

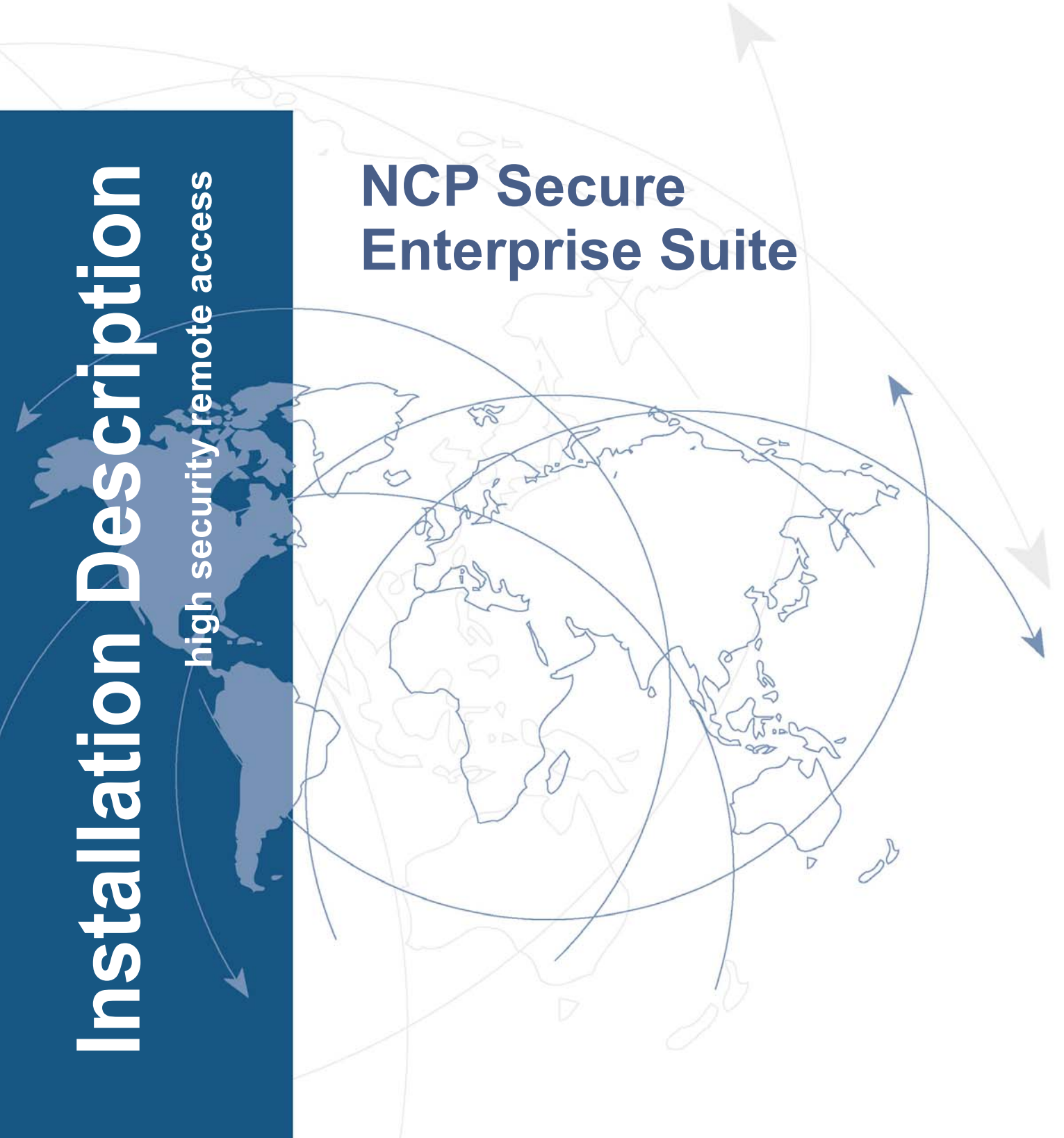


SECURE COMMUNICATIONS

Installation Description

high security remote access

NCP Secure Enterprise Suite





Copyright

Considerable care has been taken in the preparation and publication of this manual, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.

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 use for any particular purpose.

Furthermore NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and 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.

© NCP engineering GmbH,
September 2010

Network
Communications
Products engineering GmbH

GERMANY
Headquarters:
Dombühler Straße 2
D-90449 Nürnberg
Tel.: +49-911-99680
Fax: +49 - 911 - 9968 299
internet
<http://www.ncp-e.com/en>
E-mail: info@ncp-e.com

Installing the Secure Enterprise Suite



In this document you will find in addition to the installation description a brief product description. Furthermore special possibilities of installation and licensing procedure are explained.

Overview of Contents

- **Product Description**
- **Notes for Installing**
- **Communication Media**
- **Automatic Media Detection**
- **Prerequisites for using Certificates**
- **Default Installation**
- **Assistant for initial Configuration**
- **Secure Client Programs**
- **Dynamic Personal Firewall**
- **Licensing**
- **Testing the Client**
- **Extended Installation**
- **Deinstallation**



Further descriptions of profile settings and IPSec configurations you will find in the documents **Secure Client Monitor** and **Secure Client Parameters**.



