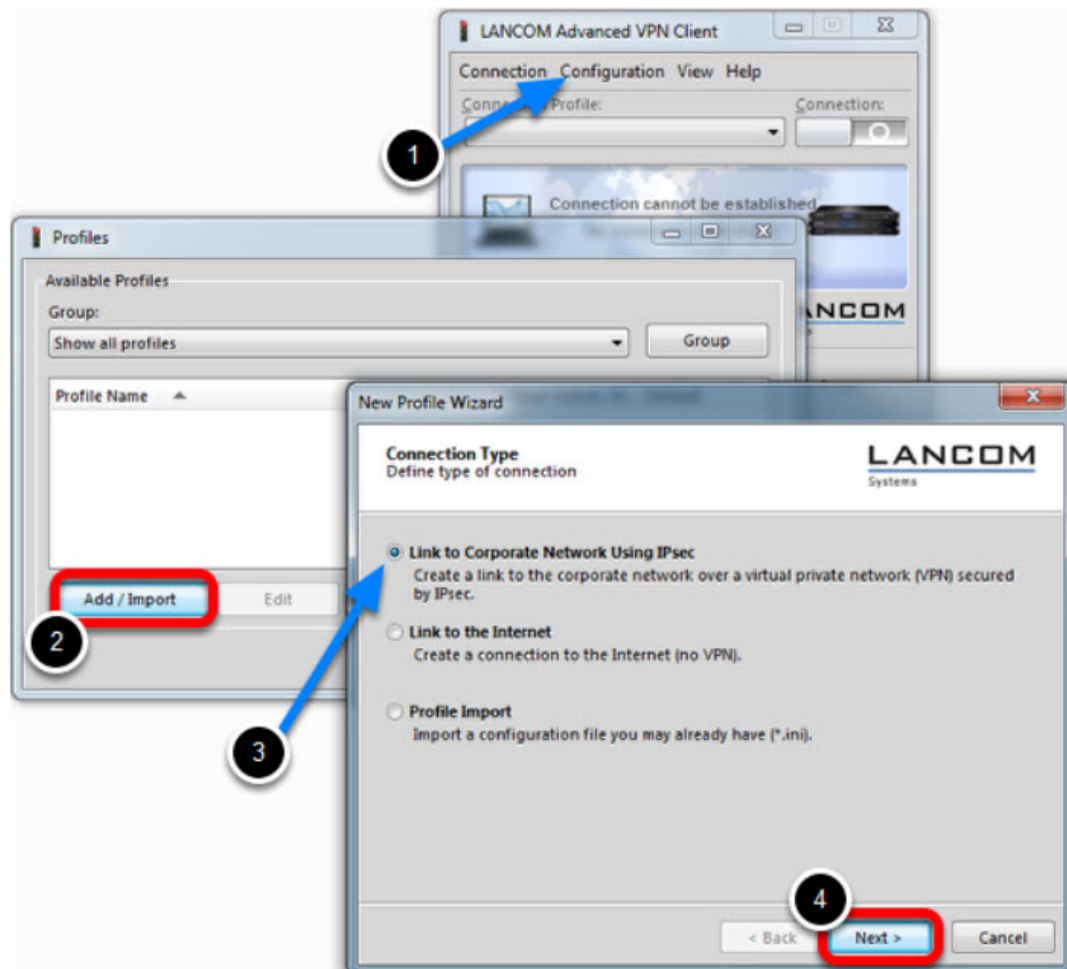
Highlight the **Standard certificate configuration** and click **Edit**.

Set the **PKCS#12 Filename** in our example C:\Program Files (x86)\LANCOM\Advanced VPN Client\CaCerts\vpnclient-cert.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

New Profile Wizard

Profile Name
Enter the profile name of the connection

LANCOM
Systems

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

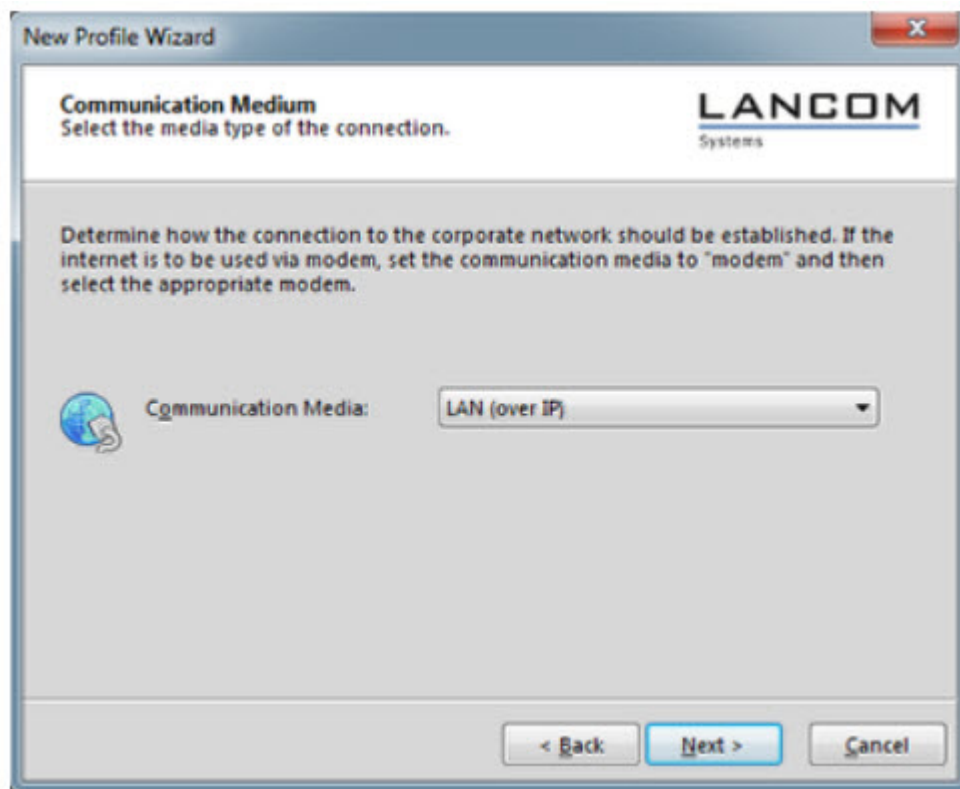
 Profile Name:
EAGLE30_x509

< Back Next > Cancel

Enter a **Profile Name**

Click **Next**

Communication Medium



Select **LAN (over IP)** as communication media

Click **Next**


VPN Gateway Parameters


New Profile Wizard

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

LANCOM
Systems

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to.
Using Extended Authentication (XAUTH) 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 (XAUTH)**

User ID:

Password: **Password (confirm):**

< Back Next > Cancel

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


IPsec Configuration

New Profile Wizard

IPsec Configuration
Configure the basic IPsec parameters

LANCOM
Systems

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:**
main mode (IKEv1)

PFS Group:
DH-Group 2 (1024 Bit)

☐ IPsec Compression

☐ IPsec over HTTPS*
(LANCOM VPN router with operating system LCOS 8.0 or higher required)

*based on NCP VPN Path Finder technology.

