NCP Secure Entry Client (Win32/64)
Readme

Installation Instructions

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.

Prior to executing installation, make sure that the following prerequisites are fulfilled.

System Requirements (Windows)

Release Notes

Prior to executing installation, notice the Release Notes.

Remote Gateway

The remote gateway has to support one of the following communication media: ISDN, PSTN (analog modem), Mobile Network, LAN over IP, Wi-Fi or DSL.

License Key from Version 10.10

Software Updates and License Keys

From the current software version, every new major release will require a specific license key for the same version.

If the software is updated without performing a license update, the client will receive a license for the remainder of the 30-day trial period.

New Installation and License Keys

For a new installation, the client software is installed under the Program Files directory (previously Program Files (x86)) and licensed as a trial version (for a maximum of 30 days) until a valid license is entered.

Operating System

You can install the software on a computer (with a minimum of 128 MB RAM) and the Microsoft Windows Vista, Windows 7, Windows 8.x or Windows 10 operating systems.

Communication interface at the Client PC

The following paragraph shows the interfaces and communication media, supported by the Client. One of these interfaces or communication media has to be set per profile of the remote side of the Client:
– ISDN Adapter (ISDN)
– Analog Modem (Modem)
– LAN Adapter (LAN over IP)
– Broadband Device (xDSL, PPPoE)
– Mobile Network Card (GPRS / UMTS / HSDPA / HSUPA)
– WI-FI Adapter (WLAN)

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

Prerequisite for Using Certificates

The administrator of your company network is in responsible for your use of certificates and their use in a PKI environment. The online help provides you with a description of their use.

Installing the Software

MSI Installer – Updating to NCP Secure Entry Client Version 10.00

NCP Secure Client version 10.00 software is distributed in the Microsoft .msi format.

All NCP Secure Entry Client software versions earlier than 10.00, must first be de-installed using the Microsoft "Programs and Features" functions. Then the new software can be installed from the .msi package; existing profiles can be preserved across the update. Subsequent updates can be applied, when available, using the MSI Update feature.

Default Installation

Unzip the downloaded zip file and start the installation from Windows Explorer by opening the EXE file for the correct the product version:
NCP_EntryCl_Windows_x86-64_xxxx_yyyy (NCP Secure Entry Client for Windows 64 Bit)
NCP_EntryCl_Windows_x86_xxxx_yyyy (NCP Secure Entry Client for Windows 32 Bit)

(xxxx = number of the current version, for example 10.11; yyyy = revision number)

In the following window you can select the setup language. After clicking “OK” the setup program prepares the Install Shield Wizard, which continues the installation.

Please read the instructions in the Welcome window and follow the instructions of the installation wizard.

You must accept the license agreement with "yes" or the installation will be terminated.

(Custom installation offers two options: an option to select the installation directory (the default is "NCP Secure Client") and an option to display the program icon on the desktop.)

After finishing the installation, the system must be restarted. After the device is restarted, the NCP client monitor is started automatically and you will asked whether you would like to begin a trial of the NCP Secure Client.

Trialversion

If you choose to begin a trial, the trial license is valid for 30 days following the installation of the application and cannot be used after this point. When you start the trial, two VPN profiles are created for test connections, one for IPsec with IKEv1 and the other with IKEv2. Both use a test certificate which has the PIN 1234.

Licensing

If you are in possession of a license, enter the serial number of your software license and the activation key in the monitor menu “Help / Licensing”. Alternatively a NCP Volume Licens Server (VLS) can be used.

Wizard for New VPN Profile

With the Configuration Wizard connections can be quickly made to the company network or the Internet depending on the required VPN transmission protocol. After choosing the basic settings by answering a few simple configuration questions, the VPN profile is created in the list of available VPN profiles. The following data are required for configuration.

Connection to the corporate network via IPsec:
→ Profile Name
→ Communication Medium
→ Access data for Internet Service Provider (User ID, Password, Phone Number)
→ VPN-Gateway selection (VPN Gateway, Tunnelsecret)
→ Certificate use
→ Access data for VPN Gateway (VPN User ID, VPN Password)
→ Static key (Preshared Key) as long as no certificate is used (IKE ID Type, IKE ID)

Establish connection with the Internet:
→ Profile Name
→ Communication Medium
→ Access data for Internet Service Providers (User ID, Password, Phone Number)

Alternatively an already existing VPN profile can be imported. Following formats are supported:
*.ini; *.pcf; *.wgx; *.wgc

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 IKEv1"
"Test Connection IPsec IKEv2"

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 "client1.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 IKEv1

Access Data:
Tunnel Endpoint (Dest.) : vpntest.ncp-e.com
VPN Protocol : IPsec
XAUTH User ID : ncpipsecnative
XAUTH Password : ncpipsecnative
Authentication : Certificate; Standard Configuration (client1.p12)

Test Connection IPsec IKEv2

Access Data:
Tunnel Endpoint (Dest.) : vpntest.ncp-e.com
VPN Protocol : IPsec
XAUTH User ID : ncpipsecnative
XAUTH Password : ncpipsecnative
Authentication : Certificate; Standard Configuration (client1.p12)

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 0,00 Secounds 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.

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.

NCP engineering GmbH, September 2016

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299