

NCP Secure Entry Client

Administration Guide

© NCP engineering GmbH 2023

Version 4.70 macOS



Next Generation Network
Access Technology

www.ncp-e.com

Contact

For more information or questions about NCP products and services:

Germany

NCP engineering GmbH

Dombühlerstraße 2

D-90449 Nürnberg

Tel.: +49 (911) 9968 0

Homepage: <http://www.ncp-e.com>

Mail: info@ncp-e.com

E-Mail Support:

support@ncp-e.com (german)

helpdesk@ncp-e.com (english)

Support Hotline:

0900 / 1 99 68 00

(only available from Germany, 80 Cent / per minute)

Our support times are from monday to friday from 08:00 am to 17:00 pm.

Contact USA, North American HQ

NCP engineering, Inc.

19321 US Highway 19 N, Suite 401

Clearwater, FL 33764

Phone: +1 (650) 316-6273

For a support request we need the following information:

- exact product name
- serial number
- version number
- precise description of the problem
- any error message(s)

NCP Secure Entry Client

While considerable care has been taken in the preparation and publication of this manual, errors in content, typo-graphical or otherwise, may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP. NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or suitability of use for any particular purpose.

Furthermore, NCP reserves the right to revise this publication and to make amendments to the contents, at any time, without obligation to notify any person or entity of such revisions or changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH. All trademarks or registered trademarks appearing in this manual belong to their respective owners.

Table of contents

Online Help	8
Product Description	9
Configuration Tips	10
Creating Profiles	10
Connection Setup	12
FIPS Certification	13
Customizing the GUI	13
Certificate Configuration	14
Configuration Parameters	15
Settings	19
Certificates [Configuration]	20
User Certificate [Configuration]	21
PIN Policy	21
Certificate Renewal	22
Computer Certificate	22
IPsec	23
IKEv1 Policy [IPsec Configuration]	25
Name [IKE Policy]	26
Authentication [IKE Policy]	26
Encryption [IKE Policy]	26
Hash [IKE Policy]	26
IKEv2 Policy [IPsec Configuration]	27
Name [IKEv2 Policy]	27
Encryption [IKEv2 Policy]	27
Pseudorandom Function [IKEv2 Policy]	27
Integrity Algorithm [IKEv2 Policy]	28
IPsec Policy [Profiles]	29
Name [IPsec Policy]	30
Protocol [IPsec Policy]	30
Transform / Encryption	30
Authentication [IPsec Policy]	30
Proxy for SSL VPN (NCP VPN Path Finder)	31

EAP Options [Configuration]	32
Profiles [Parameters]	33
Basic Settings [Profiles]	35
Profile Name	36
Line Management [Profiles]	37
Connection Mode [Line Management]	38
Inactivity Timeout [Line Management]	39
Prioritize Voice over IP	39
Disconnect the logical VPN tunnel when the connection is broken	40
IPsec [Profile]	40
Gateway (Tunnel Endpoint)	41
IPsec Policy [Selection]	41
Exchange Mode [Profiles]	42
Tunnel IP Version	44
Policy Lifetimes	44
Life Time Type [Policy]	44
Life Time [Security]	45
Volume [Policy]	45
PFS / DH Group	45
Advanced IPsec Options	46
IPsec Compression	46
Disable DPD (Dead Peer Detection)	46
SSL VPN (NCP VPN Path Finder)	46
Identities	48
Type [Identities]	49
IKE ID [Profiles]	49
IPsec Pre-shared Key [VPN Tunneling]	49
Certificate Configuration [Profiles]	50
Extended Authentication (XAUTH)	50
IPsec Address Assignment	51
Assignment of the Private IP Address	51
DNS Server	52
Domain Name	52
Split Tunneling / Remote Network	55
Remote IP Networks (IPv4)	55
Full Local Network Enclosure Mode	55
Remote IP Networks (IPv6)	56
Certificate Check	57

Incoming Certificate's Subject	57
Incoming Certificate's Issuer	59
Issuer's Certificate Fingerprint	60
SHA1 Fingerprint	60
Extended Authentication [Pre-authentication]	61
IKEv1 / IKEv2	61
IKEv1 Policy	62
IKEv2 Policy	62
Life Time [Policy]	62
IKE DH Group [IKE Policy]	63
IKE ID Type [Profiles]	64
IKE ID [Profiles]	64
View	65
Show Profiles	65
Show Statistics	65
Connect / Disconnect	66
Connection Info	67
Certificates [View]	68
View Issuer Certificate	69
View User Certificate	71
View Incoming Certificate	73
View CA Certificates	76
Hardware Certificate (View)	78
Enter PIN	80
Reset PIN	80
Change PIN	81
Configuration Locks	81
Unlock Locks	82
Exit	83
Logbook	84

Online Help

The structure of the Online Help for

Settings: Global settings can be defined that are applicable to all VPN connections:

- for the use of [Certificates](#) ^[14]
- for the use of [IPsec Settings](#) ^[23]
- for the use of the [SSL VPN \(NCP VPN Path Finder\)](#) ^[46]
- for the use of [EAP](#) ^[32]

Profiles: The configuration data for each specific VPN connection, and especially the access data for that particular VPN gateway, is stored in a [profile](#) ^[10]. By selecting a profile from the pulldown menu in the Client Monitor, a connection to the corresponding destination gateway is established. New profiles can be created manually via this menu item or with the help of an assistant.

Connection

A VPN [connection](#) ^[12] can be manually established or disconnected using this menu. Using this menu item the [certificate](#) ^[68] to be used can be displayed and the PIN entered, reset or changed. If [parameter locks](#) ^[82] have been configured by central management, these can be deactivated using the connection menu, subject to central management's approval by them having issued the corresponding username and password previously configured for this specific client.

View

The appearance of the GUI can be altered using the [View](#) ^[13] menu. For example, statistics or the profile selection pulldown menu can be displayed or blanked out.

Log

The [Log](#) ^[84] feature logs all communication processes of the Client Software. This menu allows you to view the current log file or create a log book.

Help

The menu [Help / NCP Secure Entry Client](#) ^[10] offers you configuration tips.

For each of the submenus of the client, a separate help chapter with index and possibly a configuration tip has been created. These two help pages take you to the functional descriptions of the individual parameters. The corresponding function descriptions are also opened if you press the help button in the respective configuration field of the profile settings on the monitor.

Tips for a quick start with the client

[Setting up a VPN profile for connection to the corporate network](#) ^[10]

[Setting up a VPN connection](#) ^[12]

[Using a certificate](#) ^[14]

[FIPS Certification](#)  13

[Modifying the clients GUI](#)  13

Overview:

[All configuration areas and their parameter](#)  15

Product Description

The *NCP Secure Entry Client* may be used in any VPN environment. It uses communication protocols based on the IPsec standards to communicate with the VPN gateways of various manufacturers and it is the alternative to the IPsec Client technology available on the market.

In order to establish a connection to the VPN gateway, the client software uses the default Internet connection which must have been configured beforehand.

Further features simplify access to the holistic remote access VPN solution:

- * Compatibility with almost all common VPN gateways on the market
- * Extended authentication (XAUTH) support for authentication via USER ID / password and/or OTP
- * Internet Key Exchange Config Mode (IKE CFG) for dynamic assignment of IP address, DNS server and domain name
- * Dead Peer Detection (DPD) - configurable handling of tunnel failure; user configurable timeouts for detection of a broken connection to the peer, designed to provide flexible control over re-establishment of the VPN tunnel,
- * Network Address Translation-Traversal (NAT-T) for communication between client and gateway via network components which perform NAT
- * Use of digital certificates in a public key infrastructure (PKI), and
- * Graphical user interface.

Client Monitor - graphical user interface

The graphical user interface of the Client gives the user a clear view of the system. It informs the user whether the computer is online, how long it has been online, the current data throughput and to which destination address a secure connection has been established.

PKI Support

Security of access to the computer and through that to the corporate network can be improved by using soft certificates (PKCS#12) or the PKCS#11 interface. In order to achieve this, features are incorporated which enable the Client to be integrated into a PKI (Public Key Infrastructure).

Support of High Availability Services

The client is able to use failsafe and load balancing servers to ensure both on-going system availability for non-stop VPN operations as well as an equally distributed and efficient use of available VPN system resources.

Central Management


The Client can be administrated by the NCP Secure Enterprise Management (SEM). The NCP SEM is the central administration tool for the whole VPN.

FIPS Certification

The IPsec Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747).

FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection:

- Diffie Hellman Group: Group 2 or higher (DH starting from a length of 1024 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 and 256 Bit or Triple DES

The respective modules can be configured in the [IPsec Settings](#) .

Configuration Tips

The configuration tips describe the most important and most widely used configurations and serve as examples for them. They cover the following topics:

[Setting up a VPN profile for connection to the corporate network](#)  10

[Setting up a VPN connection](#)  12

[Using a certificate](#)  14

[FIPS Certification](#)  13

[Modifying the clients GUI](#)  13

[Overview of the configuration areas and its parameter](#)  23

Creating Profiles

The configuration tips describe the most important and most widely used configurations and serve as examples for them. They cover the following topics:

[Setting up a VPN connection](#)  12

[Using a certificate](#)  14

[FIPS Certification](#)  13

[Modifying the clients GUI](#) ^[13]

A wizard helps you to configure various profiles at your client. For connection setup, you can comfortably select these profiles from the [profile selection](#) ^[65].