< Back Next > Cancel

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

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

Click **Next**

Local Identity (IKE)

The screenshot shows the 'New Profile Wizard' window from LANCOM Systems. The title bar says 'New Profile Wizard' with a close button. The window has a header with 'Pre-shared Key' and 'Common Secret for Authentication' on the left, and the 'LANCOM Systems' logo on the right. Below the header, there is explanatory text: 'A shared secret or pre-shared key is used to encrypt the connection. This then needs to be identically configured on both sides (VPN client and VPN gateway). Enter the appropriate value for the IKE ID according to the selected ID type.' The main area contains two sections. The first section, 'Pre-shared Key', is accompanied by a key icon and has two text input fields labeled 'Shared Secret:' and 'Confirm Secret:'. The second section, 'Local Identity (IKE)', is accompanied by a user icon and has a 'Type:' dropdown menu set to 'ASN1 Distinguished Name' and an 'ID:' text input field containing the value '/C=DE/ST=BW/O=Hirschmann/OU=L3-Support/CN=VPNCLIENT'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Delete the pre-shared keys

Set the Type to **ASN1 Distinguished Name**

Using the test certificates, copy the DN **/C=DE/ST=BW/O=Hirschmann/OU=L3-Support/CN=VPNCLIENT** in the **ID** field

Click **Next**

IPsec Configuration - IP Addresses


New Profile Wizard

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


LANCOM
Systems

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**
Manual IP Address

IP Address:
172.16.106.201

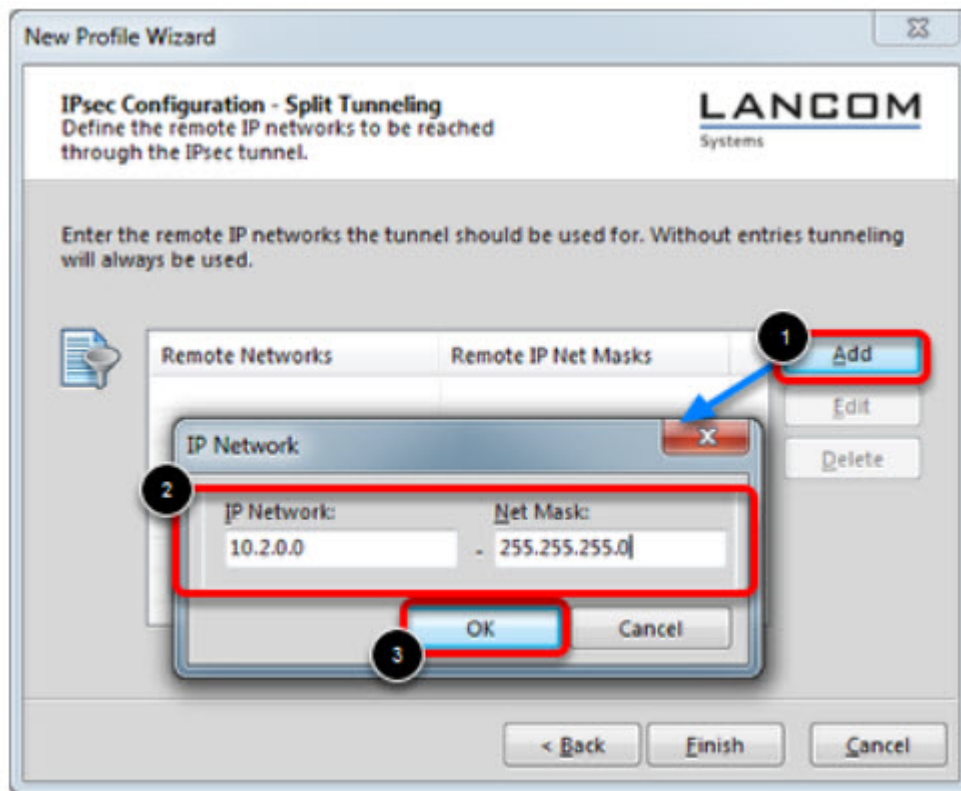
 **DNS / WINS Servers**

DNS Server: 0.0.0.0 **WINS Server:** 0.0.0.0

< Back Next > Cancel

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

IPsec Configuration - Split Tunneling

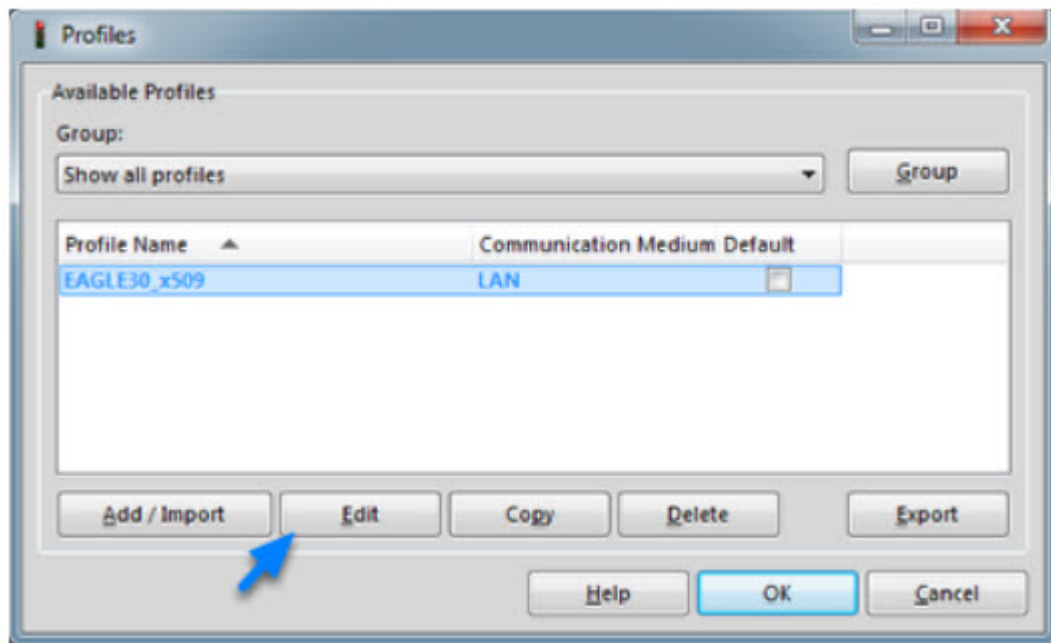


Define the remote IP network to be reached through the IPsec tunnel.

In our example 10.2.0.0/24.

Click Finish.

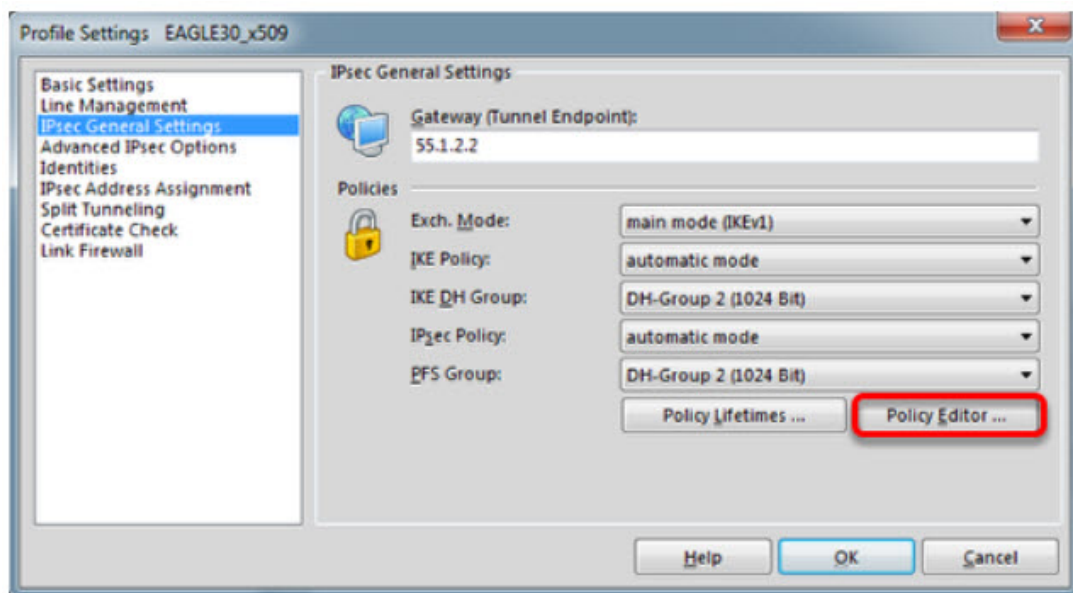
Profile Window



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

Highlight the profile and click **Edit**.