The easiest way to receive the desired information is via the **Suite Navigator**. All available documents about your product are recorded in this pdf file.

Starting from navigator, you can jump directly into all relevant documents and download them from the NCP homepage in case they are not yet saved in your navigator directory.

Product Description



For a trial period, the NCP Secure Enterprise client may either be installed as **NCP Dynamic Personal Firewall** or as **NCP Secure Enterprise Client**. After choosing either option, the full software is installed on the computer. Please note, that the Dynamic Personal Firewall does not offer a VPN feature.

After the trial period, the product variant installed may be purchased and licensed. Its features are specified by the license key purchased.

Secure Enterprise Client

The NCP Secure Enterprise Client offers all features available. All modules are displayed in the **Options** menu item of the “view” menu. If need be, they can be displayed or hidden:

- Dialer for Internet Connections (additional external dialer)
- Wi-Fi (including Hotspot Logon)
- EAP (Extended Authentication in LAN / Wi-Fi)
- Firewall (Personal Firewall)
- VPN (security modes IPsec and L2sec, PKI support, automatic media detection, LAN over IP)

The NCP Secure Enterprise Client is a component of the holistic NCP Secure Enterprise Solution. This communication software serves universal teleworking in any remote access VPN environment. On the basis of IPsec standards, highly secure data connections may be established to either NCP Secure Enterprise Server or to VPN gateways of all renowned producers. Any network may be used for data transfer - i.e. the conventional telephone network, public Wi-Fi networks, LANs (e.g. the corporate network), the internet as well as narrowcasting networks like Wi-Fi networks within the corporate headquarters or at hotspots. Teleworker may use any device on any location to access the central data network or any application.

Universal application possibilities demand comprehensive security mechanisms in order to combat attacks in any remote access environment and at hotspots during logon and logoff. Apart from VPN tunneling the most important integrated security components are: data encryption, a **dynamic personal firewall**, OTP (one time password) token support and certificates within a PKI (public key infrastructure). Via the personal firewall, firewall rules and applications may be defined for: ports, IP addresses and segments. A further security component is friendly net detection, i.e. the software automatically recognizes secure and insecure networks. Depending on this the applying firewall rules are activated or deactivated.

The administrator may centrally set all configuration parameter so that they may not be altered by the user. Mechanisms of the central management (**Secure Enterprise Management**) allow for automatic transfer of all configuration parameter to the client. Furthermore the NCP dialer offers protection from costly external dialers.

Stationary PC and mobile PC workstations are integrated as equal participants in the corporate network over public networks (via Internet) and beyond. Teleworkers work in their accustomed manner as they do at office workstations. All LAN applications and resources are available to them 1:1 on their remote PC.

The software works on the principle of LAN emulation, i.e. the software appears to the PC operating system as a LAN adapter (virtual network adapter). Consequently it is possible to assign the remote client a private IP address from the central Secure Enterprise Gateway, (among other things). This private IP address can be assigned either permanently or variably (dynamically) from an address pool, as required. If needed the client can retain a one-time assigned IP address, even in manual connection mode, in spite of physical connection clearing (e.g. with Short Hold Mode). This means that the logical connection between remote client and central resource remains intact. Even accessing networks in different local area networks poses no problem, in spite of changing IP addresses. The remote user can always be identified with the same name in the corporate network, wherever he is located. Integration in a DDNS (Dynamic Domain Name Service-Protocol) structure is also possible. Optionally the connection to the central server and connection monitoring are automated unnoticed in the background of the user's activities.

The NCP Secure Client Software supports the routable protocols TCP/IP and IPX/SPX. The Client Software for ISDN has been tested with the D-Channel protocol DSS1. However, other D-Channel protocols like VN3/4, NT1, CT1, 5ESS, Austel, etc. are supported as well.



The current version and future versions of the Secure Client will only be tested for the Windows systems Windows XP, Windows Vista and Windows 7. The full functionality of the client software under Windows 2000, Windows NT or Windows 98/95 cannot be guaranteed.

The NCP Secure Communication solution guarantees that a teleworkstation cannot be attacked from the Internet, nor from other LAN participants (at hotspots for instance), through the Personal Firewall, which comes standard with the product.

Dynamic Personal Firewall

Users, who want to benefit from the advantages of a centrally administrable firewall including friendly net detection but do not need the VPN feature, are now able to install this module.



Via the personal firewall, firewall rules and applications may be defined for: ports, IP addresses and segments. A further security component is **friendly net detection**, i.e. the software automatically recognizes secure and insecure networks. Depending on this the applying firewall rules are activated or deactivated.

At first the licensed Dynamic Personal Firewall only appears as tray icon. The monitor has to be opened via the menu of the firewall in the tray icon. Only then, the features of the firewall are displayed in the view menu, where the features may also be displayed or hidden:

- Dialer for Internet Connections (additional external dialer)
- Wi-Fi (including Hotspot Logon)
- EAP (Extended Authentication in LAN / Wi-Fi)
- Firewall (Personal Firewall)

The NCP Dynamic Personal Firewall comprises all features of the software, except for the VPN feature. Like the Secure Enterprise Client, it is centrally administrable via the Secure Enterprise Management.