Configure profiles using the wizard

Select "Profiles" in the menu of the client's GUI and open the wizard for a new profile by clicking on [add].

Then you enter a freely assigned name for the new profile.

The "VPN gateway parameter" and the "IPsec configuration" have to meet the presets of the administrator of the IPsec gateway. You receive the relevant data from your administrator.

Manually configuring and changing profiles

You can also enter or change data at a later point in time after the profile has been saved once.

You find a description of most important parameter below this text. The words in square brackets behind the parameters display where to find them in the profile settings.

[Gateway \(Tunnel Endpoint\)](#) ^[41]

[Extended Authentication](#) ^[50]

[Advanced IPsec Options](#) ^[50] with SSL VPN (NCP VPN Path Finder)

[IPsec-Settings](#) ^[23] according to Policies

[IP Address Assignment](#) ^[51] [IPsec Address Assignment](#) ^[51],

[DNS Server](#) ^[52]

Save the new [VPN profile](#) ^[33]. If you configured various different profiles, you can organize them in [groups](#) ^[33] and display them according to different criteria.

Add / Import

Click on this button to start a wizard which helps you to either configure a new profile or import an existing profile.

The client supports different types of import files (*.ini).

Extended Authentication (XAUTH) with Certificate

If you wish to use a certificate for extended authentication instead of user ID and password, you have to carry out a [certificate configuration](#) ^[14]. Select [Settings](#) ^[19] and [Certificates](#) ^[20] in the menu item *NCP Secure Entry Client*.

Connection Setup

How to set up the VPN connection?

Using the Mac Client, one click is sufficient to set up a VPN connection between the computer and the corporate network. Provided the computer is connected to the internet and you have configured a profile with your personal data and the data for the VPN gateway. [Connection setup](#)^[38] may be carried out automatically or alternatingly between manually and automatically.

The client offers three modes (manual, automatic, variable) for connection set up. They can be set in the profile settings in the parameter folder [line management](#)^[37].

Manual connection set up

The default setting for connection set up is manual. In this case you have to establish the connection manually i.e. via clicking on the connection switch. A disconnect depends on the value set for inactivity timeout. If this value is set to zero (0), i.e. no inactivity timeout is configured, the connection has to be disconnected manually.

If you use this mode for connection set up, the inactivity timeout should be set with a significantly higher value than zero (0) to enable auto-disconnect for the case that no data transfer occurs. Otherwise unnecessary connection charges could arise.

Auto-connect

The client software automatically executes auto-connect for the selected profile if an application software is opened (e-mail, internet browser, terminal emulation etc.).

The connection to the remote side is automatically set up according to the settings of the profile selected. This means, that user ID and password have to be entered for this ISP in the parameter folder "dial-up network" because otherwise the auto-connect feature stops at password verification and does not establish a connection.

Auto-disconnect is carried out according to the inactivity timeout settings.

Variable connection mode

After the variable connection mode has been selected the connection has to be set up manually. Then the mode changes depending on the type of disconnect:

If the connection is disconnected by the inactivity timeout, e.g. automatically, the connection is set up automatically the next time it is required by an application i.e. the browser. If the disconnect is carried out manually via the connection switch, it has to be connected manually for the next connection establishment.

Please note for variable connection mode: If the inactivity timeout value is set to zero (0), i.e. no timeout is set, you have to disconnect manually.

FIPS Certification

The IPsec Client incorporates cryptographic algorithms conformant to the FIPS standard 140-2. The embedded cryptographic algorithms has been validated with certificate #1747.

FIPS conformance will always be maintained when the following algorithms are used for establishment and encryption of the IPsec connection:

- Diffie Hellman Group: Group 2 to 14 (DH length of 1024 bits up to 2048 bits)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES

The respective modules can be configured in the [IPsec General Settings](#)^[40]. The respective modules can be configured in the [IPsec Settings](#)^[23].

Customizing the GUI

How to customize the client monitors GUI

The client interface can be adapted in different ways: It can either be changed in the [view](#)^[65] menu item of the monitor or the configuration menu itself. The configuration interface in the profile settings can be directly adapted via [parameter locks](#)^[81] by the administrator. Via the program menu the client monitor can be minimized to an icon in the menu bar.

Monitor interface

The "view" menu item is used to show or hide various information and statistics fields. They are used in order to enlarge the size of the monitor on the display with information fields if needed, or to diminish it to its smallest possible size by switching off all information fields. The monitor can also be minimized as icon which will be displayed in the menubar (see [view](#)^[65]).

Configuration interface

The parameter locks could be set by the administrator. They have two main functions: The first is to reduce the complexity of configuration possibilities which gives the design of the software interface a slim appearance. This function hides parameter folders for features which are not used, so that the user only sees the settings which are relevant for his working environment. The second function is that pre-settings can be made which are unchangeable for the user. This avoids misconfigurations and undesired connection set ups. In this case, after installation, the user only has to enter his personal passwords for connection set up.

Parameter locks can be unlocked via the menu item "Connection". There user ID and password have to be entered. Refer to [Unlock Parameters](#) ⁸².

Certificate Configuration

The MAC Client allows the user to use any number of different certificates. A certificate configuration defines which of the certificates available on the computer is used in which way.

When the "certificates" menu item is opened for the first time on the monitor, the [default configuration](#) ²⁰ "none" is displayed in the user certificate list.

Editing the certificate configuration, you can select one of the offered types of certificates. Depending on the type of certificate, i.e. soft-certificate stored on the hard drive (PKCS#12-file), read from a token, you can define type specific settings.

The default configuration will be obtained. Additional certificate configurations have to be stored with new names.

A further certificate configuration can be set for either, the same type of certificate but different soft certificate or for a different type of certificate. In this manner you can add any number of certificate configurations.

Per profile one of these certificate configurations can be selected. This offers the possibility to authenticate with different certificates against different VPN gateways e.g. authentication towards VPN gateway 1 via soft certificate (PKCS#12) and towards gateway 2 via a certificate stored on a token (PKCS#12).

In "profile settings" you can define which certificate configuration is used for which VPN connection. Select "profiles" in the configuration menu of the monitor and then select the profile you wish to edit. Then open the parameter folder "Security".

Here you select the desired certificate configuration. The certificate configured in this VPN profile is used for authentication during IPsec connection set up (for IKE).

A further configuration step offers you the possibility to use the same certificate instead of a pre-shared key ([XAUTH with Certificate](#) ⁵⁰). Instead of entering user ID and password under, you can select one of the certificate fields in the drop-down list in the configuration field [Identity](#) ⁵⁰. This certificate then provides the corresponding data for authentication at the gateway.

Viewing the certificates

[Certificate \[View\]](#) ⁶⁸

[Display issuer certificate](#) ⁶⁹

[Display user certificate](#) ⁷¹

[Display incoming certificate](#) ⁷³

[Display CA certificate](#) ⁷⁶

PIN Handling

[Enter PIN](#) ⁸⁰

[Reset PIN](#)  80

[Change PIN](#)  81

Using the certificates

[Certificate \[Configuration\]](#)  20

[User certificate](#)  21

[PIN policy](#)  21

[Certificate renewal](#)  22

[Certificate validation](#)  57

[User of the incoming certificate](#)  57

[Issuer of the incoming certificate](#)  59

[Fingerprint of the issuer certificate](#)  60

[Use SHA1 fingerprint instead of MD5](#)  60

Configuration Parameters

[Certificate Configuration](#)  50

[Certificates \[Configuration\]](#)  20

[User Certificate](#)  21

[PIN Policy](#)  21

[Certificate Renewal](#)  22

[IPsec Policies](#)  23

[IKEv1 Policy \[IPsec Configuration\]](#)  25

[Name \[IKE Policy\]](#)  26

[Authentication \[IKE Policy\]](#)  26

[Encryption \[IKE Policy\]](#)  26

[Hash \[IKE Policy\]](#)  26

[IKEv2 Policy \[IPsec Configuration\]](#)  27

[Name \[IKEv2 Policy\]](#)  27

[Encryption \[IKE Policy\]](#)  27

[Pseudorandom Function \[IKEv2 Policy\]](#) 

[Integrity Algorithm \[IKEv2 Policy\]](#) 

[IPsec Policy \[Profiles\]](#) 

[Name \[IPsec Policy\]](#) 

[Protocol \[IPsec Policy\]](#) 

[Encryption \[IPsec Policy\]](#) 

[Authentication \[IPsec Policy\]](#) 

[Proxy for SSL VPN \(NCP VPN Path Finder\)](#) 

[EAP Options](#) 

[Profile Settings](#) 

[Basic Settings \[Profiles\]](#) 

[Line Management \[Profiles\]](#) 

[Connection Mode \[Line Management\]](#) 

[Inactivity Timeout \[Line Management\]](#) 

[Prioritize Voice over IP \(VoIP\)](#) 

[Disconnect the logical VPN tunnel when the connection is broken](#) 

[Extended Authentication \[Pre-authentication\]](#) 

[IPsec](#) 

