

Kennisbank > Products > HiSecOS > VPN with LANCOM Advanced VPN Client

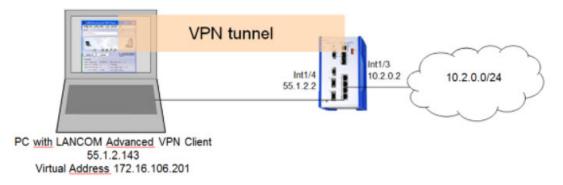
VPN with LANCOM Advanced VPN Client

- 2024-07-31 - 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

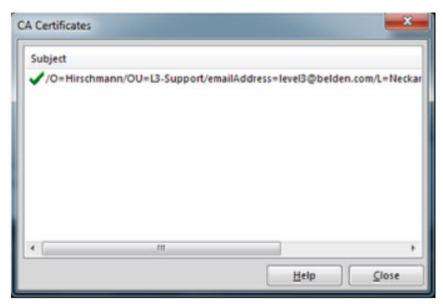
Organize • Include in library •	• Sł	are with - New folder		(EE -	- 08
	*	Name	Date modified	Туре	Size
Desktop	-	C cacert.pem	14.04.2015 15:38	PEM File	2
Documents		🥩 vpnclient-cert.p12	14.04.2015 15:47	Personal Information Exchange	4

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

	Connection Confi	guration View Help	
	Connection Profile:	<u>C</u> onnecti	ion:
ertificates	and the second second	X shed	
Certificate configuration			
Name	User Certificate	LANC	
Standard certificate configuration	PKCS#12 file	ystees	
		DC 0 sec	
	C	1 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
	Certificates	ate configuration	
	Name: Standard certific	ate configuration Certificate Renewal	
Add	Name: Standard certific User Certificate PIN Policy Certifica <u>t</u> e:	ate configuration	
Add	Name: Standard certific	ate configuration Certificate Renewal	
Add	Name: Standard certific User Certificate PIN Policy Certifica <u>t</u> e:	ate configuration Certificate Renewal	
Add	Name: Standard certific User Certificate PIN Policy Certificate: Seject Certificate:	ate configuration Certificate Renewal from PKCS=12 file 1 C:\Program Files (x86)\LANCO	
Add	Mame: Standard certific User Certificate PIN Policy Certificate: Seject Certificate: PKCS#12 Eilename:	ate configuration Certificate Renewal from PKCS=12 file 1 C:\Program Files (x86)\LANCO	
Add	Name: Standard certific User Certificate <u>PIN Policy</u> Certificate: Seject Certificate: PKCS#12 <u>Fi</u> lename: Enable Certificat	ate configuration Certificate Renewal from PKCS=12 file 1 C:\Program Files (x86)\LANCO	
Add	Name: Standard certific User Certificate PIN Policy Certificate: Seject Certificate: PKCS#12 Filename: Enable Certificat Cgrtificate Path:	ate configuration Certificate Renewal from PKCS#12 file 1 C:\Program Files (x86)\LANCO te Selection	
Add	Name: Standard certific User Certificate <u>PIN Policy</u> Certificate: Seject Certificate: PKCS#12 <u>Fi</u> lename: Enable Certificat	ate configuration Certificate Renewal from PKCS#12 file 1 C:\Program Files (x86)\LANCO te Selection	

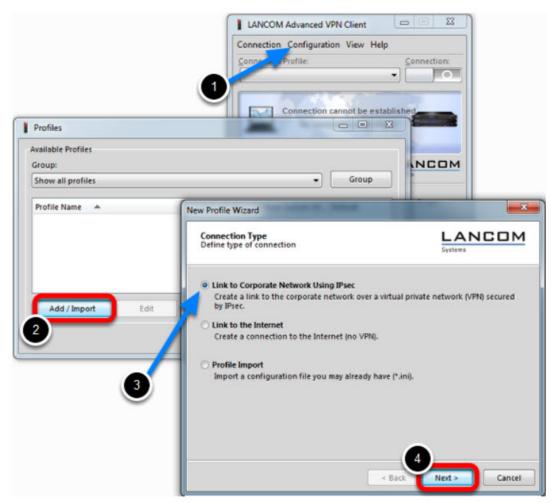
Highlight the Standard certificate configuration and click Edit.