At a later point in time, an upgrade to the Secure Enterprise Client is still possible with the respective license key.

Secure Enterprise Management

NCP Secure Enterprise Management offers a seamless range of functionality. Maximum transparency for network administration and minimization of total cost of ownership are guaranteed.

Secure Enterprise Solution



For further information please consult the NCP web site: <http://www.ncp-e.com>

Notes for Installing

The actual version and further versions of the Secure Client will only be tested for the operation systems Windows XP, Windows Vista and Windows 7. The full functionality of the client software under Windows NT or former versions can not be guaranteed.

A setup program performs the installation of the client software quickly and smoothly. The installation procedures for all versions of NCP Client Software are the same. The following text describes the procedures for installing the client software under Windows Vista.

Prior to executing setup be sure that the following prerequisites are fulfilled.

Starting with version 8.31 the client will be installed in the program directory of the operating system (programs\NCP\SecureClient) for a new installation.

Old Path: %Windows%\ncple

New Path: %Programme%\NCP\SecureClient

For an update in addition the path is used that was entered for the last installation.

Registry Repair (RegRep)

The setup program checks the registry entries for each new installation of the client, i.e. even when an older version was uninstalled. If problematic entries are found then they will be adjusted. The setup programme will generate a message to request a restart of the PC.

Prerequisites for Installation

Operating System

In order to be able to communicate with the Client Software it is essential to have either Microsoft Windows XP, Windows Vista or Windows 7 installed on your PC (minimum of 128 MR RAM).

Remote Destination

In order to communicate with the remote destination it must support one of the following media types: ISDN, PSTN (analog modem), GSM, GPRS/UMTS, LAN over IP, Wi-Fi or PPP over Ethernet (PPPoE). (One of the following communication media has to be set in any profile of the Secure Client. Per mouse click on one of the boldly printed red terms, you jump to the respectively given configuration description of the documents **Client-Parameters** or **Mobile-Computing**.)

Secure Client

One of the following communication devices must be properly installed.

ISDN adapter (ISDN)

The device (e.g. adapter internal or external) must support the ISDN CAPI 2.0 standard. When using **PPP Multilink** the software can bundle up to 8 ISDN B-Channels. Any **ISDN** device supporting the ISDN CAPI 2.0 can be used. Please check your device to be sure that such a driver is available. The Client Software does not support TAPI based ISDN devices.

Analog Modem (Modem)

The Client Software can communicate with any industry standard analogue PC **Modem**, provided that it and the modem drivers have been properly installed and the Modem Init. String and the COM-Port definition for the modem is correct. The modem has to support Hayes AT commands.

Mobile telephones can also be used for data communication, after the associated software has been installed that presents itself to the client precisely as if it were an analog modem. The serial interface, IR (infrared) interface, or Bluetooth can be used as interface between mobile phone and PC. The opposite side must have the appropriate dial-in platform

depending on the transfer rate (GSM, v.110, GPRS or HSCSD). The initialization string in the Secure Client modem configuration must be obtained from the ISP or the manufacturer of the mobile phone.

LAN adapter (LAN over IP)

When the Link Type **LAN (over IP)** has been defined the Client Software may be used as a VPN Client in a LAN that communicates across a LAN Network and associated Router to a central site VPN Gateway. When defined as a LAN Client, the Client Software can also be used as a VPN or VPN/PKI Plug-in for Microsoft's RAS (Dial-Up Network) client.

Adapters for a wireless LAN (Wi-Fi adapter) are handled exactly like normal LAN adapters.

Broadband Device (xDSL (PPPoE))

Cable Modems, Splitters (e.g. for ADSL), etc. can be used in conjunction with **PPP over Ethernet** (PPPoE), which is supported by the Client Software. This may be useful for xDSL or other broadband services that employ time based charges.

xDSL (AVM - PPP over CAPI)

The link type **AVM - PPP over CAPI** has been added in the "Basic Settings" configuration field in the telephone book. If an AVM Fritz DSL card is to be used then this link type may be selected. AVM specific init strings may be entered in the field "Destination Phone Number" ("Dial-Up Network" group) for the connection. It is recommended to use the standard setting "xDSL (PPPoE)" with Windows operating systems as this provides direct communication over the network interfaces. No additional network card is necessary with the AVM Fritz! DSL card.

3G Card

If you are using a **3G Card**, special features of the mobile computing can be used depending on the card characteristics. Due to the direct support of the multi-function card for UMTS / GPRS / Wi-Fi through the Secure Client, installation of management software from the card implemented, is not necessary.

On the basis of the end-to-end security principle, the NCP Secure Client unites all mechanisms of communication and security technology for efficient data communication. The client monitor pro-

vides optical displays of the connection states, the field strength, the selected network and the provider.

