NCP Secure Entry Client (Win32/64)
Liesmich

Installationsanweisungen

Die Installation der Software für Windows-Systeme erfolgt komfortabel über Setup. Der Installationsablauf ist für alle Versionen des Clients identisch.

Bevor Sie die Software installieren, müssen die folgenden Installationsvoraussetzungen erfüllt sein.

Systemvoraussetzungen (Windows)

Release Notes

Bevor Sie die Software installieren, beachten Sie bitte die beiliegenden Release Notes.

Gegenstelle

Die Gegenstelle muss eines der folgenden Verbindungsmedien unterstützen: ISDN, PSTN (analoges Modem), Mobilfunknetz, LAN over IP, WLAN oder DSL.

Lizenzschlüssel ab Version 10.10

Software Update und Lizenzschlüssel

Ab der aktuellen Software-Version benötigt jedes zukünftige Major Release der Software einen neuen Lizenzschlüssel gleicher Version.

Erfolgt das Software Update ohne nachfolgendes Lizenz Update so kann der Client nur für die Restlaufzeit der 30-Tage-Testversion bis zum Erhalt der neuen Lizenz für die neue Version betrieben werden.

Neue Installation und Lizenzschlüssel

Bei Neu-Installationen wird die Client Software standardmäßig im Verzeichnis „Programme“ (vorher „Programme (x86)“) installiert und als Testversion (max. 30 Tage) bis zur Eingabe der passenden Lizenz für die neue Version betrieben.

Betriebssystem

Die Software kann auf Computern (min. 128 MB RAM) mit den Betriebssystemen Microsoft Windows Vista, Windows 7, Windows 8.x oder Windows 10 (32 oder 64 Bit) installiert werden.

Kommunikationsschnittstelle am Client

Im folgenden sind die vom Client unterstützten Schnittstellen und Verbindungsmedien aufgeführt, wovon jeweils eines pro Profil der Gegenstelle am Client eingestellt sein muss:
– ISDN-Adapter (ISDN)
– Analoges Modem (Modem)
– LAN-Adapter (LAN over IP)
– DSL (xDSL, PPPoE)
– Mobilfunkkarte (GPRS / UMTS / HSDPA / HSUPA)
– WLAN-Adapter (WLAN)

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Voraussetzungen für Zertifikatsverwendung

Der Administrator des Firmennetzes sorgt dafür, dass Sie Zertifikate in einem PKI-Umfeld einsetzen können. Die Online-Hilfe listet für den Secure Client die Einsatzmöglichkeiten von Zertifikaten auf.

Installation der Software

MSI-Installer – Update auf die NCP Secure Entry Client Version 10.00

Der NCP Secure Client wird ab Version 10.00 im Microsoft-Format MSI ausgeliefert.

Software-Versionen des NCP Secure Entry Clients kleiner als 10.00 müssen über Microsoft „Programme und Eigenschaften“ deinstalliert werden. Anschließend kann die neue Software mittels MSI-Installer eingespielt werden, wobei bereits existierende Profile übernommen werden können. Im Weiteren können neue Versionen via MSI-Update-Funktionalität eingespielt werden.

Standard-Installation

Entpacken Sie die heruntergeladene ZIP-Datei und starten Sie die Installation unter dem Windows Explorer mit Aufruf der EXE-Datei, die die Produktversion bezeichnet:
NCP_EntryCl_Windows_x86-64_xxxx_yyyy (NCP Secure Entry Client für Windows 64 Bit)
NCP_EntryCl_Windows_x86_xxxx_yyyy (NCP Secure Entry Client für Windows 32 Bit)

(xxxx = Nummer der aktuellen Version, z.B. 10.11; yyyy = Nummer der Revision)

Im folgenden Fenster können Sie die Setup-Sprache auswählen. Nach Klicken auf „OK” bereitet das Setup-Programm den Install-Shield Assistenten vor, mit dessen Hilfe die Installation fortgesetzt wird.

Lesen Sie bitte die Hinweise im Willkommen-Fenster und folgen Sie den Anweisungen des Installationsassistenten.

Wenn die Lizenzbedingungen gezeigt werden, stimmen Sie dem Vertag mit „Ja” zu, da sonst die Installation abgebrochen wird.

(Eine „Benutzerdefinierte Installation“ bietet zwei Optionen an: die Wahl eines beliebigen Installationsverzeichnisses (Standard ist „NCP Secure Client”) und die Möglichkeit das Programm-Icon auf dem Desktop anzeigen zu lassen oder nicht.)

Nach Durchführung der Installationsschritte muss das System neu gestartet werden. Nach diesem Reboot wird der Client-Monitor automatisch gestartet und in einem Dialogfenster gefragt, ob die Testversion des Secure Clients gestartet werden soll.