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

ew Profile Wizard	×
Profile Name Enter the profile name of the connection	LANCOM Systems
The connection may be given a descriptive name, up characters long. Enter the name in the following fit	
EAGLE30_x509	
	Back Next > Cancel
<	Back Next > Cancel

Enter a **Profile Name** Click **Next**

Communication Medium

w Profile Wizard	×
Communication Medium Select the media type of the connect	ttion.
	he corporate network should be established. If the et the communication media to "modem" and then
Communication Media:	LAN (over IP)
	< Back Next > Cancel

Select LAN (over IP) as communication media Click Next

VPN Gateway Parameters

New Profil	le Wizard		×
VPN G To whi establi	ateway Parameters ch VPN gateway should the connec shed?	tion be	м
212.10 Using auther			the
88	55.1.2.2 Extended Authentication @AU User ID:	TH)	
	Password:	Password (confirm):	
		< Back Next > Car	ncel

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

IPsec Configuration

	le Wizard	
IPsec Config	Configuration gure the basic IPsec parameters	LANCOM Systems
"auton In the	sic IPsec parameters can be specified here. Th natic mode" which are pre-defined (default) p event that uniquely defined IKE- / IPsec polici of and assigned using the policy editor under Exchange Mode:	roposals. es are to be used, these can then be
1	main mode (IKEv1)	•
	main mode (IKEv1) PFS Group:	•
		•
	PFS Group:	

Set the Exchange Mode to main mode (IKEv1) Set PFS Group to DH-Group 2 (1024 Bit) Click Next

Local Identity (IKE)

lew Profil	e Wizard		×
	ared Key on Secret fo	r Authentication	LANCOM Systems
be ider	ntically conf	igured on both sides ate value for the IKE I d Key	d to encrypt the connection. This then needs to (VPN client and VPN gateway). D according to the selected ID type. Confirm Secret:
	Local Iden	ntity (IKE)	
0	Type:	ASN1 Distinguis	hed Name 🔹
	ID:	/C=DE/ST=BW/C	=Hirschmann/OU=L3-Support/CN=VPNCLIENT
			< <u>Back</u> Next > Sancel

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

w Profi	e Wizard	
	Configuration - IP Addresses ing the IP address to the client	LANCOM Systems
the di	ent's IP address is dynamically as	oing to use. By selecting "Use IKE Config Mode" signed by the VPN gateway. VINS servers (if used) can be found.
ADK	Manual IP Address	•
	IP Address:	
	172.16.105.201	
e	DNS / WINS Servers	
U	DNS Server:	WINS Server:
	0.0.0.0	0.0.0.0

Set the IP Address Assignment to Manual IP Address.

IPsec Configuration - Split Tunneling

nfiguration - Split Tunneling he remote IP networks to be reached the IPsec tunnel.	
e remote IP networks the tunnel should be ys be used.	used for. Without entries tunneling
Remote Networks Remote IP	Net Masks
IP Network	Delete
2 IP Network: <u>Net N</u> 10.2.0.0 - 255.2	lask: 155.255.0
З	Cancel
	Back Einish Cance

Define the remote IP network to be reached through the IPsec tunnel. In our example 10.2.0.0/24. Click Finish.

Profile Window

how all profiles		•	Group
Profile Name 🔺	Communication	Medium Default	
AGLE30_x509	LAN		

The new profile is created and displayed in the **Profile** window Highlight the profile and click **Edit.**

Profile Settings

Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identities	IPsec General Settings	ndpoint):	
IPsec Address Assignment Spiti Tunneling Certificate Check Link Firewall	Policies Exch. <u>M</u> ode: [KE Policy: IKE <u>D</u> H Group: IP <u>s</u> ec Policy: <u>P</u> FS Group:	main mode (IKEv1) automatic mode DH-Group 2 (1024 Bit) automatic mode DH-Group 2 (1024 Bit) Policy Lifetimes	۲ ۲ ۲ ۲ Policy <u>E</u> ditor
		Help	<u>C</u> ancel

Highlight IPsec General Settings in the left pane.