From version 9.02 build 5 the Secure Client supports new PCMCIA cards, after importing the file g3detect.dll. For further information on the PCMCIA cards supported please refer to: <http://www.ncp-e.com/en/support/compatibility/umts-3g-hardware.html>

Wi-Fi adapter (Wi-Fi)

The **Wi-Fi** adapter can be operated with the link type “Wi-Fi”. In the monitor menu the special “Wi-Fi settings” menu item is displayed where the access data for the wireless network can be saved in a profile. If this “Wi-Fi configuration” is activated, then the management tool of the Wi-Fi card, or the Microsoft tool must be deactivated. (Alternatively the management tool of the Wi-Fi card or the Microsoft tool can be used as well.)

If the link type Wi-Fi is set for the destination system in the phonebook, then under the graphic field of the Client Monitor an additional area is shown where the field strength and the Wi-Fi network are displayed.

Please note for configuring the Wi-Fi settings the description **Mobile Computing**.

Automatic Media Detection

Automatic Media Detection may only be used if alternative communication media are available.

If different communication media are used alternately, for example, LAN or Wi-Fi (within the corporate network) or modem and ISDN (during remote access), manual selection of the profile with the respective communication medium is rendered superfluous, provided the profile with communication medium LAN has been changed to a profile with automatic media detection and a profile for each alternatively available communication medium like modem, ISDN, DSL or GPRS/3G is available.

For configuration, please refer to the explanation in the PDF **Enterprise Client Parameter**.

Prerequisites for using Certificates



If certificates should be used for extended authentication please note the document **Secure Client Certificates**.

Supported Interfaces and Formats

The secure client can be used in public key infrastructures as of **X.509. V.3** standard. Additionally the Entrust Ready functionality has been granted for the Enterprise version. Thus the client supports all the important guidelines from Entrust relative to the implementation of certificates and their use. (See the description **Entrust-Ready**).

The secure client supports the following interfaces/formats:

- Smartcards, USB-Tokens: PKCS#11, TCOS 1.2 and 2.0, CSP
- Soft Certificates: **PKCS#12-File**
- PC/SC conform **Chipcard Reader**: The client software supports all chip card readers which conform with PC/SC. The chip card readers are included in a list of the client once the reader is connected and the corresponding driver software has been installed.

– **Automatic Recognition of connected PC/SC Readers**: If the use of a PC/SC chip card reader is configured on the client for the PKI environment, the client recognizes and automatically uses the connected one.

This automatically simplifies profile creation within the Enterprise Management System, since no user specific chip card readers have to pre-configured in the central certificate configuration.

If a user receives a configuration without entry for the chip card reader from the Management System and if a certificate is pre-configured, then the client automatically reads the data of the PC/SC reader which is installed on the user PC and uses this reader.

This feature can only be used in connection with smartcards which can be addressed directly without interface software such as NetKey chip cards (Telesec).

- **PKCS#11-Module**: Drivers in form of a PKCS#11 library (DLL) are supplied with the software for smartcards or tokens. This driver software has to be installed initially.

Then the relevant PKSC#11 module can be selected via an assistant.

CA Certificates

The administrator of the company network determines which certificate issuers can be trusted. This happens by applying the CA certificate of his choice into the installation directory under <CA-CERTS>. The application can happen automatically during software distribution if the issuer certificates are located in the directory <DISK1> during software installation from a data carrier. (See **Extended Installation**)

Retrospectively, issuer certificates can be distributed automatically via the Secure Management Server (only to Enterprise Clients) or the user can save them himself as long as he has the relevant write permissions in the relevant directory.

Currently the formats *.pem and *.crt are supported for issuer certificates. They can be viewed in the monitor under the main menu item “Connection / Certificates / **Display CA Certificates**”.

If the secure client receives the certificate of a remote station, then the NCP client will determine the issuer by searching the issuer certificate initially on smartcard or USB token or in the PKCS#12 file and finally in the installation directory under <CACERTS>. If the issuer certificate cannot be found then the connection will not be successful. If no issuer certificates are available, then no connection is allowed.

If Soft Certificates are created with the PKI plug-in of the management server then the issuer certificate is saved in the PKCS#12 file.

Use of a Revocation List (CRL)

The secure client can have access to the corresponding CRL (certificate revocation list) for each issuer certificate. It is applied to the installation directory under <CRLS>. If a CRL is available, then the secure client checks incoming certificates against the CRL. The client downloads the corresponding CRL automatically if the incoming server user certificate includes the **certificate extension CDP**.

Default Installation

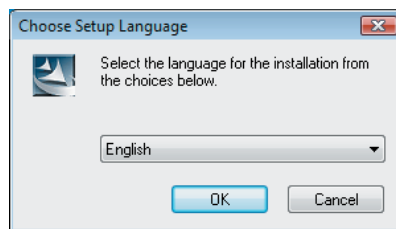
You can obtain the software as ZIP file by downloading it from the website under www.ncp-e.com.

Installing the software after a download as a test version, first you extract the ZIP file. Extracting the data the directory <Disk1> will be made automatically.

Start the installation under the Windows Explorer bei executing setup.exe in the directory <Disk1>.