[IPsec Policy \[Selection\]](#)  41

[Lifetime Type \[Policy\]](#)  44

[Lifetime \[Security\]](#)  45

[Volume \[Policy\]](#)  45

[PFS / DH Group](#)  45

[IPsec Compression](#)  46

[Advanced IPsec Options](#)  46

[Disable DPD \(Dead Peer Detection\)](#)  46

[SSL VPN \(NCP VPN Path Finder\)](#)  46

[IPsec Address Assignment](#)  51

[Assignment of the Private IP Address](#)  51

[DNS Server](#)  52

WINS Server

[Domain Name](#)  52

[Split Tunneling / Remote Network](#)  55

[Remote IP Networks](#)  55

Close the GUI

[Exit](#)  83

Connection

[Connect / Disconnect](#) 

Certificates View

[Certificates \[View\]](#) 

[View Issuer Certificate](#) 

[View User Certificate](#) 

[View Incoming Certificate](#) 

[View CA Certificate](#) 

PIN Handling

[Enter PIN](#) 

[Reset PIN](#) 

[Change PIN](#) 

Parameter Locks

[Lock / Unlock Locks](#) 

Information under menu item "View"

[View \[Menu\]](#) 

[Show Profiles](#) 

[Show Statistics](#) 

Information under menu item "Log"

[Log](#) 

Licensing under menu item "Help"





[Help](#) 

[Licensing](#) 

Settings

The most important configuration settings can be made manually under the menu item **NCP Secure Entry Client**

This concerns the settings:





- [Using Certificates](#)  20
- [IPsec Policies](#)  23
- [SSL VPN \(NCP VPN Path Finder\)](#)  31
- [EAP Settings](#)  32

Certificates [Configuration]

Here you determine whether you want to use certificates for authentication of the client and where you want to store the user certificates.

Further configuration fields define the PIN policy and set the time interval within which the certificate expires or a certificate renewal must be requested

Settings for the following parameters can be made:

[User Certificate](#)  21
[PIN Policy](#)  21
[Certificate Renewal](#)  22
[Computer Certificate](#)  22

Name and "Standard Certificate Configuration"

For each Secure Client a large number of certificate configurations can be created, with a unique name for each.

For each profile you can select one of the stored certificate configurations. In this way, you get the option of various ways for authentication with different certificates against different VPN gateways. E.g. authentication with soft certificate against gateway 1 and authentication with certificate from token against gateway 2.

In the configuration field Identities select the certificate configuration to be used for extended authentication.

User Certificate [Configuration]

Certificate

Define here whether or not you want to use the certificate and hence use "Extended Authentication", and where the certificate is stored.

none:

The default value is "None", meaning that certificates will not be used.

from PKCS#12 file:

In order to use a soft certificate select "from PKCS#12 File" and then select the directory (path) where the PKCS#12 file is stored for access purposes. Normally you will receive this file (encrypted) from your network administrator or your CA (Certification Authority).

PKCS#11 module:

Select "PKCS#11-Module" from the list in conjunction with "Extended Authentication" in order for the respective certificate to be read from a token.

PKCS#12 File Name:

If you are using the PKCS#12 format, then you will receive a file from your system administrator that must be copied to your PC's hard disk. In this case enter the path and filename of the PKCS#12 file or alternatively after clicking the selection button [...] select the file.

Important: The path for the filename can be abbreviated by entering the variable %CertDir% (the installation directory of the user certificates). E.g.:

%INSTALLDIR%/Certs/Test.p12

PIN Request at each Connection

Default: If this function is not used, the PIN request is displayed only for the first connect of the VPN/PKI Client.

If this function is activated, the PIN will be requested at each connect.

PIN Policy

Minimum number of characters

Default is a 6-digit PIN. An 8-digit PIN is recommended for security reasons.

Further Policies

It is recommended to implement all PIN policies, other than the one specifying that only numbers may be contained. Additionally, the PIN should not begin with a number.

The specified policies are displayed when the PIN is changed, and the policies that are only fulfilled at entry are highlighted in green (see: Change PIN).

Certificate Renewal

In this configuration field specify whether a message is to be displayed that warns of the expiration of validity, and also specify how many days prior to the certificate validity expiration this message should be displayed. After the prior date and time are reached, a message is displayed each time the certificate is used, indicating the expiration date of the certificate.

Computer Certificate

In order for the additional authentication to be used with a hardware certificate, the "Hardware certificate CN" option must be activated under Link profiles at the gateway.

With a hardware certificate, the computer authenticates itself to the gateway. If it is used in addition to a user certificate, it can be ensured that the user always dials in from the same computer.

Keychain

The certificate is imported via keychain management into the keychain "System" with the private key. If a certificate has been imported accordingly, this can be used by the client for authentication.

Subject CN / Issuer CN

The respective certificate from the keychain can be selected with the corresponding common name of applicant and issuer (Subject CN and Issuer CN), if several certificates are available.

Enter the corresponding string either in the Subject CN field or in Issuer CN. Please note:

- a) the string can contain stars * for wildcards.
- b) if the search string has a circumflex & approx; begins, the string denotes exactly the expression to be used for the search.

IPsec

Enter the IP address of the IPsec gateway in the corresponding field. In addition, select the policies to be used for negotiations carried out as part of the tunnel establishment procedure.

When, instead of a specific policy, "automatic mode" is to be used (by selecting "automatic Mode" from the pulldown list), the client and the IPsec gateway will negotiate the use of a proposal from a list of proposals sent by the client. If "automatic mode" is selected then the policy must be chosen in coordination with the remote gateway; select the required policy from the pulldown list.

The following policies are delivered with the software:

IKE Policy

The pulldown "IKE policy" list also includes the "Pre-shared key" and "RSA signature" policies, select one of these instead of the default "automatic Mode" setting.

IPsec Policy

Alternatively, IKEv2 policies are also provided.

IPsec Policy

The pulldown "IPsec policy" list also includes the "ESP - AES128 - MD5" policy, select this instead of the default "automatic mode" setting. (See also the guidelines for policies / proposal lists for IKE and IPsec policies).

See also the following:

[Gateway](#) ⁴¹ [\(Tunnel Endpoint\)](#) ⁴¹
[Exch. Mode \[Profiles\]](#) ⁴² [IKEv2 Policy \[Selection\]](#) ²⁷

As a rule, the policies will only require reconfiguring when there is no proposal in the client's policy (proposal list) that exactly matches the IKEv1, IKEv2 or IPsec proposals at the gateway.

The IPsec Policy folder contains the policy "ESP-AES128-MD5".

The authentication negotiations between client (IPsec initiator) and IPsec gateway are carried out in accordance with the IKE proposal agreed between client and gateway and an encoded control channel is established between the two.

The exact algorithms used for encrypting and authenticating data in the IPsec tunnel are based on the IPsec proposal agreed between client and gateway.

See also following topics:

[IKEv1 Policy \[IPsec Configuration\]](#)

[IKEv2 Policy \[IPsec Configuration\]](#)

[IPsec Policy \[Profiles\] \(Phase 2-Parameter\)](#)

IKEv1 Policy [IPsec Configuration]

The parameters in this folder apply to the Internet Key Exchange (IKE) with which the control channel for the SA negotiation is established.

The IKE policies which you configure here will then be listed for selection in the "IKEv1 Policy" pulldown in the IPsec General Settings folder.

Two IKE policies are delivered with the software and they provide differing functionally: "Pre-shared Key" and "RSA-Signature". Every policy lists at least one proposal for authentication and encryption algorithms (IKEv1 policy, authentication, encryption), i.e. a policy consists of one or more proposals. One IKE policy is delivered with the software: "Pre-shared Key". Every policy lists at least one proposal for authentication and encryption algorithms (IKEv1 policy, authentication, encryption), i.e. a policy consists of one or more proposals.

The same policies including the associated proposals should apply for all users, meaning that the same proposals should be configured in policies, both on the client side and on the VPN gateway.

Algorithms and Parameters

The following policy/proposal parameters are common to all connection profiles:

[Name \[IKEv1 Policy\]](#) 

[Authentication \[IKEv1 Policy\]](#) 

[Encryption \[IKEv1 Policy\]](#) 

[Hash \[IKEv1 Policy\]](#) 

Name [IKE Policy]

When adding a new policy, first give it a name by which it can be referenced later.

Authentication [IKE Policy]

Open the proposals folder by clicking on the "Proposal" tab. The two sides of the VPN link must have authenticated each other before the Control Channel for Phase 1 negotiations (IKE Security Association) can be established.

Pre-shared Key

Select this setting if the same pre-shared key (also referred to as the shared secret) is to be used on the client and the VPN gateway for mutual authentication.

RSA Signature

Select this setting if details from a certificate, configured for the "Extended Authentication" (XAUTH), are to be used for mutual authentication.

(In Main Mode the certificate will also be encrypted. Note: only select "RSA Signature" if a PKI infrastructure is in place.

Encryption [IKE Policy]

Symmetrical encryption of messages 5 and 6 in the Control Channel occurs according to one of the optional encryption algorithms if Main Mode (identity protection mode) is used. In automatic mode the encryption is determined by the communication partner.

For each IKE policy proposal, a custom encryption algorithm can be selected from the pull-down menu.

Hash [IKE Policy]

This is the mode that determines how the hash value over the ID is formed, or in other words how the certificate of messages is formed in the control channel.