Click Policy Editor

IKE Policy Settings

IPsec Configuration	
ST IKE Policy ST Pre-shared Key ST RSA Signatur ST IPsec Policy ST ESP-AES128-MD5	
	Copy Delete
Add Edit	Cobl

Highlight **RSA Signature** in the IKE Policy

Click **Edit**

	A Signatur		
Authentication	Encryption	Hash	
RSA-Signature	AES 128 Bit	SHA	
uthentication:	RSA-Signature		Add
uthentication:	RSA-Signature AES 128 Bit		<u>A</u> dd

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

sec Configuration	1		x
- 3T IKE Policy 3T Pre-sh 3T RSA S - 3T IPsec Polic 3T ESP-A	ared Key gnatur Y		
Add	Edit	Copy Delete	
		Help	Close

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

IPSec Policy

lame:	ESP-AES128-SHA	
Protocol	Encryption	Authentication
ESP	AES 128 Bit	SHA
Lar		
rotocol:	ESP	- Add
	_	- <u>A</u> dd - <u>R</u> emove

Change the Name to ESP-AES128-SHA.

Set Encryption to AES-128 Bit.

Set Authentication to SHA.

Click OK.

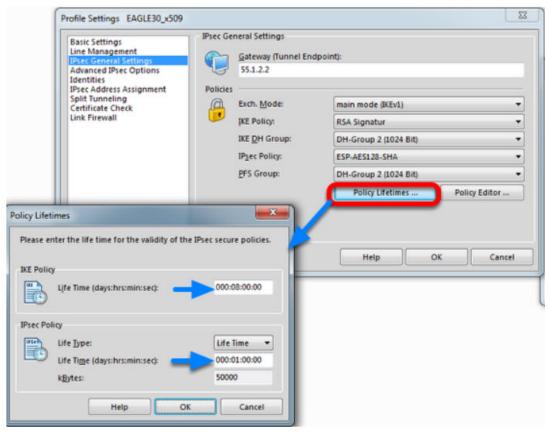
 $\label{eq:close} \textbf{Close} \text{ the IPsec Configuration window.}$

Select IKE and IPsec Policy

Basic Settings Line Management IPsec General Settings Advanced IPsec Options Identities IPsec Address Assignment Split Tunneling Certificate Check Link Firewall	IPsec General Settings <u>Gateway</u> (Tunnel En 55.1.2.2	idpoint):	
	Policies Exch. Mode: JKE Policy: IKE DH Group: IPSec Policy: PFS Group:	main mode (IKEv1) RSA Signatur DH-Group 2 (1024 Bit) ESP-AES128-SHA DH-Group 2 (1024 Bit)	
		Policy Lifetimes	Policy <u>E</u> ditor

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

Basic Settings Line Management Psec General Settings	Local Identity (IKE)	
Psec General Settings Advanced IPsec Options	Type:	ASN1 Distinguished Name 👻
Identities IPsec Address Assignment	ID:	/C=DE/ST=BW/O=Hirschmann/OU=L3-Sup
Split Tunneling Certificate Check Link Firewall	Pre-shared Key	
	Shared Secret:	
	Confirm Secret:	
	Certificate configuration:	Standard certificate configuration 👻
	Extended Authentication	(XAUTH)
	OD User ID:	
	Password:	
	from the configur	ation above 👻

Navigate to Identities.

Select Standard certificate configuration.

Click **OK.**

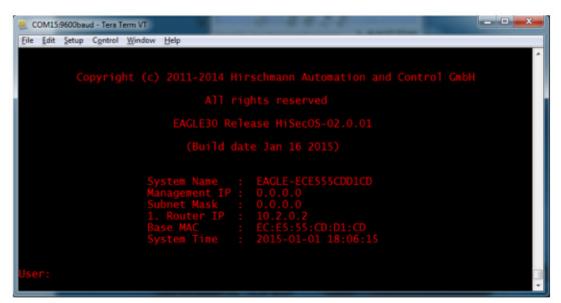
Click **Ok** to close the **Profile** Window.

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

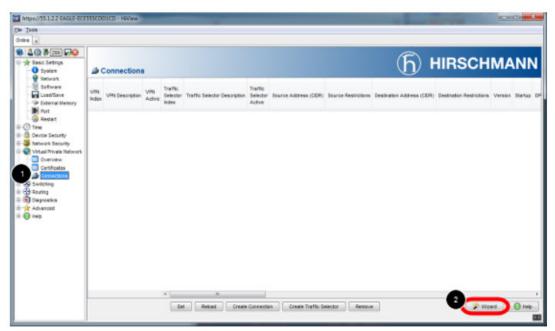
!*(EAGLE)((Interface)1/4)#ip routing

!*(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

1 Create or Select Entry 2 Authentication	VPN Index	VPN Descri	VPN Active	Authentication Type	Startup	Operational Status	Remote Host
2 Authentication 3 Endpoint and Traffic Selectors 4 Advanced Configuration	BINDER .		ALITE	1394		Contra	
	Create/Edit Index 1		LANCOMClient				