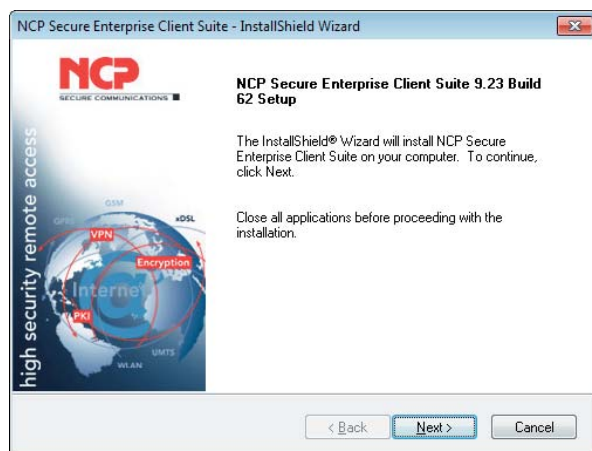
Choosing the Setup Language

In the following window you can “Choose Setup Language”. After selecting the language click on “OK”.



The “Install Shield Assistant” is now started. It will guide you through the installation.

Read the terms of the Welcome window carefully and click on “Next” (illustration below).



Please deactivate any VPN client or personal firewall of another producer to avoid instability and data loss.

The next window displays the Software Licensed Agreement. In order to proceed with the installation of the licensed version click on “Yes”. Clicking “No” will stop the installation process.

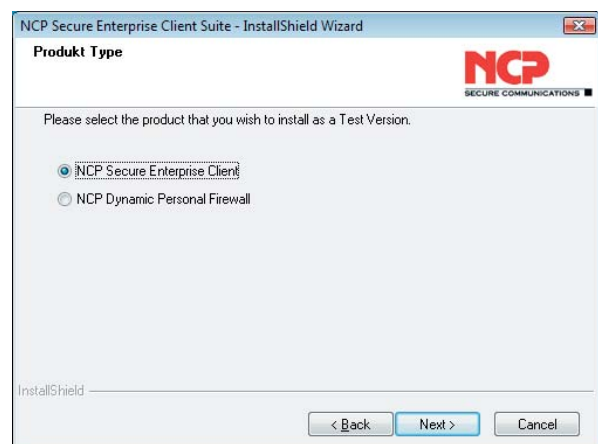


Testversion

If you are not in possession of an Authorized Client Software License, select in this window install as a test version. (If you install the the free 30 day limited test version, it is valid only for a period of 30 days from the day of installation. Thereafter it cannot be used.)

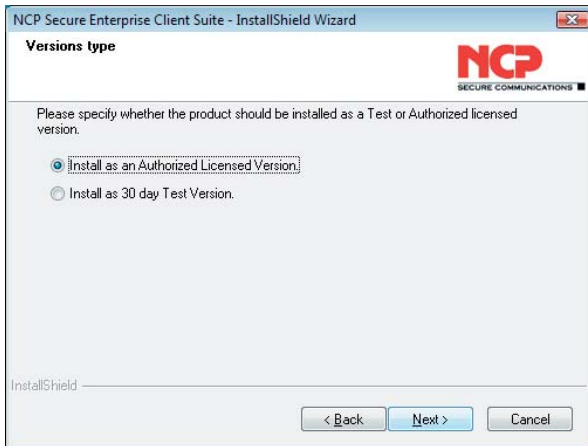


The NCP Enterprise Suite can be installed as **NCP Secure Enterprise Client** **NCP Dynamic Personal Firewall** or (illustration below).



Licensing

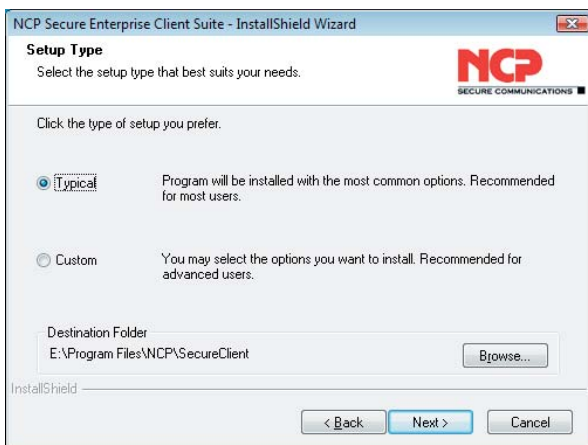
If you are in possession of a license, select in this window “Install as Authorized Licensed Version” and click on “Next”.



Enter the serial number of your software license and the activation key in the appropriate fields when prompted to do so. (Please refer the bill of delivery.) Upon entering these codes correctly, the “Next” button will be activated. By clicking on “Next” the Client Software will be activated as an authorized license version.