From the displayed list a value can be selected.





IKEv2 Policy [IPsec Configuration]

The parameters in this folder apply to phase 1 of the IKEv2 (Internet Key Exchange version 2) protocol with which the control channel for the security association (SA) is established.

The IKEv2 policies which you configure here will then be listed for selection in the "IKEv2 Policy" pulldown in the IPsec General Settings folder.

No IKEv2 policies are delivered with the software.

Algorithms and Parameters

[Name \[IKEv2 Policy\]](#) 
[Encryption \[IKEv2 Policy\]](#) 
[Pseudorandom Function \[IKEv2 Policy\]](#) 
[Integrity Algorithm \[IKEv2 Policy\]](#) 

All the above parameters can be edited by selecting/adding the appropriate policy and modifying/adding the appropriate proposal.

Name [IKEv2 Policy]

When adding a new policy, first give it a name by which it can be referenced later.

Encryption [IKEv2 Policy]

Symmetrical encryption of IKEv2 messages 3 and 4 (the second exchange) in the Control Channel occurs according to the encryption algorithms negotiated between initiator and responder during messages 1 and 2 of the IKEv2 exchange (the first exchange).

The keys used are generated using the Pseudorandom Function negotiated between the two parties during the first exchange. In automatic mode the encryption is determined by the communication partner.

For each separate proposal select an Encryption algorithm from the pulldown list.

Pseudorandom Function [IKEv2 Policy]

Random values used for Integrity Protection and Encryption during the second IKE exchange are generated using a Pseudorandom Function negotiated between initiator and responder during the first exchange.

For each separate proposal select a Pseudorandom Function from the pulldown list.

Integrity Algorithm [IKEv2 Policy]

IKEv2 incorporates integrity protection functionality to protect the SA creation process from interference by third parties.

The cryptographic algorithm to be used for integrity protection is negotiated during the first IKEv2 exchange.

For each separate proposal select an Integrity Algorithm from the pulldown list.

IPsec Policy [Profiles]





The parameters in this folder apply to phase 2 of the SA negotiation. The IPsec policies which you configure here are listed for selection for the internally created SPD.

Only one IPsec policy with ESP (Encapsulating Security Payload) is delivered with the software - ESP-AES128-MD5. As IPsec mode with AH security is unsuitable for flexible remote access, the AH protocol is not available.

Every IPsec policy lists at least one proposal for IPsec protocol and authentication, i.e. a policy can consist of one or more different proposals.

The same policies including the associated proposals should apply for all users. This means the same proposals should be available for the policies, both on the client side and on the central system.

Algorithms and Parameters

[Name \[IPsec Policy\]](#) 
[Protocol \[IPsec Policy\]](#) 
[Encryption \[IPsec Policy\]](#) 
[Authentication \[IPsec Policy\]](#) 

Name [IPsec Policy]

When adding a policy first give it a name by which it can be referenced later.

Protocol [IPsec Policy]

The default value is ESP.

Transform / Encryption

When using the security protocol ESP, the algorithm to be used for encrypting the payload can be selected from the displayed list.

Authentication [IPsec Policy]

Select the authentication mode to be used for the ESP security protocol from the displayed list.

Proxy for SSL VPN (NCP VPN Path Finder)

If the SSL VPN (NCP VPN Path Finder) option is used under [Advanced IPsec Options](#) ⁴⁶ in the configuration menu of the profiles but Internet access is only available via a proxy server, either define the proxy settings manually here or select the system settings configured under Windows.

EAP Options [Configuration]

You can specify whether EAP authentication (802.1x) will be executed on all network interfaces, in the "EAP Options" of the monitor menu. The setting made here applies globally for all profile entries. The authentication methods EAP-MD5 and EAP-TLS are supported.

- disabled
- for all network interfaces

Use of the Extended Authentication Protocol Message Digest version 5 (EAP MD5) can be specified via the main menu of the monitor under "Configuration / EAP Options". This protocol can then be used if a switch, a hub, or if an access point is used, which support 802.1x and the according Authentication Mode for the access to the Wi-Fi. You can prevent unauthorized users from getting into the LAN via the hardware interface with the Extended Authentication Protocol (EAP MD5).

You can use either [User ID](#)^[50] with [Password](#)^[50] ([Identities](#)^[50]) or your own "EAP User ID" with an "EAP Password".

The contents of the certificate can be imported automatically in such a way that the [username](#)^[50] and [password](#)^[50] are imported from the certificate in the profile under [Identity](#)^[48] / [Extended Authentication](#)^[50] and the "VPN username and VPN password" is enabled in the EAP options.

For EAP-TLS (with certificate) now the EAP identity can be directly referenced from the certificate configuration. The following content of the configured certificate can be used by entering the appropriate placeholders in the EAP configuration:

Commonname: %CERT_CN%

E-mail: %CERT_EMAIL%

Profiles [Parameters]

Select this menu option and any profiles already defined will be displayed in a list.

The buttons below the list of profiles will not be available if the corresponding lock-outs have been set. If there are no restrictions on profile settings, all buttons will be available, and clicking will initiate their respective functions.

To edit the (default) values of a profile, use the mouse to select the profile and then click on the [Edit] button. This opens the profile setting and displays the following list of configuration folders on the left hand side:

Basic Settings [Profiles]	35
Line Management [Profiles]	37
IPsec [Configuration]	40
Advanced IPsec Options	46
Identities	48
IPsec Address Assignment	51
Split Tunneling	55
Certificate Check	57
Extended Authentication	61

Profile Groups

The list of all profiles displayed is sorted by name.

Should the list of profiles be too long, profiles can also be divided up into groups. Click on [Group] above the phone number display to open the group configuration.

Clicking on [+] will add a new group to the column on the left, which you can then name.

Select profiles from the right-hand column to add to the new group in the column on the left. You can associate each profile with multiple groups where required.

Click on [Edit] to edit the name of the group. Click on [-] to remove the group currently displayed, and the relevant profile associations. The profiles themselves will not be deleted.

Group Display

You can now display all profiles, or alternatively only those profiles that have been associated with a selected profile group.

On the user interface of the monitor in the profile selection area, use right mouse click to decide whether all profiles should be displayed, or just those associated with a particular group.

Basic Settings [Profiles]

The client software enables individual profiles to be created and each can be configured according to user requirements. In order to distinguish between profile settings, allocate a name for the profile in this parameter field. See [Profil Name](#) ³⁶

Profile Name

When you define a new profile, you should initially enter a distinctive name for the profile (e.g. IBM London). The name may contain any desired letters as well as numbers and may be up to 39 characters including blanks.

Line Management [Profiles]

In the "Line Management" folder define the connection mode, together with any timeout values that will specify when a link is to be automatically disconnected.

Please also refer to the following topics:

[Connection Mode \[Line Management\]](#)  38

[Inactivity Timeout \[Line Management\]](#)  39

[Prioritize Voice over IP \(VoIP\)](#)  39

[Disconnect the logical VPN tunnel when the connection is broken](#)  40

Connection Mode [Line Management]

Define here how and when connections are established:

manual

The default setting for Connection Mode.

When Connection Mode is set to "manual", VPN connection establishment has to be activated manually (by pressing Connect). The connection will be disconnected on expiry of the inactivity timeout provided that this parameter has been set to a non-zero value (0). If the inactivity timeout is set to zero then the connection must be manually disconnected.

always

When Connection Mode is set to "always", a VPN connection is always established automatically when the Client starts. Connection establishment is independent of the "Connect" button, of the onset of data transfer, or of how the monitor is set to be displayed - see Autostart.

variable (Connect starts always mode)

If this mode is selected, when "Connect" is pressed to establish a VPN connection the Client starts using the "always" mode - see "always" above. The Client continues using "always" mode until the monitor is closed, when the mode reverts to this setting.

Inactivity Timeout [Line Management]

This parameter is for setting the time delay to be used following the last transmission of data before automatically executing disconnect. Time is expressed in seconds. Possible settings are from 0 to 65356 seconds.

Note: In order for the inactivity timeout to be activated it is necessary to enter any value from 1 to 65356. The value "0" (zero) means that no automatic timeout (disconnect) is executed. When the inactivity timeout is set to "0" (zero) you must manually execute disconnect.

Important: The inactivity timer only begins counting down after the last data transmission and after any communications handshaking has stopped.

Prioritize Voice over IP

Should this client be used for communication with Voice over IP, this function should be activated in order to send and receive the speech data without delays or distortions.

Disconnect the logical VPN tunnel when the connection is broken

This switch modifies the default behavior of the Client

(maintain logical connection)

If the Client's default setting is switched off, the logical connection will also be disconnected when the physical connection breaks, and the VPN tunnel will be disconnected.

Visual Feedback about Status of Tunnel

When a break occurs in the physical communication medium connection used to establish a VPN tunnel, the existing VPN tunnel remains established, for an unspecified length of time. Thus the tunnel remains logically active while the new physical connection is being established.

During the period the physical connection is broken, the normally solid green bar displayed in the Client monitor changes to a dashed green bar and the icon in the system tray flashes yellow and green. These indicators remain until the physical connection is re-established, when they return to solid green.

The monitor does not show the dashed green bar if the Client's default behavior is switched off in the profile being used for connection establishment.