Specify the index and description of the VPN connection. Click Next

Upload Certificate/Key

Pre-sh	e Wizard ared Key on Secret fo	r Authentication		
be iden	tically conf	igured on both sides (ate value for the IKE ID d Key	to encrypt the connect /PN client and VPN gate according to the select C <u>o</u> nfirm Sec	ted ID type.
8	Local Ider Type: [D:	ASN1 Distinguish		upport/CN=VPNCLIENT
			< 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

Create or Select Entry Authentication	Authentication Type Method	Certificate Bundle (PKCS12)
Endpoint and Traffic Selectors Advanced Configuration	Pre-shared key (PSK) Pre-Shared Key Confirm Pre-Shared Key Certificate Certificate Certificate Authority	Choose
	Local Certificate Encrypted Private Passphrase (PKCS Confirm Passphras	Choose Choose
		K Cancel

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

Uncheck Set/Change Passphrase

1 Create or Select Entry 2 Authentication	Authentication Type Method	Certificate	Bundle (PKCS12)
Endpoint and Traffic Selectors Advanced Configuration	Pre-shared key (PSK) Pre-Shared Key Confirm Pre-Shared Key		📝 Change
	Certificate Certificate Authority		Choose
	Local Certificate	EAGLE20-cert.p12	Choose
	Encrypted Private Key		Choose
	Passphrase (PKCS12) Confirm Passphrase		Set / Change
			Upload certificate/key
			2

- 1. uncheck Set/Change
- 2. click **Next**

Endpoint and Traffic Selectors

Create or Select Entry Authentication Endpoint and Traffic Selector:	Endpoints Specifies the hostname or IP address of the security	Endpoints Specifies the hostname or IP address of the security gateway.				
Advanced Configuration	Local Gateway	55.1.2.2				
	Remote Gateway	55.1.2.143				
	Traffic Selectors					
	Index Description Source Address (CDR) Sou	urce Restrictions Destination Address (CIDR) Destination Res				
Add Traffic Selector						
Add Traffic Selecto						
Index	1					
Description						
Source Address (0						
Source Restrictions						
Destination Addres						
Destnation Restrict						
	OK Cancel					
<u></u>						

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

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

Advanced Configuration

Create or Select Entry	General		
2 Authentication 3 Endpoint and Traffic Selectors	Margintime (s)	150	
Advanced Configuration	IKE/Key-Exchange	,	
	Version	KEv1	
	Startup	responder	•
	IKE Local Identifier Type	id	•
	KE Local D	Support/CN=EAG	
	Remote Identifier Type	id	
	IKE Remote ID	upport/CN=VPNCL	ем] 🗲
	IKE Exchange Mode	main	•
	Key agreement	modp1024	
	integrity (MAC)	hmacsha1	•
	Encryption	acs128	•
	DPD Timeout [s]	120	
	Lifetime [s]	28800	
	PSec/Data-Exchange		
	Key agreement	modp1024	•
	Integrity (MAC)	hmacsha1	•
	Encryption	aes128	•
	Lifetime [s]	3600	

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

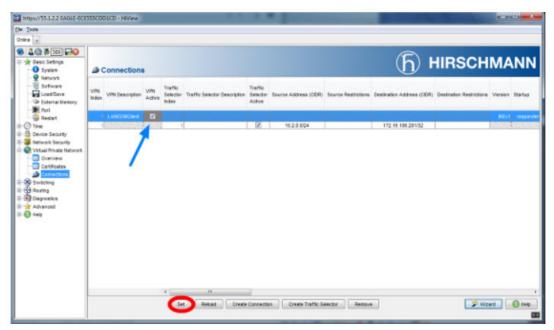
IKE Local ID: /C=DE/ST=BW/O=Hirschmann/OU=L3-Support/CN=EAGLE20