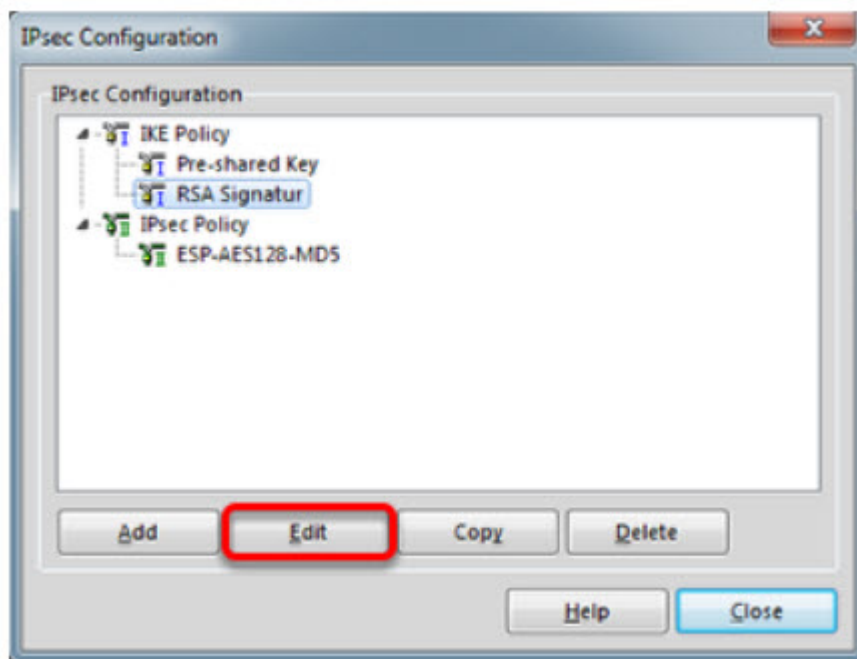
Profile Settings



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

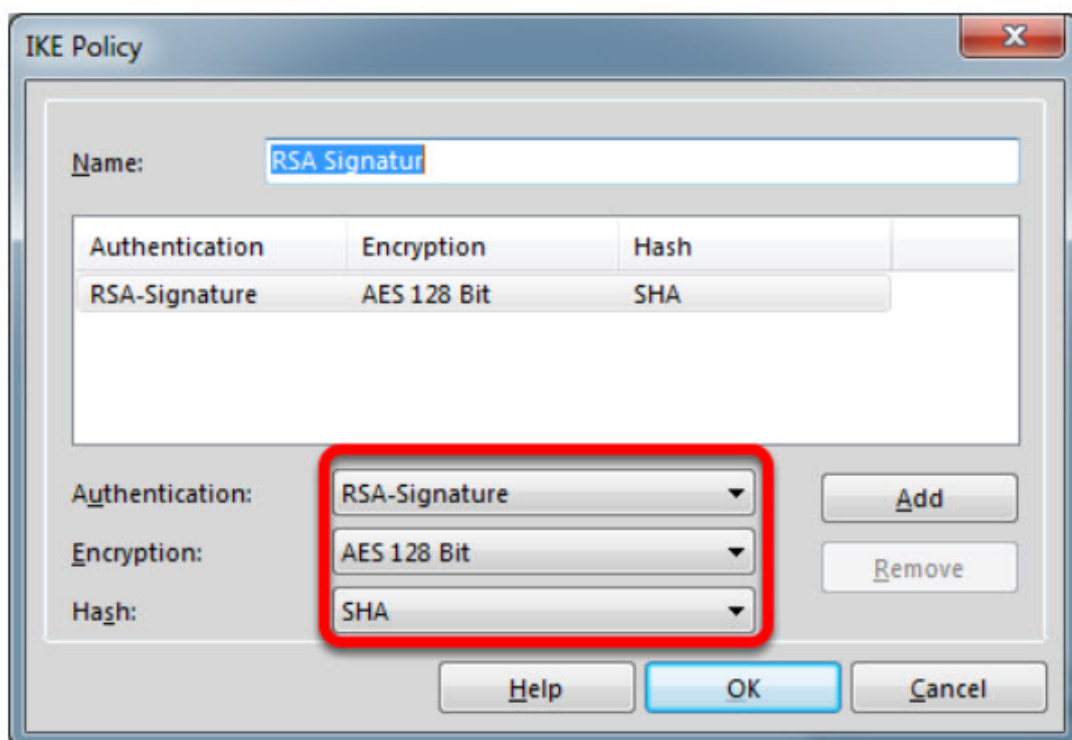
Click **Policy Editor**

IKE Policy Settings



Highlight **RSA Signature** in the IKE Policy

Click **Edit**

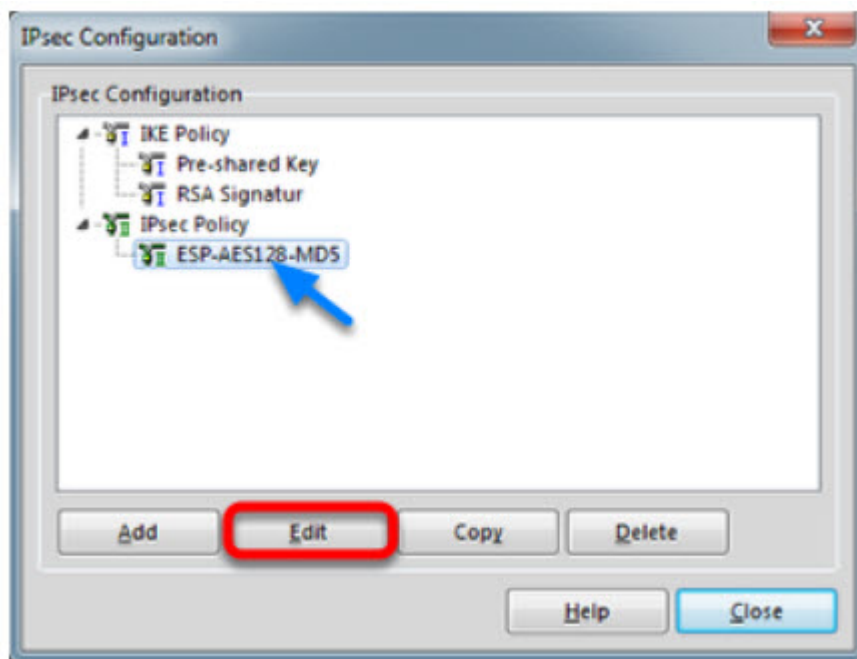


Set **Encryption** to **AES 128 Bit**.

Set **Hash** to **SHA**.

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

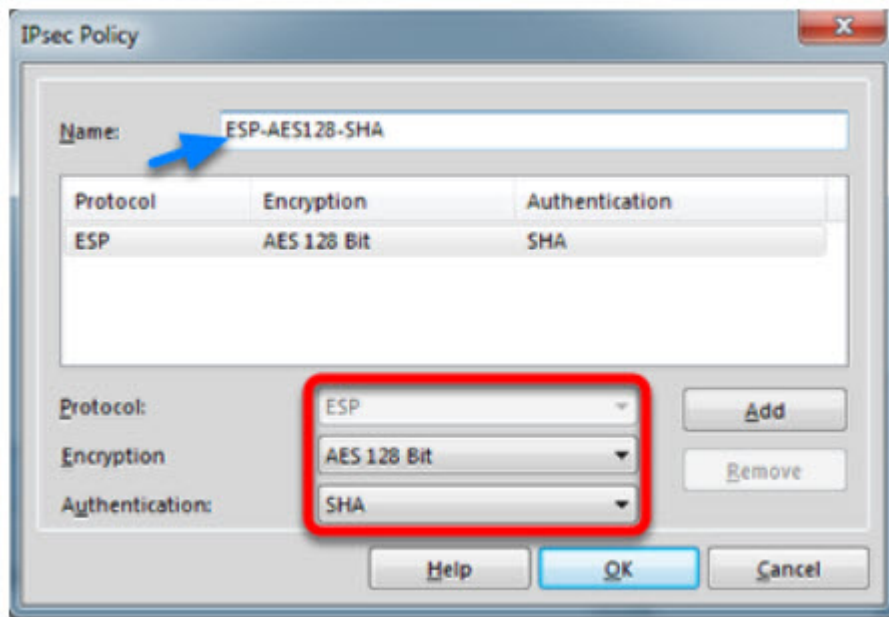
IPsec Policy Settings



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

Click **Edit**.