IPsec [Profile]

Here the preconfigured IPsec guidelines can be selected as well as the encryption defined and, if necessary, the IPsec compression set:

[Gateway \(Tunnel Endpoint\)](#) 

[Exchange Mode](#) 

[Tunnel IP Version](#) 

[IKE Policy](#) 

[IKE DH Group](#) 

[IPsec Policy](#) 

[PFS Group \(DH Group\)](#) 

[Policy Lifetimes](#) 

Gateway (Tunnel Endpoint)

Enter the address of the remote gateway here. You will receive that address from your administrator, either as an IP address or as a name string.

Notes

Alternative tunnel endpoints can be entered in addition to the first tunnel endpoint. The addresses must all be separated by comma (,) or all by semicolon (;). Spaces are not allowed as separators.

A maximum of four different tunnel endpoints may be defined in the Client for use in connection establishment. These will be selected as follow:

1. If the alternative tunnel endpoints are separated from each other by a semicolon (;), attempts to establish a connection will be made in the sequence of tunnel endpoints, starting with the first entry in the list. If that attempt fails, the next address in the list will be used and the process will be repeated by the Client for a maximum of seven successive attempts or until a connection attempt is successful.
2. If the alternative tunnel endpoints are separated from each other by a comma (,), attempts to establish a connection will be made in the sequence of tunnel endpoints, but the address of the first attempt will be chosen at random. If that attempt fails, the next address in the list will be used and the process will be repeated by the Client for a maximum of seven successive attempts or until a connection attempt is successful.

IPsec Policy [Selection]

automatic mode:

In this case, the configuration of the IPsec policy via the IPsec configuration can be omitted.

ESP-AES256:

As an alternative to the automatic mode, this preconfigured IPsec policy can be used.

Select the IPsec policy from the pulldown list. (default: ESP_AES_GCM256) Preconfigured: ESP-AES128-MD5.

automatic Mode:

In this case it is not necessary to configure the IPsec policy in the IPsec menu.

If the Secure Entry Client is to use special policy proposals or lifetimes, modify or delete the respective details under [IPsec](#) ²³ settings.

Exchange Mode [Profiles]

The Exchange Mode determines how Internet Key Exchange should proceed. Two modes are available:

Main Mode (IKEv1) also referred to as Identity Protection Mode, and Aggressive Mode (IKEv1).

These modes differ in the number of messages passed between the two parties and by their use of encryption.

Main Mode (IKEv1):

In Main Mode (default setting) six messages are sent over the Control Channel and the last two messages are encrypted. The last two messages contain the user ID, the signature, the certificate and, if required, a hash value. This is why it is also known as "Identity Protection Mode".

Aggressive Mode (IKEv1):

In Aggressive Mode only three messages are sent over the Control Channel and nothing is encrypted.

IKEv2:

The Internet Key Exchange Protocol Version 2 (IKEv2) includes the Mobility Extensions (MOB IKE) in the Client's base.

Tunnel IP Version

This parameter can be used to configure for which IP version the IPsec negotiation should be performed. The configuration option exists only for IPsec connections with key exchange via IKEv2!

Only if the [Exchange Mode IKEv2](#) ⁴² is set, this option is displayed to select the tunnel IP version:

IPv4

Is the default setting (this ensures that the VPN client behaves exactly the same way after a software update).

IPv6

If the gateway of a third-party manufacturer supports IPv6, this setting can be selected. VPN gateways from other manufacturers, which do not support IPv6 but receive IPv6 packets, behave differently and may not build a tunnel. Therefore, it is recommended that you do not configure IPsec negotiation for IPv6 in this case.

IPv4 + IPv6

With this setting, for example, a network architecture can be supported whose gateway (destination address) only supports IPv4, but the devices of the company network IPv6.

Note that split tunneling is visible only for IPv6 only, if the exchange mode IKEv2 is selected and the tunnel IP version IPv6 is set.

Policy Lifetimes

Policy Lifetimes [IPsec General Settings]

All IKE and IPsec policies are subject to the same set of lifetime parameters. These can be reconfigured if necessary and are accessed via the [Policy Lifetimes] button.

See also following topics:

[Life](#) ⁴⁴ [Type \[Policy\]](#) ⁴⁴
[Life Time \[Policy\]](#) ⁶²
[kBytes \[Policy\]](#) ⁴⁵

Life Time Type [Policy]

Determines the criteria for key lifetime; this can be based either on duration or transferred bytes or both. When the counter (time or number of bytes) expires, a new SA negotiation takes place.

Life Time [Security]

Set the length of the life time for use of an SA created using the IPsec policy. When the counter (time, in seconds) expires, a new SA negotiation takes place.

Volume [Policy]

The amount of kbytes specified here, which are transferred between client and server, determines the validity period of a security association (see [IPsec Policy](#) ²³). After transmission of the specified kBytes, a new SA negotiation takes place. With each new SA negotiation, the counter is reset.

PFS / DH Group

The selection of one of the available Diffie Hellman groups determines that a complete key exchange (PFS) should additionally occur in phase 2 with the SA negotiation. The higher the DH group, the more secure the Key Exchange.

Advanced IPsec Options

Please also refer to the following topics:

[IPsec Compression](#) 

[Disable DPD \(Dead Peer Detection\)](#) 

[SSL VPN \(NCP VPN Path Finder\)](#) 

IPsec Compression

Turn IPsec compression on or off using this switch. The remote station specifies which IPsec compression is used. The data transmission with IPsec can be compressed in the same way as with a transfer without IPsec. This allows for a maximum three-fold increase of the throughput.

Disable DPD (Dead Peer Detection)

DPD (Dead Peer Detection) runs in the background, when supported by the destination gateway. The IPsec Client uses DPD to check, at regular intervals, if the remote peer is still active.

When no data is received over the VPN tunnel, the VPN client will trigger DPD. If the VPN client receives a response from the VPN gateway, it will try again in the configured DPD interval.

If the VPN client does not receive a response, it will send a retry within 5 seconds to detect a dead session fast.

If the VPN client will receive no response after the amount of configured retries in a row, it will disconnect the session.

This functions switches off DPD.

SSL VPN (NCP VPN Path Finder)

The major prerequisite for SSL VPN (NCP VPN Path Finder) is a VPN gateway with SSL VPN (NCP VPN Path Finder) technology (e.g. NCP Secure Server 8.00 or later). There, an alternative port must be configured in the VPN / IPsec settings of the local system.

Whenever a standard IPsec connection, i.e. via port 500 or UDP encapsulation via a freely configurable port, can not be established, SSL VPN (NCP VPN Path Finder) automatically switches to the alternative connection protocol, TCP encapsulation with SSL Header (Port 443).

This is relevant when only HTTPS port 443 is available for the client and a standard IPsec connection can not be established. This is often the case, for example, in a hotel or at a hotspot.

If a proxy server is to be used for this connection, it can be set and configured in the configuration menu under Proxy for SSL VPN (NCP VPN Path Finder).

If a connection is established using this technology (i.e. using port 443), the monitor displays this via an icon in its state display (below and to the right of the HQ / gateway).

The monitor interface displays the icon after VPN dial up.

Identities

A number of more detailed security settings can be made that are dependent on the IPsec security mode.

See following parameters:

[IKE ID-Type \[Identities\]](#) 

[IKE ID \[Identities\]](#) 

[Certificate Configuration](#) 

[Pre-Shared Key](#) 

[Extended Authentication \(XAUTH\)](#) 

Type [Identities]

Native IPsec differentiates between outgoing and incoming connections. The value selected by the initiator as ID for an outgoing connection must be selected by the remote gateway as ID for incoming connections.

The following ID types can be selected:

- IP Address
- Fully Qualified Domain Name / (equivalent of host name)
- Fully Qualified Username / (e-mail address of the user)
- ASN1 Distinguished Name
- IP Subnet Address
- ASN1 Group Name
- Free String used to identify Groups

IKE ID [Profiles]

For IPsec there is a differentiation of incoming and outgoing connections. The value selected by the IPsec initiator as ID for outgoing connections must also be selected at the remote gateway as ID for incoming connections.

Enter the [IKE ID-Type](#) ⁴⁹ string that corresponds to the associated "IKE ID Type".

The default for the type is U-FQDN (Fully Qualified Username)





IPsec Pre-shared Key [VPN Tunneling]

"IPsec Pre-shared Key" is the password required to build a tunnel to the VPN gateway. The tunnel is only set up if the password set in the VPN Gateway is the same as the password set at the Secure Client. The "IPsec Pre-shared Key" can be up to 16 characters long.

Certificate Configuration [Profiles]

A certificate which was installed using the client monitor's Certificate Configuration can be selected here for extended authentication (XAUTH).

Refer also to:

[User Certificate](#)  21
[PIN](#)  21 [Policy](#)  21
[Certificate Renewal](#)  22

none:

A certificate is not used for data encryption and authentication.

Extended Authentication (XAUTH)

On the Entry Client, extended authentication (XAUTH protocol, draft 6) is not active by default. It can be switched on at this point if it is supported by the IPsec gateway. In addition to the pre-shared key, the following parameters can also be used for authentication:

User ID [Identity]

Obtain the user ID for XAUTH from your system administrator. The name may be up to 256 characters long.