Testversion

Starten Sie die Testversion, so ist diese vom Zeitpunkt der Installation für 30 Tage gültig und kann danach nicht mehr genutzt werden. Mit dem Start der Testversion können zugleich zwei VPN-Profile für Testverbindungen angelegt werden, eine für IPsec mit IKEv1, eine mit IKEv2. Beide nutzen ein mitgeliefertes Testzertifikat mit der PIN 1234.

Lizenzierung

Haben Sie eine Lizenz für die Software erworben, so können die Aktivierungsschlüssel und Seriennummer Ihrer Software-Lizenz über das Monitormenü „Hilfe / Lizenzierung“ eingetragen werden. Alternativ kann auch ein NCP Volume License Server (VLS) genutzt werden.

Assistent für neues VPN-Profil

Mit dem Konfigurations-Assistenten können Verbindungen mit dem Internet oder, je nach erforderlichem VPN-Übertragungsprotokoll, zum Firmennetz rasch hergestellt werden. Je nach Auswahl der gewünschten Grundeinstellung wird das VPN-Profil nach wenigen Konfigurationsabfragen in der Liste verfügbarer VPN-Profile abgelegt. Im Folgenden die jeweils nötigen Daten zur Konfiguration:

Verbindung zum Firmennetz über IPSec:
→ Profil-Name
→ Verbindungsmedium
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)
→ VPN-Gateway-Parameter (VPN-Gateway, Tunnelsecret)
→ Nutzung von Zertifikaten
→ Zugangsdaten für VPN-Gateway (VPN-Benutzer, VPN-Passwort)
→ Statischer Schlüssel (Preshared Key) sofern kein Zertifikat eingesetzt wird (IKE ID-Typ, IKE ID)

Verbindung mit dem Internet herstellen:
→ Profil-Name
→ Verbindungsmedium
→ Zugangsdaten für Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)

Alternativ kann ein bereits bestehendes VPN-Profil folgender Formate importiert werden:
*.ini; *.pcf; *.wgx; *.wgc

Tests des Clients

Während der Installation wurde im Startmenü die Programmgruppe „NCP Secure Client" angelegt. Starten Sie nun aus der Programmgruppe „NCP Secure Client" das Programm „Client Monitor".

Das Telefonbuch des Clients enthält vorkonfigurierte Zielsysteme für Testzwecke:
„Testverbindung IPsec IKEv1"
„Testverbindung IPsec IKEv2"

Ebenfalls für Testzwecke wurde ein „X.509 Soft-Zertifikat" beigegeben. Es wird bei der Installation als PKCS#12-Datei im Installationsverzeichnis gespeichert. Der Dateiname ist „client1.p12" und die PIN „1234". Dieses Zertifikat kann genutzt werden, um Extended Authentication zu testen. Bei Verwendung eines Preshared Keys ist „shared secret" vorkonfiguriert.

Testverbindung IPsec IKEv1

Zugangsdaten:
Tunnel-Endpunkt (Ziel) : vpntest.ncp-e.com
VPN-Protokoll : IPSec
XAUTH-Benutzername : ncpipsecnative
XAUTH-Passwort : ncpipsecnative
Authentisierung : Zertifikat; Standardkonfiguration (client1.p12)

Testverbindung IPsec IKEv2

Zugangsdaten:
Tunnel-Endpunkt (Ziel) : vpntest.ncp-e.com
VPN-Protokoll : IPSec
XAUTH-Benutzername : ncpipsecnative
XAUTH-Passwort : ncpipsecnative
Authentisierung : Zertifikat; Standardkonfiguration (client1.p12)

Testen mit FTP

Bei bestehendem Tunnel können die FTP-Funktionalität testen. Ihre Zugangsdaten:
IP-Adresse : 172.16.12.100
Benutzer : anonymous
Geben Sie dazu in einer DOS-Kommandozeile folgendes ein:
C:\>ftp 172.16.12.100
Verbindung mit 172.16.12.100 wurde hergestellt
220 (vsFTPd 2.0.4)
Benutzer (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 empfangen in 0,00Sekunden 407000,00KB/s
ftp> close
ftp> quit

Testen der Web-Funktionalität

Nachdem Sie eine Testverbindung aufgebaut haben, geben Sie an Ihrem geöffneten Web-Browser die Adresse 172.16.12.100 ein. anschließend erhalten Sie die NCP-Website auf Ihrem Bildschirm.

Testen mit Ping

Bei bestehendem Tunnel können Sie die IP-Adresse 172.16.12.100 anpingen.
Geben Sie dazu in einer DOS-Kommandozeile folgendes ein:
C:\>ping 172.16.12.100 (<ENTER>)
Bei erfolgreichem Ping sehen Sie folgende oder ähnliche Ausgaben:
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
Im Monitor werden die versendeten (Tx) und die empfangenen (Rx) Bytes angezeigt.

NCP engineering GmbH, September 2016

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com