IPsec Policy



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

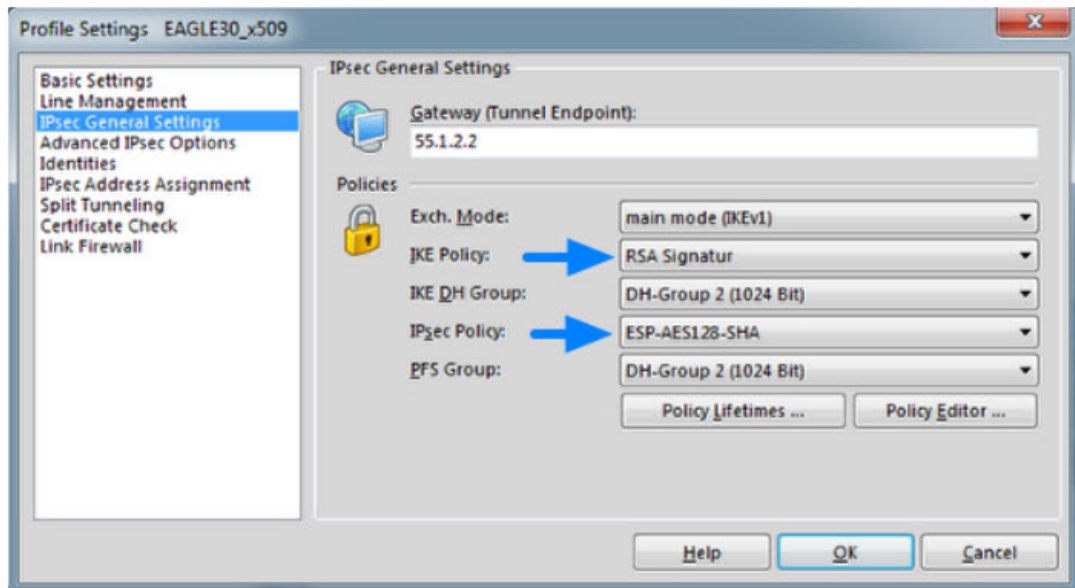
Set **Encryption** to **AES-128 Bit**.

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

Click **OK**.

Close the IPsec Configuration window.

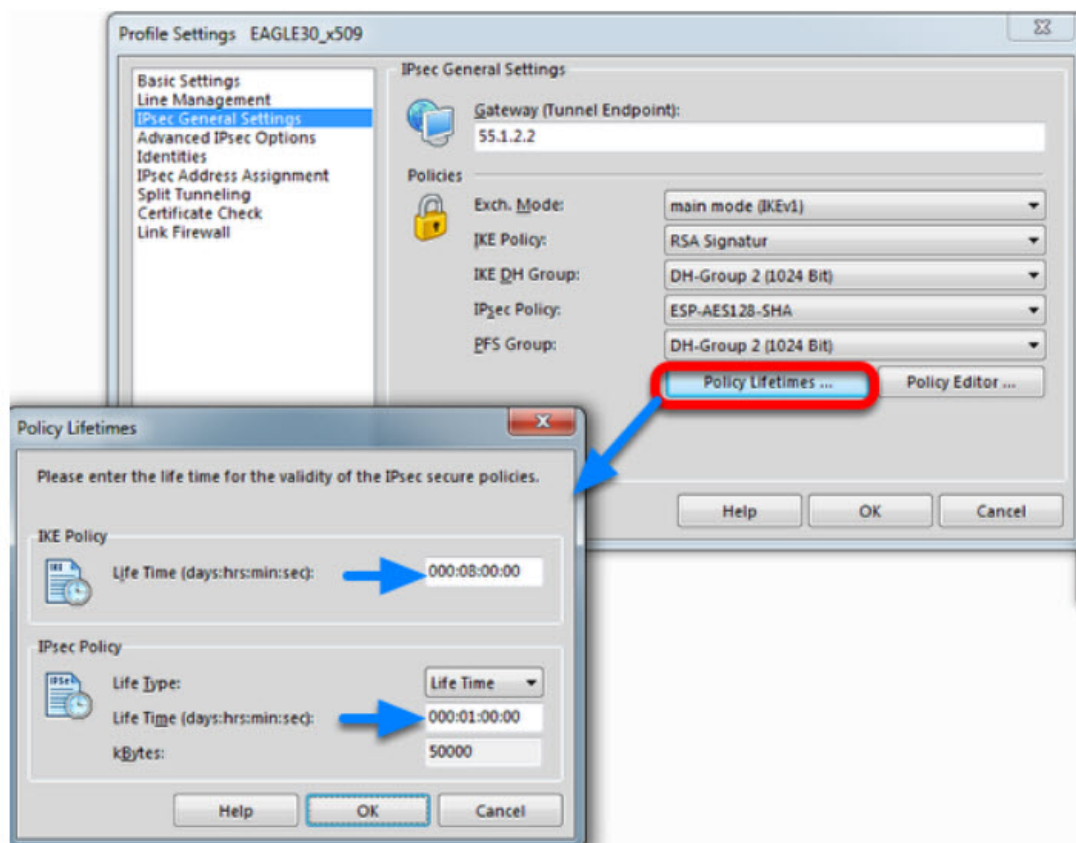
Select IKE and IPsec Policy



Set the IKE Policy to **RSA Signature**

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

Policy Lifetimes



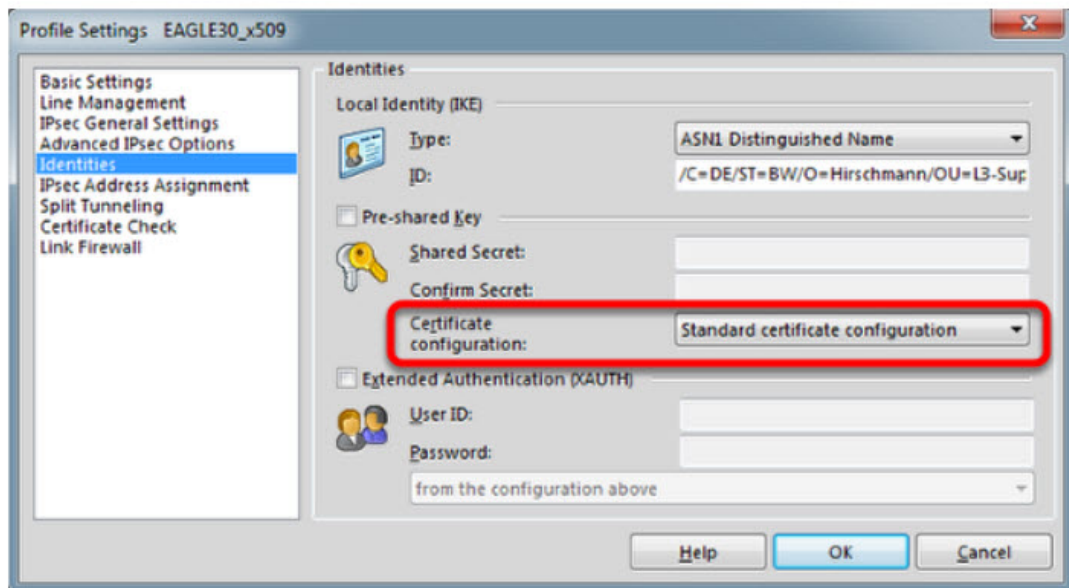
Click the button **Policy Lifetimes**.

Change the **IKE Policy Life Time** to 8 hours

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

Click **OK**.