Password [Identity]

Obtain the password for XAUTH from your system administrator. The name may be up to 256 characters long.

Alternatively a certificate of the certificate configuration can be used.

IPsec Address Assignment

When using native IPsec, the Client's IP addresses can be assigned in a number of different ways, each of which can be configured here.

Note:

[Assignment of the Private IP Address](#)  51

[DNS-Server](#)  52

[DNS domains to be resolved in the tunnel](#)  52

Assignment of the Private IP Address

Use this parameter to define how the IP address should be assigned. Select the option required from the pulldown list.

IKE Config Mode

With IKE config mode (Draft 2) the IP addresses of the client, the DNS servers as well as the domain name are dynamically assigned.

With IPsec tunneling, DPD (Dead Peer Detection) and NAT-T (NAT Traversal) are automatically executed in the background, when this is supported by the remote gateway. The client uses DPD to check, at pre-specified intervals, whether the remote gateway is still active. If the remote gateways fails to respond then the connection is automatically disconnected.

The negotiation of NAT Traversal is handled automatically by the client and is always necessary when a device using network address translation is employed by the destination system.

Local IP address

In this case the IP addresses (also DHCP) currently configured in the computer's network settings are used for the IPsec Client.

This is the default setting for the Entry Client.

Manual IP address

Enter the IP address and the subnet address here. In this case the addresses entered here are used, independently of the configuration in the computer's network settings.

DHCP over IPsec

As an alternative to using IKE config mode, a DHCP server of the gateway can also be used; the IP address is then assigned to the client via the VPN tunnel by means of a DHCP negotiation.

One or two DNS servers can be assigned, dependent on your requirements; the primary server is used as the default server.

DNS Server

You can define an alternative DNS server as opposed to using the one that is automatically assigned during the PPP negotiation. Please be sure to activate "Enable DNS" in the DNS configuration folder under the windows network settings.

In accordance with your requirements you can assign one or two DNS servers. The primary server is used as the default server. If no alternative server has been defined, the server assigned via PPP is used.

First / Second DNS Server: The first DNS server entry is used instead of the address assigned during any connection establishment negotiations. The second DNS server entry is used as a backup server.

Domain Name

DNS domains to be resolved in the tunnel

This field is blank in the default settings for a new VPN profile, i.e. this parameter is not in use and all DNS requests are forwarded outside the tunnel to the DNS server that has been allocated in the Internet (by the provider).

If an asterisc "*" is entered, all DNS queries are forwarded through the VPN tunnel.

If an address is entered, the Client checks each outgoing (from the computer) DNS packet for the DNS name being queried. If the most significant (i.e. right-most) characters in the DNS name in the packet are identical with the sequence of characters entered here, the DNS query is forwarded via the VPN tunnel. If the check fails the DNS query is sent to the Internet. DNS queries with names that do not include a "." are always forwarded via the VPN tunnel.

The Domain Suffix appended when using IKE Config Mode is automatically appended to all names in the list of domain names to be resolved via tunnel.

Syntax

- names in the list are not case sensitive,
- all alphanumeric characters (0 - 9, a - z) and minus (hyphen) are allowed, umlauts and special characters (including space) are not allowed,
- comma, semicolon or space can be used as separator in a list domain names, and
- question mark "?" and asterisk "*" can be used as wildcards. Note that an "*" can only be used in the least significant (i.e. left most) position of the domain name.

Examples:

*.ncp.de ->
www.ncp.de, or
www.intranet.ncp.de, or
www.webserver.ncp.de, ...

www??.uni.de ->
www01.uni.de, or
www02.uni.de, or

www03.uni.de, ...

www.ncp-e.com -> www.ncp-e.com

Split Tunneling / Remote Network

Exactly those IP networks can be defined here, with which the client must communicate via VPN tunnel. If tunneling is used and no entries are made here, then the connection will always be established to the tunnel endpoint of the gateway. Should both tunneling to the central office and communication via the Internet be enabled simultaneously, then enter in this list the IP network(s) that the client may only reach via the tunnel. You will then be able to alternate between access to the Internet and the gateway of the company headquarters. This is known as Split Tunneling.

Click on the "Add" button and enter IP address and network subnet mask in the window which appears.

Please also refer to:

[Remote IP Networks \(IPv4\)](#)  55

[Full Local Network Enclosure Mode](#)  55

[Remote IP Networks \(IPv6\)](#)  56

Remote IP Networks (IPv4)

Enter here the address of the IP network to be reached by the client via the VPN Gateway. You can obtain the address(es) from your system administrator.

If you do not make an entry in this list, all IP packets will be sent via the VPN tunnel.

Please make sure that the IP address of the VPN Gateway does not lie in the range of the network addresses.

A maximum of twenty networks can be configured.

Remote IP Net Masks

Enter the appropriate IP network subnet mask here. You obtain the address(es) from your system administrator.

Please make sure that the IP address of the VPN Gateway does not lie in the range of the network addresses.

In the case of Split Tunneling refer to the notes about DNS queries under DNS domains to be resolved in the tunnel.

Alternative address input

If the prefix length is additionally entered when entering the IP address (for example, 175.16.15.0/24), the subnet mask is created from the prefix length when leaving the input field and entered in the corresponding column.

Full Local Network Enclosure Mode

Enable this function if you wish to route all the local LAN traffic over the VPN tunnel.

Remote IP Networks (IPv6)

Data entry for an IPv6 network is accomplished by entering the IP address and attached prefix length (e.g., 2001: 0db8: 85a3: 08d3 :: / 64).

A maximum of twenty networks can be configured.

Certificate Check

Checking the certificate contents

You can specify in the "Certificate Check" parameter field, per destination system, which entries must be present in a certificate from the remote side (Secure Server)(see: Display Incoming Certificate, General).

Please also refer to the following topics:

[Incoming Certificate's Subject](#)  57

[Incoming Certificate's Issuer](#)  59

[Issuer's Certificate Fingerprint](#)  60

[Use SHA1 Fingerprint](#)  60

Incoming Certificate's Subject

All attributes of the user, to the extent known - even with wildcards -, can be used as user certificate entries of the remote side (server). In this regard compare the entries that are always listed under users for "Display Incoming Certificates".

Use the attribute name abbreviations for this. The attribute type abbreviations for certificate entries are as follows:

cn	Common Name
s	Surname
g	Givenname
t	Title
o	Organization
ou	Organization Unit
c	Country
st	State
l	Location
email	e-mail
sn	Serialnumber

Example:

cn=VPNGW*, o=MyCompany, c=de

In the above example:

- The common name of the security server is checked here only as far as the wildcard "*". All subsequent positions, such as 1 - 5 as numbering, will be ignored.
- The organization must always be "MyCompany".
- The country must be United States.

Incoming Certificate's Issuer

All attributes of the user, to the extent known - even with wildcards -, can be used as user certificate entries of the other side (server). In this regard compare the entries that are always listed under users for "Display Incoming Certificates".

Use the attribute name abbreviations for this. The attribute type abbreviations for certificate entries have the following meaning:

cn	Common Name
s	Surname
g	Givenname
t	Title
o	Organization
ou	Organization Unit
c	Country
st	State
l	Location
email	e-mail
sn	Serialnumber

Example:

cn=My Common Name

Only the common name of the issuer is verified here.

Issuer's Certificate Fingerprint

In order to prevent an unauthorized person, imitating a trusted CA, from using a counterfeited issuer certificate, the issuer's fingerprint can also be entered if it is known.

A comparison check is performed on each character entered, and each character must exactly match the corresponding character in the fingerprint, starting from the first, i.e. left most character. The accuracy of the check increases with the number of characters entered.

SHA1 Fingerprint

The algorithm for fingerprint generation can be either MD5 (Message Digest version 5) or SHA1 (Secure Hash Algorithm 1).

Extended Authentication [Pre-authentication]

Local biometric authentication before the VPN connection is established is available with MacOS version 10.10+

Biometric Authentication

When this setting is enabled, an authentication prompt is displayed as soon as the user clicks connect in the client. The VPN connection will only be initiated after successful authentication via the method which is configured on the operation system (fingerprint recognition, face recognition, PIN entry, etc.).

IKEv1 / IKEv2

Depending on the [Exchange Mode](#) ⁴² either an IKEv1 policy or an IKEv2 policy is suggested for further configuration.

[IKEv1 Policy](#) ⁶² when selecting Main Mode (IKEv1), also Identity Protection Mode, or Aggressive Mode (IKEv1).

[IKEv2 Policy](#) ⁶² when selecting IKEv2 Exchange Mode.

Further parameters:

[Lifetime](#) ⁶² of the policy

[IKE DH Group](#) ⁶³

[IKE ID Type](#) ⁴⁹

[IKE ID](#) ⁴⁹

IKEv1 Policy

IKEv1 and IKEv2 Policies [Profiles]

IKEv1 Policy

Select the IKEv1 policy from the pulldown list (preconfigured: "Pre-shared Key" and "RSA Signature"). All IKEv1 policies which were created during software installation or during IPsec configuration are listed by name in the pulldown.

automatic Mode: In this case it is not necessary to configure the IKEv1 policy in the IPsec menu.