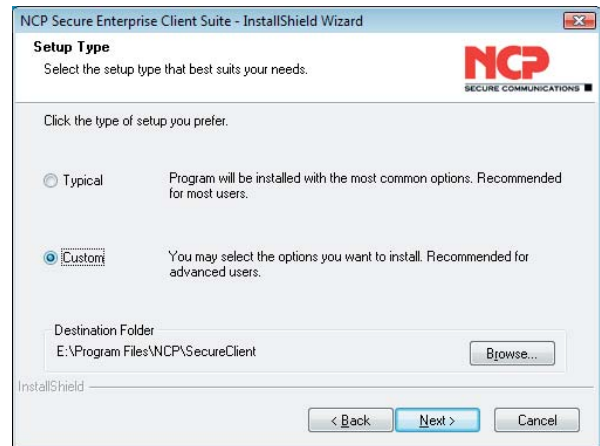


If you select “Standard Installation” in the following window the installation will continue automatically and the setup is finished.



Customized Installation

Selecting the “Custom” installation you can define settings according to your requirements.

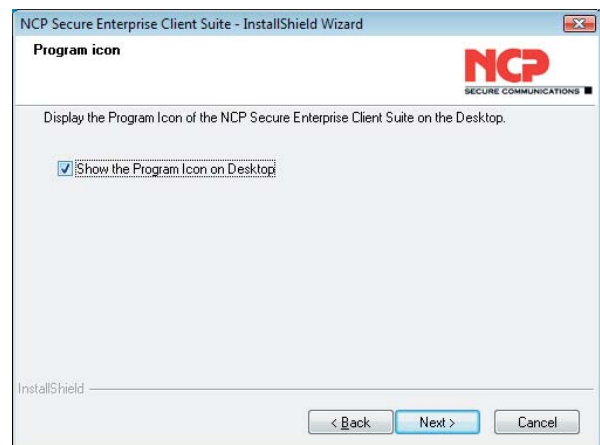


Independently of “Typical” or “Custom” installation you can select any folder for the software installation by clicking on “Browse” (illustration above). This is particularly important if the user should have no rights on the system root directory. Default: %Programme%\NCP\SecureClient.

In the following window of the “Custom” Installation you define the program folder for the client software. (Default: “NCP Secure Client”).

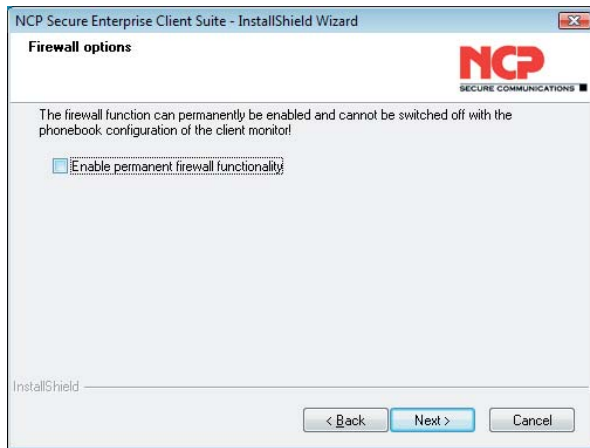


You can define whether the program icon should be displayed on the desktop.



Firewall Option for the Enterprise Client

Only the user defined installation of the Enterprise Client allows for the firewall function to be activated permanently so that only communication within a tunnel is possible.



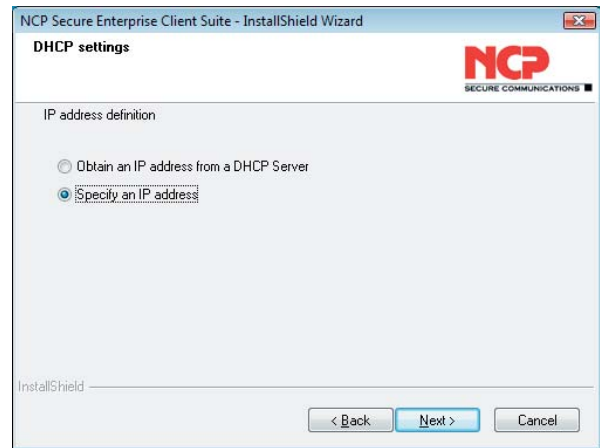
If this is set during installation, it is in effect for all profiles and even if the client has been stopped. The function **Keep Firewall active after Client has been terminated** cannot be switched off.



It is only possible to deactivate the firewall if the client software is deinstalled and then reinstalled.

Further customized Settings

It is necessary to contact your administrator or Internet service provider for more information about other settings relative to your communication gateway.



Communication with DHCP (Dynamic Host Control Protocol) means that a temporary IP Address will be assigned automatically for each communication session. If required, click on “Obtain an IP Address from DHCP Server”.

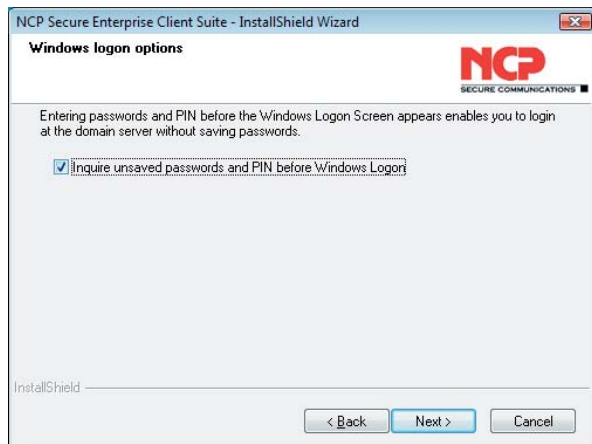
If you “Specify an IP Address”, enter the IP address in the next window (below).