Profile Settings - Identities



Navigate to **Identities**.

Select **Standard certificate configuration**.

Click **OK**.

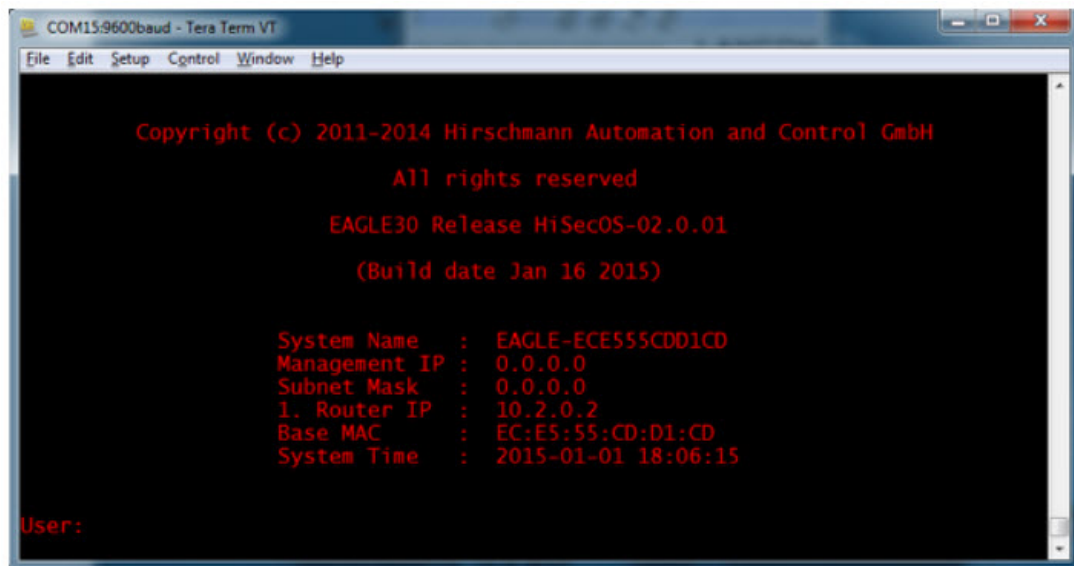
Click **Ok** to close the **Profile** Window.

LANCOM Client configured



The LANCOM Client configuration is finished

EAGLE20 Configuration



1. Set IP addresses of the router interfaces accordingly.

In our example: Int1/3 10.2.0.2/24; Int1/4: 55.1.2.2/24

2. Switch the EAGLE30 into router mode

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

```
!*(EAGLE)>enable
```

```
!*(EAGLE)#configure
```

```
!*(EAGLE)(Config)#interface 1/3
```

```
!*(EAGLE)((Interface)1/3)#ip address primary 10.2.0.2 255.255.255.0
```

```
!*(EAGLE)((Interface)1/3)#ip routing
```

```
!*(EAGLE)((Interface)1/3)#exit
```

```
!*(EAGLE)(Config)#interface 1/4
```

```
!*(EAGLE)((Interface)1/4)#ip address primary 55.1.2.2 255.255.255.0
```

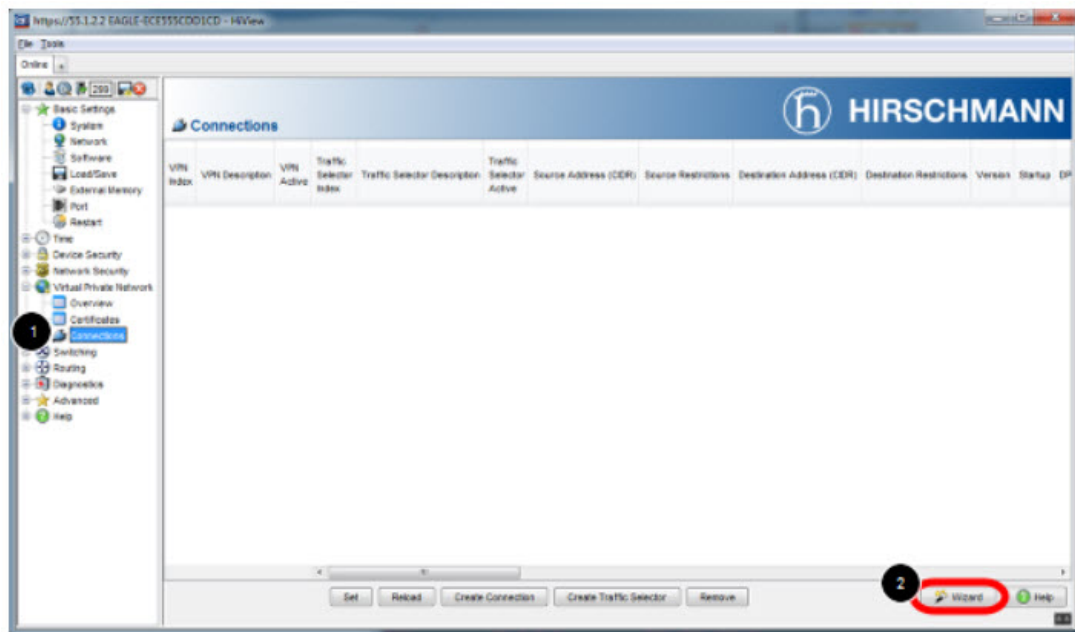
```
!*(EAGLE)((Interface)1/4)#ip routing
```

```
!*(EAGLE)((Interface)1/4)#exit
```

```
!*(EAGLE)(Config)#ip routing
```

3. Login to the webinterface of the EAGLE30 from the int1/3 (IP 10.2.0.2)

VPN Configuration Web Interface



1. Navigate in the web interface tree to **Virtual Private Network -> Connections**.

2. Open the Wizard

VPN - Basic Settings

VPN Configuration

1 Create or Select Entry
2 Authentication
3 Endpoint and Traffic Selectors
4 Advanced Configuration

VPN Index	VPN Descri...	VPN Active	Authentication Type	Startup	Operational Status	Remote Host
-----------	---------------	------------	---------------------	---------	--------------------	-------------

Create/Edit

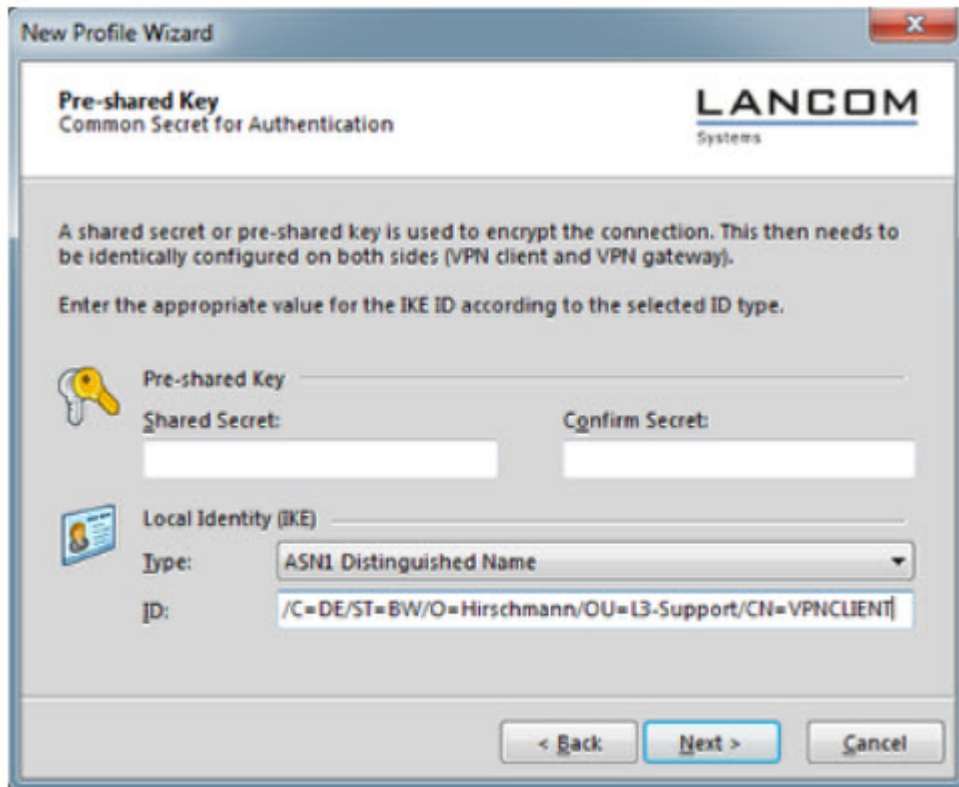
Index: 1 Description: LANCOMClient

Back Next Finish Cancel

Specify the index and description of the VPN connection.

