

Data Sheet

NCP Secure Entry Client Windows

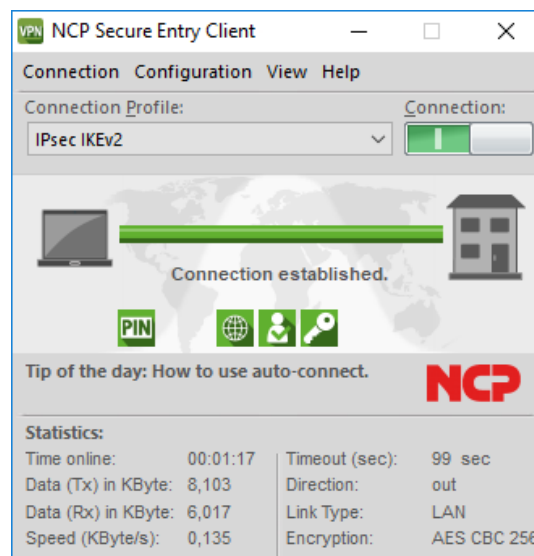


Universal VPN Client Suite for Windows 32/64 bit

- Compatible with VPN gateways (IPsec standard)
- Import of third party configuration files
- Integrated, dynamic personal firewall with IPv6 support
- Fallback IPsec / HTTPS (VPN Path Finder Technology)
- VPN Bypass
- FIPS Inside
- Strong authentication (eg. Certificate), Biometrics
- Multi Certificate Support
- Budget Manager for cost control
- Integrated support of 3G/4G hardware
- Integration of all security and communication technologies for universal remote access
- Free of charge 30 day full version

Universality and Communications

The NCP Secure Entry Client for Windows 32/64 bit operating systems is a communication software product for universal implementation in any remote access VPN environment. The teleworker works transparently and securely at any location (mobile or stationary) in the same manner as in his/her office within the corporate environment. Highly secure data connections to VPN gateways from all well-known suppliers can be established using IPsec standards. Independent of Microsoft remote data transmission dialer, the connection can be set up via any type of network (wire networks, wireless networks, LAN, Wi-Fi and Internet). Clients can be used on 32-/64-bit versions of Windows 7 and Windows 8 to access to company data networks and applications from any location. At a mobile workplace, Seamless Roaming provides a secure, always-on connection to the corporate network, automatically selecting the fastest medium for access to the Internet.



Even if the access point or the IP address changes, Wi-Fi roaming or IPsec roaming maintains the VPN connection. Even behind firewalls whose settings always block IPsec data connections, the NCP Path Finder Technology* ensures remote access is available.

To enable employees to securely log on to the Windows domain before logging on to the Windows system, the client supports domain logon using a credential service provider after establishing a VPN connection to the company network. The user then logs on to the local Windows system through this VPN connection so that the connection is authenticated in the central Windows domain or Active Directory. Secure logon to a Wi-Fi HotSpot is also supported in the pre-logon phase which means the client is optimally protected by the integrated dynamic firewall while logging on to the HotSpot. It makes no difference to the user whether they are in the office or a connected via a HotSpot.

Next Generation Network Access Technology

Data Sheet

NCP Secure Entry Client Windows



Security

The NCP Secure Entry Client also provides additional security mechanisms such as the integrated, dynamic Personal Firewall.

Rules for ports, IP addresses, IP subnets and applications can be defined centrally by the administrator. Based on predefined values for these security rules, "Friendly Net Detection" detects whether the user's computer is located in a friendly or an unknown network. The corresponding Firewall rule is activated, dependent on the network detected, and similarly, when connecting to a hotspot, especially when logging on to and off from the Wi-Fi network. In contrast to normal firewalls, the NCP Firewall starts to work as soon as the computer is booted.

Other security features include support for One-Time Password (OTP) solutions and Certificates in a Public Key Infrastructure (PKI).

Furthermore, the VPN client features biometric authentication before the VPN connection is established, for example via fingerprint or face recognition. Authentication takes place directly after clicking the Connect button in the client GUI, and the connection is not established until authentication is completed. If hardware for biometric authentication is not present or enabled, the user can also authenticate via their password.