Default Gateway: If a network adapter with a Default Gateway is already installed, you will have to delete this Default Gateway Address. It is not possible to have more than one network adapter with a Default Gateway. **DNS Address:** You should only enter a DNS Address if you have been assigned one from your system administrator or ISP.

Windows Logon Options

After that you can decide whether a logon to a remote domain should occur after establishing a connection to the VPN Gateway.



Afterwards you may decide if there is to be a connection establishment to the VPN gateway of a remote domain prior to windows logon. For this connection set-up it may be required to enter your certificate PIN and the client software password (not saved). After connection to the gateway has been established, logon to the remote domain is possible. The logon is already carried out encrypted via the VPN tunnel.



If you activate the request prior to windows logon, the logon option (Gina / credential) is installed automatically. The configuration menu of the client monitor allows you to set the parameters required.

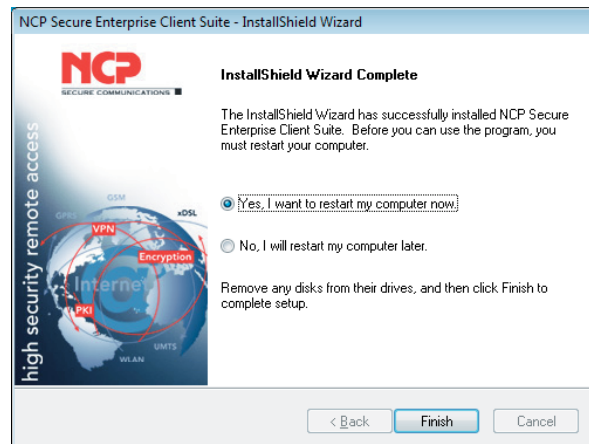


If the logon option is not activated but is to be used at a later point of time, it may be installed using the command

```
rwscmd /ginainstall
```

Finish Setup

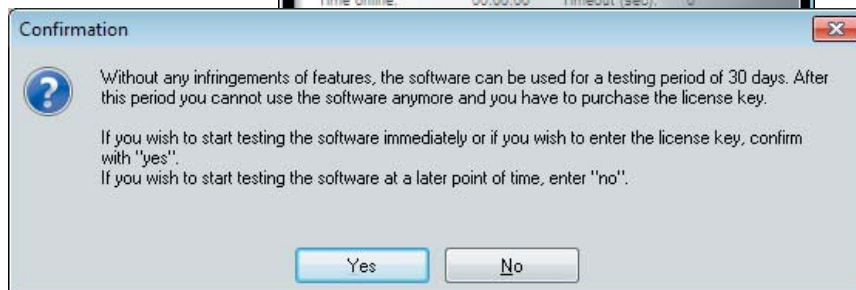
After all data necessary has been imported and the program group has been set-up, click on finish in order to finish setup.



First Start of a Test Version



If you have installed a test version (see above), you will receive a confirmation window after the first start of the client monitor (illustration below). This confirmation window offers to start testing the software immediately or at a later point of time.



If you start the test period, the free 30 day limited test version is valid for 30 days from the day of starting. Thereafter it cannot be used.

Initial Configuration Assistant

Once you have installed the client software and re-booted your PC, the client monitor will be automatically displayed on your PC. The “Initial Configuration Assistant” will also be displayed, provided that you have installed the client software for the first time on your PC and that no previous profile setting exists from an earlier client software. They are located in the installation directory.



The “Initial Configuration Assistant” offers the ability to define Test Connections. Using this offer the assistant will guide you through the definition of generic parameters (e.g. Link Type) and creates by using your data a profile in the profile settings.

When using one of the four profiles created with the aid of the “Initial Configuration Assistant”, the access data described under “Testing the Client”, will be applied. You can also use these entries later for further test purposes.

If you do not use the assistant for creating such test profiles, then no entries will be added. In this case you will have to create your own profile settings, as described under **Client Monitor**.

Secure Client Programs

If the Secure Client has been installed then you will find two programs in the Windows program group that you specified at installation:

Secure Client Monitor

Secure Client Tracer



If no **Program Icon** is displayed on the desktop you can start the Secure Client by clicking the menu item **Secure Client Monitor**. (See **Client Monitor**).

The **Secure Client Tracer** is a small autonomous application program that is used by qualified system technicians. It can be used to create traces for troubleshooting purposes.

Dynamic Personal Firewall

At first, the dynamic personal firewall is only displayed as tray icon. The monitor has to be specifically activated via the firewall menu of the tray icon. Afterwards the features of the firewall may be displayed via the view menu. Please also refer to the PDF **Enterprise Client Firewall and FND**.

Licensing

The software version implemented, and possibly the licensed version with serial number, are shown under the menu option “Licensing”.