Click Next

Upload Certificate/Key




New Profile Wizard

Pre-shared Key
Common Secret for Authentication


LANCOM
Systems

A shared secret or pre-shared key is used to encrypt the connection. This then needs to be identically configured on both sides (VPN client and VPN gateway).

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

 **Pre-shared Key** _____

Shared Secret: **Confirm Secret:**

 **Local Identity (IKE)** _____

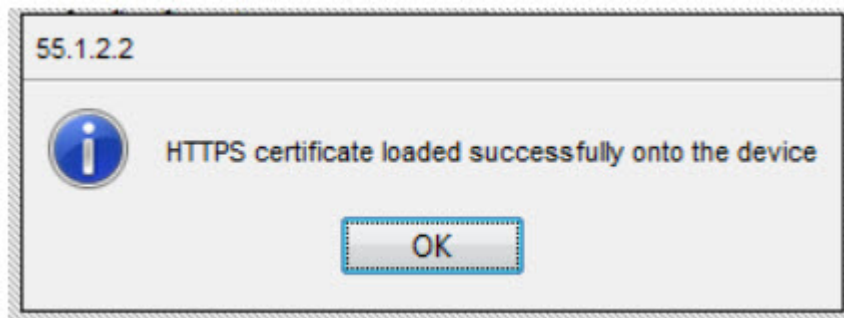
Type:

ID:

< Back Next > Cancel

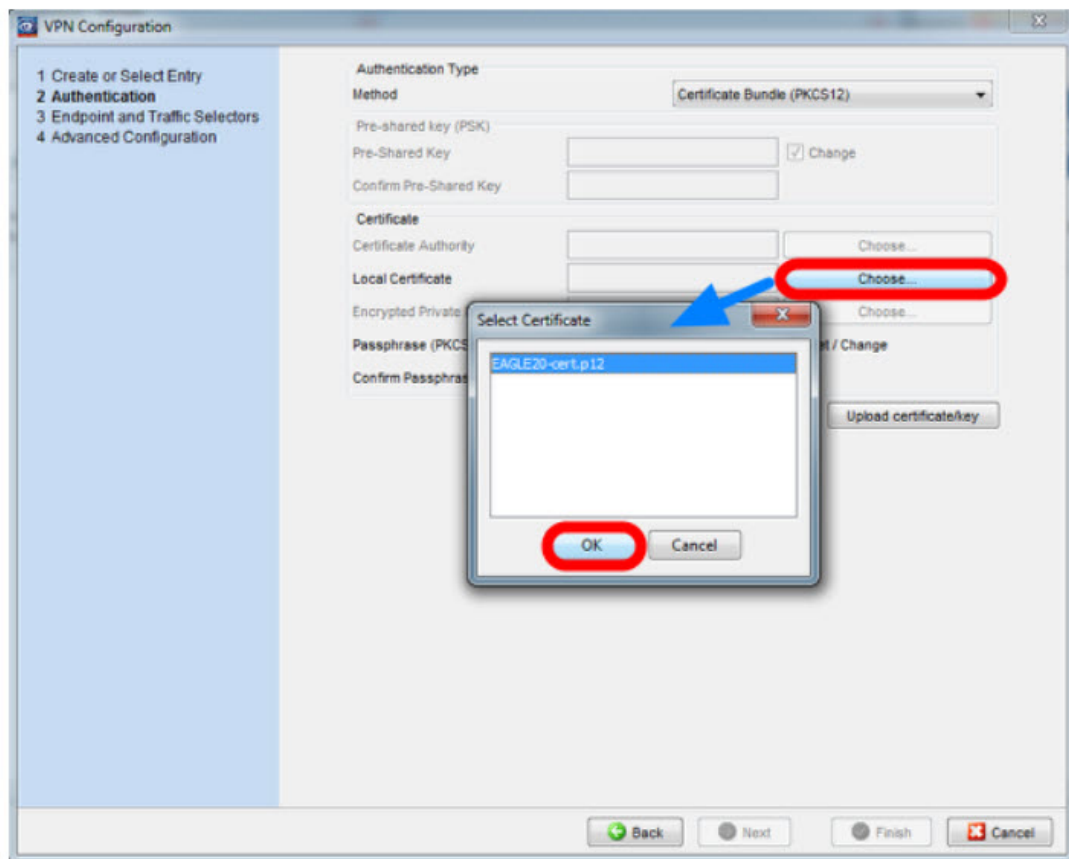
1. Select **Certificate Bundle (PKCS12)** from the Authentication Method drop-down box.
2. Click on **Upload certificate/key**
3. Specify the location of PKCS12 file and passphrase. The passphrase of the test certificate is 'vpnclient'.
4. Click OK

Upload successful



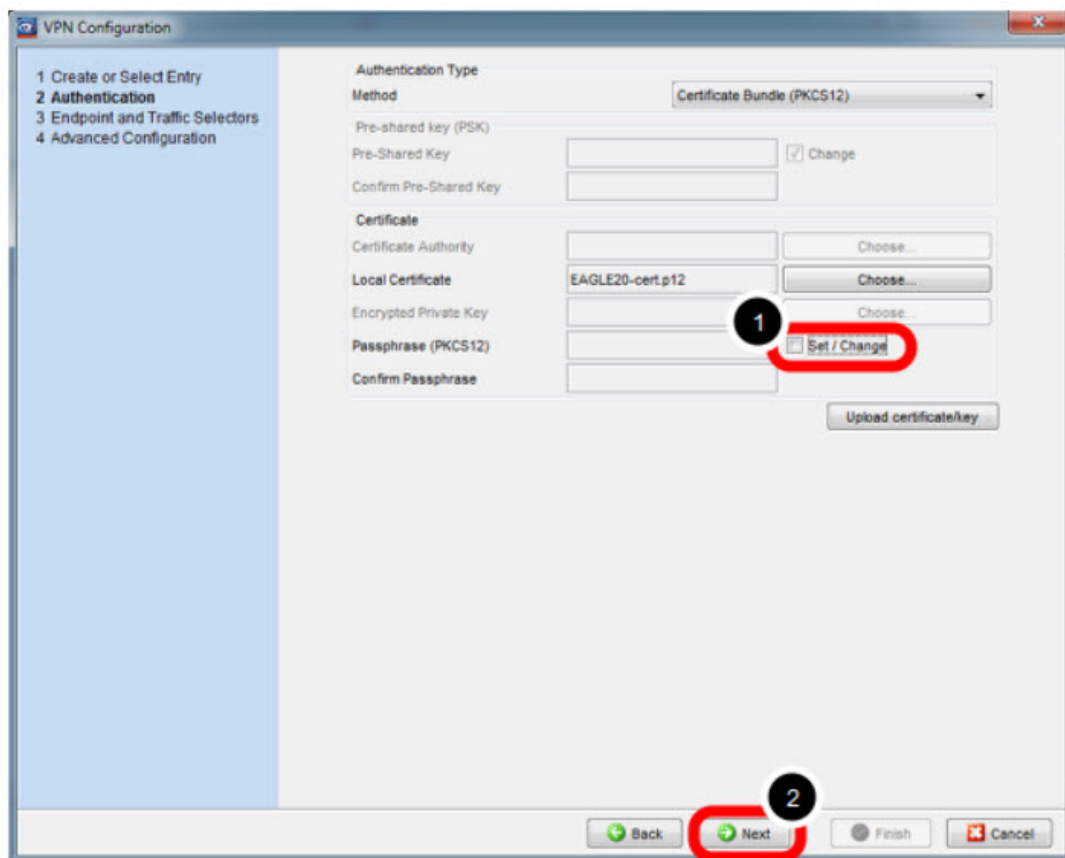
If the certificate file was uploaded successfully you see a confirmation message.
Click ok.