Pre-shared Key: This preconfigured policy can be used without PKI support. The same "Static Key / Pre-shared Key" must be used at both ends of the VPN link.

RSA Signature: This preconfigured policy can only be set if a PKI has been implemented (Secure Server). Implementation of the RSA signature as additional strong authentication requires the use of a smartcard or soft certificate.

If the Secure Entry Client is to use special IKEv1 policy proposals or lifetimes, use the [Policy Editor] and [Policy Lifetimes] buttons to create, modify or delete the respective details.

IKEv2 Policy [Profiles]

If the Secure Entry Client is to use special IKEv2 policy proposals or lifetimes, use the [Policy Editor] and [Policy Lifetimes] buttons to create, modify or delete the respective details.

If automatic mode is selected, it is not necessary to configure an IKEv2 policy.

Important: If IKEv2 has been selected as the key exchange protocol, by selecting IKEv2 as the "exchange mode", an IKEv2 authentication protocol must be selected - see "IKEv2 Authentication".

IKEv2 Policy

If automatic mode is selected, it is not necessary to configure an IKEv2 policy in the [IPsec Configuration](#) ²³ menu.

Alternatively, the IKEv2 policy AES-GCM256-HMAC-SHA384 is provided, which can be reconfigured in the IPsec settings if required.

Life Time [Policy]

Set the length of the life time for use of the policy. When the counter (time) expires, a new SA negotiation takes place. (Default Phase 1: 8 h, phase 2: 1 h.)

IKE DH Group [IKE Policy]

The selection of one of the Diffie Hellman groups offered determines the level of security for the key exchange. Later a symmetrical key will be generated according to this selection. The higher the DH Group the more secure the key exchange.

The default is DH19

IKE ID Type [Profiles]

Native IPsec differentiates between outgoing and incoming connections. The value selected by the initiator as ID for an outgoing connection must be selected by the remote gateway as ID for incoming connections.

The following ID types can be selected:

- IP Address
- Fully Qualified Domain Name / (equivalent of host name)
- Fully Qualified Username / (e-mail address of the user)
- ASN1 Distinguished Name
- IP Subnet Address
- ASN1 Group Name
- Free String used to identify Groups

IKE ID [Profiles]

For IPsec there is a differentiation of incoming and outgoing connections. The value selected by the IPsec initiator as ID for outgoing connections must also be selected at the remote gateway as ID for incoming connections.

Enter the [IKE ID-Type](#) ⁴⁹ string that corresponds to the associated "IKE ID Type".

The default for the type is U-FQDN (Fully Qualified Username)

View

Via this feature you can modify the operating surface of the monitor and choose the language. The following features are found in the "View" pull-down menu:

[Show Profiles](#) 
[Show Statistics](#) 

Show Profiles

If several configured profiles are available, whatever is required can be selected from those lists.

Show Statistics

When "Show Statistics" is enabled additional information about the connection is displayed e.g. time online, transferred data, timeout etc.

Connect / Disconnect

A connection can only be established if a profile has already been properly defined and selected; the profile to be used to establish the connection is displayed in the monitor below the menu bar.

If the function "Connect" is selected, the connection will be manually established to the destination system.

To have the link established automatically, set "Connection Mode" to the required value in the "Profile Settings / Line Management" folder.

Disconnect

A connection can be manually disconnected by clicking on "Disconnect" in the Connection pull-down menu or by clicking on the "Disconnect" switch.

Status display of the product icon



The color of the status icons change from red to green during connection.

Connection Info

The connection information under "General" shows:

- the name of the currently selected profile
- statistical information (e.g. time online, value of timeout)
- IP addresses (VPN IP address, DNS server, VPN Endpoint)
- Security mode
- the security keys used

Certificates [View]

Certificates are created and issued by a Certification Authority (CA) (also referred to as the Issuer), using a PKI manager (software), and then either burnt onto a Smart Card (chipcard) or stored as a soft certificate (or digital certificate) in a normal file. Certificates with digital signatures can be used in the same way as a digital personal identity card.

Certificates can be created with a private key up to a length of 4096 bits.

If certificates are being used, after CHAP authentication (user ID and password) between client and VPN gateway has been used for tunnel establishment, Extended Authentication is carried out using certificates stored at the client and the VPN gateway. In this process, "Extended Authentication" together with negotiation of the session key for the previously selected encryption method are carried out.

View Issuer Certificate

The Issuer Certificate (also referred to as a CA Certificate) can only be viewed if it is contained in the User Certificate; enter the User Certificate's PIN to display it.

View Issuer Certificate enables you to review which values were used to create the certificate, e.g. unique e-mail address.

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Certification Authority (CA): The issuer and user of an Issuer Certificate are normally identical (self-signed certificate). The issuer of the issuer certificate has to be identical to the issuer of the user certificate (see View User Certificate).

Serial Number: The serial number of the certificate is compared with serial numbers maintained in the Certification Authority's certificate revocation list(CRL).

Valid to/from: The validity of a certificates is limited. Normally the validity of an Issuer (Root) Certificate is longer than the validity of a User Certificate. Upon expiry of the validity of the Issuer Certificate, the validity of any User Certificate from the same CA expires as well.

Fingerprint: = hash value. The signature of the certificate is the hash value encrypted with the private key of the CA.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for the Secure Client and the Secure Server:

- keyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- Certificate Distribution Point (CDP)

keyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted. If one of the bits is not set, then the connection will be disconnected:

- Digital Signature
- Key Encipherment (keytransport, key management)
- Key Agreement (key exchange process)

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then the Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

View User Certificate

In order to view the User Certificate, first enter the PIN.

View User Certificate enables you to review which values have been used to create the certificate, e.g. unique e-mail address.

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Certification Authority (CA): The issuer/CA of your User Certificate must be identical to the issuer of the CA certificate. (see View Issuer Certificate).

Serial Number: The serial number of the certificate is compared with the serial number kept in the revocation list of the Certification Authority (CRL).

Valid to/from: The validity of a certificates is limited. Normally the validity of an Issuer (Root) Certificate is longer than the validity of a User Certificate. When the validity expires the functionality of the certificate is also lost.

Fingerprint: = hash value. The signature of the certificate is the hash value encrypted with the private key of the CA.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for Secure Client and the Secure Server:

- keyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- Certificate Distribution Point (CDP)

keyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted:

- Digital Signature
- Key Encipherment (keytransport, key management)
- Key Agreement (key exchange process)

If one of the bits is not set, then the connection will be disconnected.

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then the Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

View Incoming Certificate

View the certificate that was transmitted from the remote side (Secure Server) as part of the SSL negotiation. You can see, for example, whether you have accepted the issuer displayed here in the list of your CA certificates (see below).

If the incoming User Certificate is from one of the CAs not known in the "Display CA Certificates" list, or if it does not match with the Root Certificate in the p12 file, then the connection will not be established.

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for Secure Client and the Secure Server:

- keyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- Certificate Distribution Point (CDP)

KeyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted. If one of the bits is not set, then the connection will be disconnected:

- Digital Signature
- Key Encipherment (keytransport, key management)
- Key Agreement (key exchange process)

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

HTTP Proxy for CRL Download

A proxy for the CRL download can be configured via HTTP in the ncppki.conf file in the "HttpProxy" group:

```
[HttpProxy]
ProxyHost = xxx.xxx.xxx.xxx
#IP address of the proxy server for CRL download via HTTP
ProxyPort = 80
#Port of the proxy server for CRL download via HTTP
ProxyUser = xyz
#Username of the proxy server for CRL download via HTTP
ProxyPw = xxxx
#Password of the proxy server for CRL download via HTTP
```

CRL and ARL Checks

The client is also capable of checking the following revocation lists:

- Certificate Revocation List (CRL)
- Authority Revocation List (ARL)

The CRLs and ARLs must be copied to the respective (i.e. "\CRL" or "\ARL") subdirectories in the installation directory.

View CA Certificates

Multiple issuer certificates are supported with the client software (Multiple CA Support). For this, the issuer certificates must be collected in the installation directory under "cacerts". In the client monitor the list of CA certificates read-in is displayed under this menu item.

If a certificate of a remote system is received, then the client determines the issuer, then searches for the issuer in the CA certificates.

If no CA Certificate matches, then the connection will not be established (No Root Certificate found!).

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for Secure Client and the Secure Server:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- Certificate Distribution Point (CDP)

KeyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted. If one of the bits is not set, then the connection will be disconnected:

- Digital Signature
- Key Encipherment (keytransport, key management)
- Key Agreement (key exchange process)

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then the Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

Hardware Certificate (View)

View Hardware Certificate enables you to review which values have been used to create the certificate, e.g. unique e-mail address.

General

The General display shows information about certificate user and issuer (these are identical for an Issuer Certificate), as well as the serial number, details about duration of validity, and the fingerprint.

Certification Authority (CA): The issuer of your User Certificate has to be identical with the issuer of the CA certificate. (see View Issuer Certificate).

Serial Number: The serial number of the certificate is compared with the serial number kept in the revocation list of the Certification Authority (CRL).

Validity: The validity of a certificates is limited. Normally the validity of an Issuer (Root) Certificate is longer than the validity of a hardware Certificate. When the validity expires the functionality of the certificate is also lost.

Fingerprint: = hash value. The hash value is the signature of the certificate. The hash value is encrypted with the private key of the CA.