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

In order to use a valid full version that is not subject to time restrictions, the software must be released with the license key and serial number received.

The licensing process for the software requires your acceptance of the license conditions; these conditions can be viewed via mouse click.

License key and serial number can be entered after you have clicked on the licensing button.

Later the correctly entered license data is no longer displayed at this point (see above **Licensing**).

Testing the Client

The program group “NCP Secure Client” was created in the Start menu during the installation. Now start the “Client Monitor” program from the “NCP Secure Client” program group. The client profile settings contain pre-configured destination systems for test purposes:

Test Connection IPSec native

Test Connection IPSec über L2TP

Test Connection L2Sec

Test Connection L2TP

An “X.509 soft certificate” is also included for test purposes. It is stored as a PKCS#12 file under `x:\windows\ncple`. The file name is “user1.p12” and the PIN is “1234”. This certificate can be used to test extended authentication. Using preshared key “shared secret” is preconfigured.

Test Connection IPSec native (over LAN)

```
Gateway (Tunnel Endpoint):
vpntest.ncp-e.com
VPN Protocol               : IPSec
XAUTH User ID              : ncpipsecnative
XAUTH Password             : ncpipsecnative
pre-shared key             : shared secret
```

Test Connection IPSec over L2TP

```
Gateway (Tunnel Endpoint):
vpntest.ncp-e.com
VPN Protocol               : L2TP
User ID (VPN)              : ncpuseripsec
Password (VPN)             : ncpuseripsec
Tunnel Secret              : secret
Security Mode              : IPSec
Static Key:
00.11.22.33.44.55.66.77.88.
99.AA.BB.CC.DD.EE.FF
IKE Policy                  : Pre-Shared Key
IPSec Policy                : ESP 3DES-BF-MD5
Exchange Mode              : Main Mode
```

Test Connection L2Sec

(tests SSL Encryption with Certificate)

```
Gateway (Tunnel Endpoint):
vpntest.ncp-e.com
VPN Protocol               : L2TP
User ID (VPN)              : ncpuserssl
Password (VPN)             : ncpuserssl
Tunnel Secret              : secret
Encryption                  : SSL with Certificate
The last two items can be entered in the
"Connection" pull-down menu in the Client
Software Monitor under "Certificates /
Configuration"!
```

Test Connection L2TP

```
Gateway (Tunnel Endpoint):
vpntest.ncp-e.com
VPN Protocol               : L2TP
XAUTH User ID              : ncpuserl2tp
XAUTH Password             : ncpuserl2tp
Tunnel Secret              : secret
```


Testing with Ping

You can “ping” the IP Address 172.16.12.100 via the existing VPN tunnel link. Proceed by the entering the following command at the DOS prompt:

```
C:\>ping 172.16.12.100 (<ENTER>)
```

Upon successful pinging your reply will look something like this:

```
Reply from 172.16.12.100: bytes=32 time=109ms TTL=128
Reply from 172.16.12.100: bytes=32 time=96ms TTL=128
Reply from 172.16.12.100: bytes=32 time=82ms TTL=128
Reply from 172.16.12.100: bytes=32 time=69ms TTL=128
The monitor displays the amount of data sent (Tx) and received (Rx) Bytes.
```

Testing FTP Access

You can also make a test connection to FTP Server via the existing VPN tunnel link.

Your access data :

```
IP Address      : 172.16.12.100
User           : anonymous
```

Proceed by the entering the following command at the DOS prompt:

```
C:\>ftp 172.16.12.100
Connection with 172.16.12.100
220 (vsFTPd 2.0.4)
User (172.16.12.100:(none)): anonymous
230 Login successful
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
SecEntryCl_Linux_de.pdf
SecEntryCl_WinCe_de.pdf
SecEntryCl_WinCe_en.pdf
SecEntryCl_Win_de.pdf
SecEntryCl_Win_en.pdf
226 Directory send OK.
FTP: 64d Bytes received in 0,00Secounds 407000,00KB/s
ftp> close
ftp> quit
```

Testing Web Browser Functionality

You can also make a test connection to the Web via the existing VPN tunnel link by entering 172.16.12.100 in your Web Browser. This should connect you to NCP’s Web Site.

Extended Installation

The following possibility has been provided to automatically install additional user-specific files for certain users, or a user group, during the installation of the client software.

If the following subdirectories are created under the "DISK1" directory (or on disk1) then all files found therein will automatically be copied along with the setup of the software:

```
Disk1\ncple      -> <Installation Directory>
Disk1\system      -> SYSTEM / SYSTEM32 - Directory
Disk1\CaCerts    -> <Installation Directory>\CaCerts
```

Please note that these files are only copied after the system files of the software, so that the original system files are written over if the names are the same.

Please note as well that a version can be counterfeited when using this method so that correct support can no longer be insured.

Uninstalling

If you uninstalled the client, then you have the option to keep the configuration and profile settings in the client directory. If at a later date, a newer client version is installed in the same directory, then all personal data can be used again. If you want to delete the personal data in the client then you will have to confirm this specifically. In such a case all data and directories of the client are removed irretrievably. (Illustration below)