Select Local Certificate



Click **choose** and select the local certificate.

Uncheck Set/Change Passphrase



1. uncheck **Set/Change**

2. click **Next**

Endpoint and Traffic Selectors

VPN Configuration

1 Create or Select Entry
2 Authentication
3 **Endpoint and Traffic Selector**
4 Advanced Configuration

Endpoints
Specifies the hostname or IP address of the security gateway.

Local Gateway: 55.1.2.2
Remote Gateway: 55.1.2.143

Traffic Selectors

Index	Description	Source Address (CIDR)	Source Restrictions	Destination Address (CIDR)	Destination Restrictions
-------	-------------	-----------------------	---------------------	----------------------------	--------------------------

Add Traffic Selector

Index: 1
Description:
Source Address (CIDR): 10.2.0.0/24
Source Restrictions:
Destination Address (CIDR): 172.16.106.201/32
Destination Restrictions:
OK Cancel

Back Next Finish Cancel

1. Specify local and remote gateway addresses.

In our example

Local Gateway: 55.1.2.2

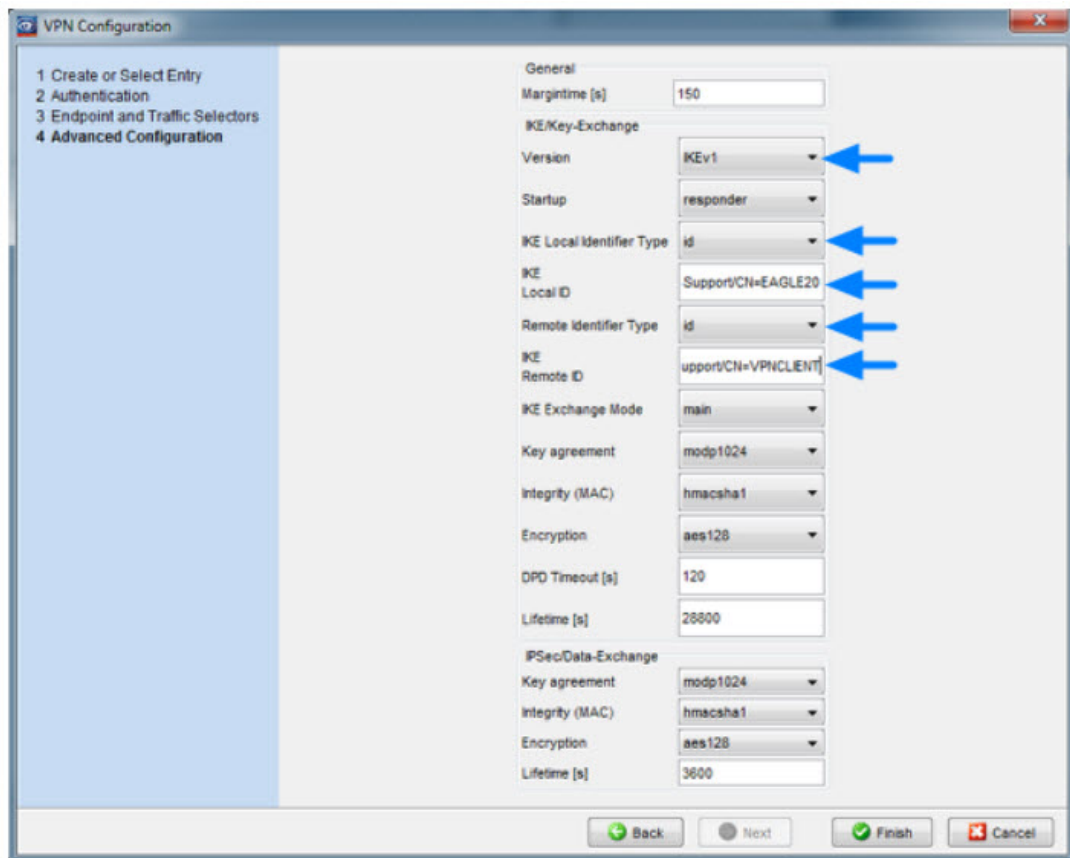
Remote Gateway 55.1.2.143

2. Add Traffic Selector with

Source Address (CIDR): 10.2.0.0/24

Destination Address (CIDR): 172.16.106.201/32 (virtual address)

Advanced Configuration



Set IKE Version 1 and specify the local and remote IDs (ASN1 DN of the certificates -see certindex.txt)

Version: **IKEv1**

IKE Local Identifier Type: **id**

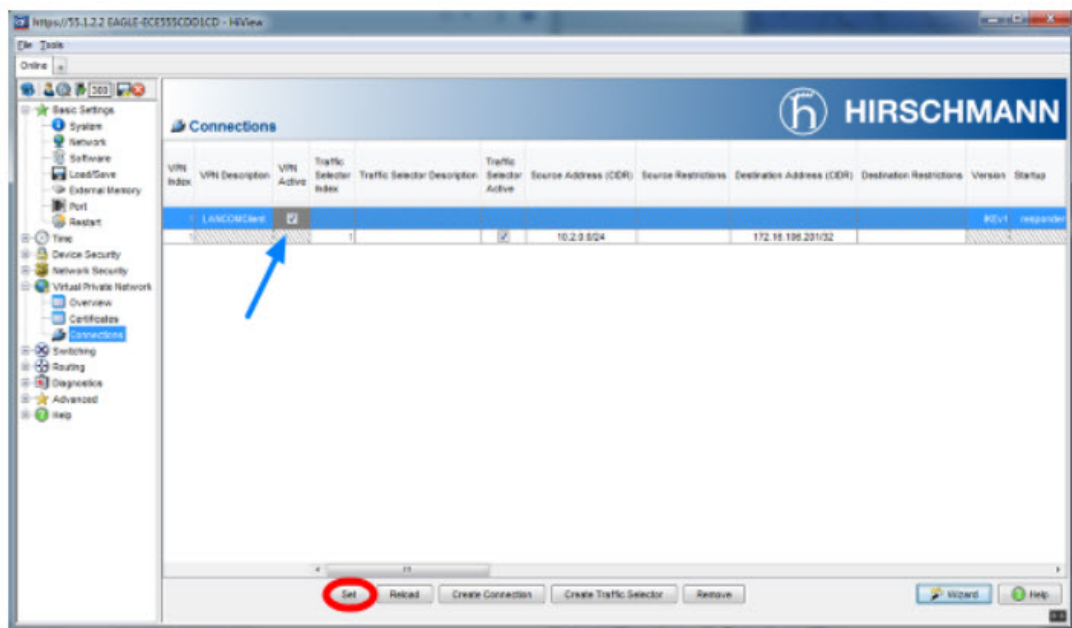
IKE Local ID: **/C=DE/ST=BW/O=Hirschmann/OU=L3-Support/CN=EAGLE20**