Extensions

Certificates can contain extensions. These are used to link additional attributes with users or public keys that are required for the administration and operation of the certification hierarchy and the revocation lists. In principle, certificates can contain any number of extensions, including those that are privately defined. The certificate extensions are written into the certificate by the issuing certification authority.

Following extensions are relevant for Secure Client and the Secure Server:

- KeyUsage
- extendedKeyUsage
- subjectKeyIdentifier
- authorityKeyIdentifier
- Certificate Distribution Point (CDP)

KeyUsage

If the KeyUsage extension is contained in an incoming certificate, then it will be verified. The following KeyUsage bits are accepted:

- Digital Signature
- Key Encipherment (keytransport, key management)
- Key Agreement (key exchange process)

If one of the bits is not set, then the connection will be disconnected.

extendedKeyUsage

If the extendedKeyUsage extension is present in an incoming User Certificate, then the Secure Client checks whether the defined extended usage is "SSL Server Authentication". If the incoming certificate is not intended for server authentication, then the connection will be refused. If this extension is not present in the certificate, then this will be ignored.

Note that SSL Server Authentication is direction dependent, i.e. the initiator of tunnel establishment checks the incoming certificate of the remote party, if the extendedKeyUsage extension is present, then the intended usage must contain "SSL Server Authentication".

subjectKeyIdentifier / authorityKeyIdentifier

A key identifier is an additional ID (hash value) to the CA name on a certificate. The authoritykeyidentifier (SHA1 hash over the issuer's public key) on the incoming certificate must agree with the subjectKeyIdentifier (SHA1 hash over the public key of the owner) on the corresponding CA certificate. If no CA Certificate is found then the connection is rejected.

The keyidentifier designates the public key of the Certification Authority and in this way not only one, but a series of certificates if required. The use of the key identifier allows a greater flexibility for the determination of a certificate path. In addition, the certificates that possess the authoritykeyidentifier extension do not need to be revoked if the CA issues a new certificate when the key remains the same.

Certificate Distribution Point (CDP)

The URL for downloading a Certificate Revocation List(CRL) is stored in the CDP. If the CPD extension is contained in the certificate, then after the connection is set up, the CRL is downloaded via the specified URL and checked. If the system determines that the certificate is invalid then the connection is disconnected. In this process the CRL is stored in the %INSTALLDIR%\crls directory, under the common name of the CA.

Enter PIN

The PIN can be entered before establishing a connection but after the Monitor has been started. If a connection requiring a certificate is to be established at a later time, then the PIN entry can be omitted - unless the configuration for the certificate demands it.

If you have selected the menu item "Connection / Enter PIN", then the PIN (at least 4 digits) can be entered in the open entry field, and confirmed with "OK".

If the PIN has not been entered before connection establishment, the PIN entry dialog is started, at the latest, when the first connection requiring the use of a certificate is to be established to a destination. After that, the PIN entry can be omitted in the case of repeated manual connection establishment, if this has been configured.

If the PIN has been entered correctly, this is indicated in the monitor interface by a green PIN symbol.

A connection can only be established after correct entry of the PIN.

Safeguarding PIN Use

If you activate the function "PIN request at each connection" in the certificate configuration, then the PIN can no longer be entered via the "Enter PIN" Monitor menu option. For this reason, the menu option "Enter PIN" is automatically switched off (grayed out). This ensures that the PIN will only be queried and can only be entered directly before the connection is set-up.

Activate this function to prevent an unauthorized user from setting up an unauthorized connection when the PIN has already been entered.

Likewise, if the "Change PIN" function has been activated, the PIN that has already been requested in connection with other functions is no longer used - i.e. when setting up a connection, or in the "Enter PIN" connection menu. Instead you can always select the menu option "Change PIN" and the new PIN will be automatically reset immediately after the change.

This ensures that when configuring "PIN query at every connection set up" on an unauthorized Secure Client Monitor, a PIN entered previously by an unauthorized user cannot be used at anytime to establish a connection.

The policies for PIN entry can be specified in the main menu under "Configuration / Certificates". These policies must be observed when the PIN is changed.

Reset PIN

This menu item is active only when the PIN has been entered correctly, i. e. the certificate is used for the connection to be established.

If the PIN is reset, this certificate can no longer be used to establish a connection, until the correct PIN is entered again.

Change PIN

The PIN for a smartcard/token or for a soft certificate can be changed under the menu item "Change PIN", providing the correct PIN number has previously been entered.

Then enter your new PIN and confirm it by repeating it in the last entry field. With a click on "OK" you have changed your PIN.

PIN policies that need to be complied with are displayed under the entry field. They can be set in the main menu under "Certificate - PIN Policies".

Configuration Locks

In order to effectively set the configuration locks, identification must be entered, which consists of "User ID" and "Password". The password must be confirmed thereafter.

To set the configuration locks effectively, you must enter an ID that is made up of "User ID" and "Password". The password must then be confirmed.

Please note that identification is absolutely necessary to activate or cancel the configuration locks. If the identification is forgotten there is no possibility to cancel the locks!

Now authorization to open menu items under the main menu item, "Configuration", can be limited for the user. As default, the user can open all menu items and edit the configurations. If the check mark is removed from the respective menu item with a mouse click, then the user can no longer open this menu item.

The editing rights for the parameters in the profile settings are divided into two groups:

- General Rights
- Visible Parameter Folders

The general rights refer only to (configuration of) the profiles. If the user is "Authorized to create profiles", but he is not "Authorized to configure profiles", he can create new profiles with the assistant, subsequent modification of individual parameters, however, will no longer be possible.

The parameter folders of the profile settings can be suppressed for the user.

Please note as well that parameters of a non-visible folder cannot be configured.

Unlock Locks

This menu item will only be displayed if configuration locks have been configured by your system administrator.

Your system administrator may have purposely hidden and locked various profile parameter folders or menu items. These will no longer be visible and therefore cannot be modified under normal circumstances.

In order to display these parameters, select this menu item. After correctly entering User ID and Password, the configurations will be unlocked, and changes can now be made;

The Connection menu item changes to "Lock Configuration Locks" when the parameters are unlocked.

Exit

If the connection is already disconnected, this menu item quits the client.

To quit the Client during an existing connection, a prompt will appear. Clicking on "Yes" quits the connection and quits the client.

Clicking on "No" quits client monitor without disconnecting the current connection.

In this case you will no longer be able to see, on the desktop interface, whether the connection is already disconnected or whether a connection fee will be incurred. In such a case, the client must be restarted in order to be able to disconnect correctly.

Logbook

Automised protocolling

The log function is continuously active in the background, even if the log window is not open. All relevant communication events of the client software are shown and saved for one week per operation day, in a log file. Files older than seven online days will be automatically deleted.

This log file is generated automatically in the installation directory under "Log" when the monitor ist finished and is named NCPyymmdd.LOG (yy=year, mm=month, dd=date).

The storage time for log files can be altered under Extended Log Settings.

The log files can be opened and analyzed with a text editor.

Selected Protocols

With opened log windows the current log messages are listed and can be followed. In this way the lines of the log protocol are automatically scrolled. The protocol created from the time of the opening of the log window until its closing is saved til the next re-boot. The contents of the log window manually can also be deleted, saved or searched through for specific events.

The following comands in the footer of the log window are prepared for these functions:

Create File

When you click this button, you receive the possibility to input name and path of a file in a further window, in which the content of the log window is written (default: ncpmon.log). All transaction with the client software, such as dialing and reception, including the numbers, are automatically protocolled and written in this file until the file is closed close. When you put in a log file, you can follow the transactions with the client for a longer period.

Close File

If you click on this button, a file with the log protocol of the window content is closed and saved under a free unused name. This file can be used for analysis of the transactions with the Secure Client or for error searches.

Clear Screen

If you click on this button the window from the last protocol entries will be emptied.

Close Logbook

The log window will be closed with this, without its contents being written in a file.

Show Search

Two search functions make the search for strings and expressions in the log protocol text easier to find.

Search

The string in the input field is searched for as it is in the log book and all the contained positions marked.

With [F3] you can jump from the chronologically oldest find spot with this string to the next latest, with Shift + [F3] you can go from the latest find spot to the next oldest.

Disable Scrolling

To stop the continuous reading in of the newer log messages you can set "Disable Scrolling".

A search for more strings at the same time, is not possible.

Filter

After the string, which is input into this field, a search in the log text is carried out. Several strings can be separated or searched for at the same time, through gap characters. In the standard setting the lines with the relevant find spots are blocked out of the log protocol.

On the other hand only the lines can be shown where the filtered strings are situated.

Saving the search and filter entries

The history of the last 10 searches and filter entries will be remembered and shown in the selection list.

The maximum number of log lines, which are internally puffered is 1000 by default. This value can be changed via the NCPMON.INI.

The following values are saved in the NCPMON.INI for this function:

MaxTraceLines=1000

WholeWords=0

CaseSensitive=0

MaxSearchEntries=10

SearchEntry_X=X. Search String

MaxFilterEntries=10

FilterEntry_X=X. Filter String

Licensing

The current software version and the version of the license (if available), are shown under the menu option "Licensing".

If the software is used as a test version, then the remaining validity period is displayed.