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

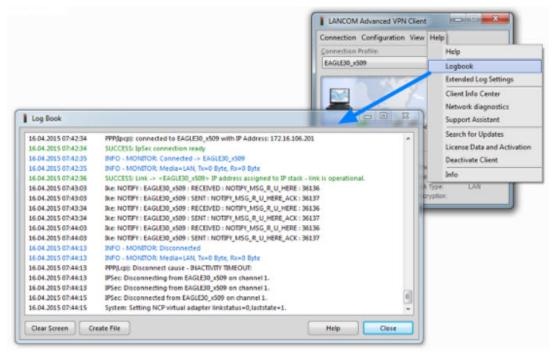


1. Move the Connection slide to the right to initialize the tunnel setup.

You will get prompted to enter the certificate's pin. In our example 'test'

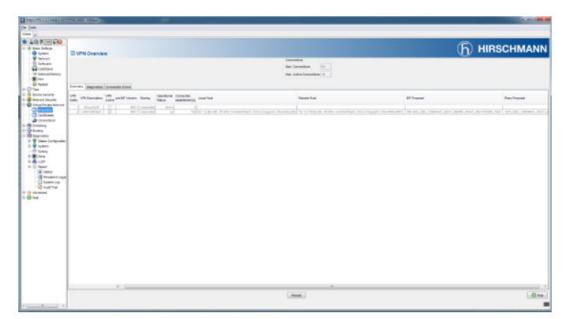
2. The connection should be established successfully.

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

8		
Q # 299 😡 Q		
Basic Settings		(ĥ) HIRSCHMAN
3 System	System Log	
P Network		
Software	System Log	
Codd/Save	System Log	
Port .		
Restat	Contraction of the Analysis of the second	
ime	System Information	
evice Security	Product	EAGLE20
Intwork Security Intual Private Network	Release	HI8ec08-02.0.01-RC2
Artual Private Network	Handware version Serial number	00 837597035010101127
lauting	Firmware software release (R/M)	837597035010101127 Hi8ec08-02.0.01-RC2.2015-01-16.15.30
Nagroatica	Applet software release (RAM)	GU-02.0.01-RC2
Status Configuration		HISec08-02.0.01-RC2 2015-01-16 15:39
2 System	Applet software release (FLASH)	GUI-02.0.01-RC2
0 Syslog	Bootcode software release (FLASH)	HE005-01.2.00 2014-05-23 07:22
Ports LLDP	IP address (management)	0.0.0
Report	MAC address (Range: 80) System Name	EC E5:55:01 2AE0 EAGLE ECE555012AE0
Chest	System Up Time	0 days 0 http 50 mints 15 aecs
Persistent Loggi		2015-04-16-08-21-40
System Lop	Bystem operating hours	15 days 1 hrs 40 mma 42 secs
- 😳 Audt Trail	Power1	OK .
dvanced	Power2	DEFECTIVE
ep	Temp	47
	Configuration state (running to NVM) Service shell admin status	OUT OF BINC enabled
	Severity threshold for high priority buffer	warring
	county on one of the bound on one	
	174: Notice Apr 16 201	5 08:21:12 [SIMPTRAP snmpd 0x00230014] Trap 'hm2NebloginSuccessTrap' was sent.
	(hm2NebLastloginUserName.0 = adm	in, hn3WebLastLoginInetAddressType.0 = 1, hn3WebLastLoginInetAddress.0 = 55.1.2.143)
	173: Notice Apr 16 201	5 08:21:12 [USHOADA usermgs 0w00022003a] Login via web interface successful for user
	'admin', role 'administrator'.	
		5 00:17:17 [USRADB usermgr 0x00022005b] Logout via web interface successful for user
	'admin', role 'administrator'.	
		5 08:17:17 [SHNPTRAP snmpd 0x00230014] Trap 'hm2NebLogoutTrap' was sent.
	(hm2WebLastLopoutUserName.0 = ad	
		5 08:11:56 [SHMETEAR sampd 0w00230014] Trap 'hm2SshLogoutTrap' was sent.
	(hm25shlastlogcutUserName.0 = ad	
	169: Notice Apr 16 201 "Administrator" from 55.1.2.143	5 00:11:56 [CLI cli Gw00120020] CLI: Legout via 80H successful for user 'admin', role
		because of timeout exceed. 5 08:11:34 [SHMPTRAP snmpd 0x00230014] Trap 'hm2VpnUpTrap' was sent. (hm2VpnConnIndex = 2,
	ha2VpnConnOperStatus = 1)	s nerrire foundations supply experienced risk unschendingly was send. (unschurouringes = 1)
	and the second sec	Relaat Search Save Deate Log Fie