IKE Remote Identifier Type: **id**

IKE Remote ID: **/C=DE/ST=BW/O=Hirschmann/OU=L3-Support/CN=VPNCLIENT**

Click Finish

Activate the VPN Connection



Activate the VPN connection

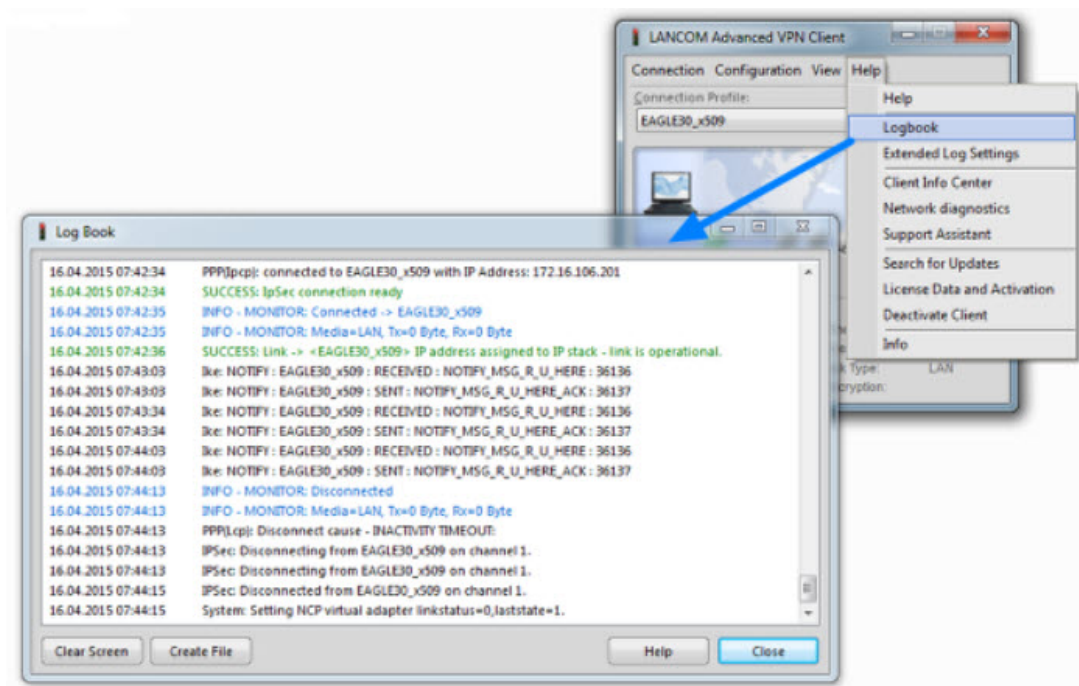
Click Set

Initialize Tunnel Setup



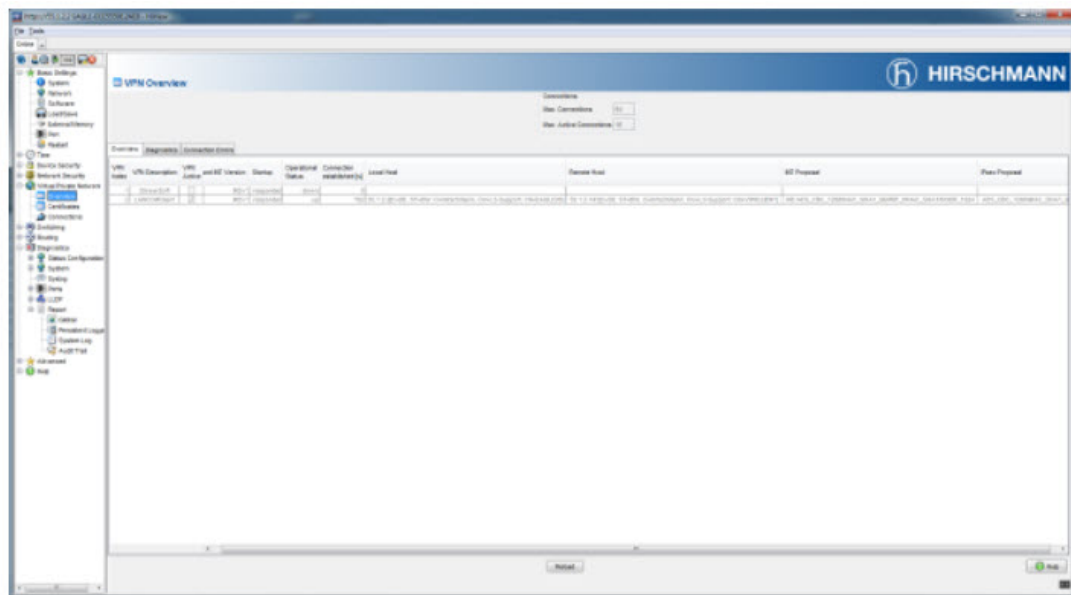
1. Move the Connection slide to the right to initialize the tunnel setup. You will get prompted to enter the certificate's pin. In our example 'test'
2. The connection should be established successfully.

LANCOM Advanced VPN Client - Log



Select Log -> Logbook

VPN Overview



In the EAGLE20/30 web interface navigate to **Virtual Private Network - Overview** to check if the VPN connection is up.

EAGLE20/30 Event Log

https://15.1.2.2 EAGLE-ECES55012AE0 - HView

Tools

Online

290

System Settings

- System
- Network
- Software
- Load/Save
- External Memory
- Port
- Reset

Time

- Device Security
- Network Security
- Virtual Private Network
- Switching
- Moving
- Diagnostics
- Status Configuration
- System
- System
- Ports
- LLDP
- Report
- Global
- Peristent Logs
- System Log**
- Audit Trail

Advanced

Help

System Log

System Information

Product	EAGLE20
Release	HISecOS-02.0.01-RC2
Hardware version	00
Serial number	837597005010101127
Firmware software release (RAM)	HISecOS-02.0.01-RC2 2015-01-16 15:39
Appld software release (RAM)	GUI-02.0.01-RC2
Firmware software release (FLASH)	HISecOS-02.0.01-RC2 2015-01-16 15:39
Appld software release (FLASH)	GUI-02.0.01-RC2
Bootcode software release (FLASH)	HISecOS-01.2.00 2014-05-21 07:22
IP address (management)	0.0.0.0
MAC address (Range 00)	EC:E5:55:01:2A:E0
System Name	EAGLE-ECES55012AE0
System Up Time	0 days 0 hrs 55 mins 15 secs
System Date and Time (local time zone)	2015-04-16 08:21:40
System operating hours	15 days 1 hrs 40 mins 42 secs
Power1	OK
Power2	DEFECTIVE
Temp	47
Configuration state (running to NVM)	OUT OF SYNC
Service shell admin status	enabled

Severity threshold for high priority buffer.....warning

```

174: Notice Apr 16 2015 08:21:12 [SIMPTRAP xmpd 0x00230014] Trap 'hm2WebLoginSuccessTrap' was sent.
(hm2WebLastLoginUserIndex=0 = admin, hm2WebLastLoginIpAddressType=0 = 1, hm2WebLastLoginIpAddress=0 = 55.1.2.143)
173: Notice Apr 16 2015 08:21:12 [USRMGR usermgr 0x0002000a] Login via web interface successful for user
'admin', role 'administrator'.
172: Notice Apr 16 2015 08:17:17 [USRMGR usermgr 0x0002000b] Logout via web interface successful for user
'admin', role 'administrator'.
171: Notice Apr 16 2015 08:17:17 [SIMPTRAP xmpd 0x00230014] Trap 'hm2WebLogoutTrap' was sent.
(hm2WebLastLogoutUserIndex=0 = admin)
170: Notice Apr 16 2015 08:11:56 [SIMPTRAP xmpd 0x00230014] Trap 'hm2WebLogoutTrap' was sent.
(hm2WebLastLogoutUserIndex=0 = admin)
169: Notice Apr 16 2015 08:11:54 [CLI cli 0x00120020] CLI: Logout via SSH successful for user 'admin', role
'Administrator' from 55.1.2.143 because of timeout exceed.
168: Notice Apr 16 2015 08:11:34 [SIMPTRAP xmpd 0x00230014] Trap 'hm2VpnUpTrap' was sent. (hm2VpnConnIndex = 2,
hm2VpnConnOperStatus = 1)

```

Reboot Search Save Delete Log File Help