When the Home Zone feature is activated, a special user profile is used for the home office network. Users just need to click the Home Zone button and the correct network configuration is made automatically. This includes special firewall rules set up by administrators which only apply when the user is in their home office. This means that users can access their printer or scanner in the home office network. If the user leaves

the Home Zone, the existing firewall rules are reactivated.

The new bypass function in the NCP VPN Client allows the IT administrator to configure the client so that certain applications are exempted from the VPN and the data is sent over the Internet even when split tunneling is disabled. This has the advantage that applications such as video streaming no longer overwhelm the server with terabytes of data.

The Multi Certificate Support feature enables VPN connections to various companies, each which demand a user certificate of its own. All Client configurations can be locked by the administrator, meaning that the user cannot change the locked configurations.

The cryptographic module complies with the requirements of FIPS 140-2 (certificate #1747).

Usability and Profitability

"Easy-to-use" for both user and administrator - the NCP Secure Entry Client is simple to install and simple to operate. A graphical, intuitive user interface provides information on all connection and security states. Detailed log information paves the road for effective assistance from the help desk.

The feature "automatic media detection" automatically selects the fastest communication medium available. A configuration wizard simplifies the set up of connection profiles.

Integrated support of Mobile Connect Cards for WLAN (Wireless Local Area Network) as well as WWAN (Wireless Wide Area Network) applies, without restriction, for all the Windows operating systems supported.

The system automatically configures mobile data connections using information from the current SIM Card and the corresponding provider (APN Access Point Name). Through that, it is easy to use inexpensive, local providers abroad.

Next Generation Network Access Technology

Data Sheet

NCP Secure Entry Client Windows



Use of the Windows 7 Mobile Broadband interface ensures the highest possible performance of 4G/LTE hardware. The additional installation of the user interface supplied by the card manufacturer is not necessary. Domain logon, too, is of course highly secure and as convenient and familiar as it is in the local network. The Client Monitor can be tailored to include your company name or support information

Usability also means cost reduction through less time spent training, less documentation and fewer support calls. VPN tunnels can be configured to be established automatically.

An integrated budget manager guarantees cost transparency because a volume or time budget or the use of a specific provider can be set and monitored.

*Option

Next Generation Network Access Technology

Data Sheet

NCP Secure Entry Client Windows



Operating Systems

Microsoft Windows (32 and 64 bit): Windows 10, Windows 8.x, Windows 7

Security Features

The Entry Client supports all IPsec standards in accordance with RFC

Personal Firewall

Stateful Packet Inspection;
IP-NAT (Network Address Translation);
Friendly Net Detection (FND) (Firewall rules are automatically adapted, if the connected network is recognized because of its IP address area, or the NCP FND server's*);
start FND dependent action;
home zone;
secure hotspot logon;
differentiated filter rules relative to: protocols, ports, applications and addresses, LAN adapter protection;
IPv4 and IPv6 support

VPN Bypass

The VPN Bypass function allows the administrator to define applications which can communicate over the Internet directly despite disabling split tunneling on the VPN connection. It is also possible to define which domains or target addresses can bypass the VPN tunnel.

Virtual Private Networking

IPsec (Layer 3 Tunneling), conform to RFC;
IPsec proposals can be determined through the IPsec gateway (IKE/IKEv2, IPsec Phase 2);
Event log; communication only in the tunnel;
MTU size fragmentation and reassembly, DPD, NAT-Traversal (NAT-T);
IPsec tunnel mode

Encryption

Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits;
Dynamic processes for key exchange: RSA to 2048 bits; seamless rekeying (PFS);
Hash algorithms: SHA-1, SHA-256,SHA384, SHA-512, MD5, DH group 1,2,5,14-21, 25, 26

FIPS Inside

The IPsec Client incorporates cryptographic algorithms conformant with the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747). FIPS compatibility is always given if the following algorithms are used for set up and encryption of the IPsec connection:

- DH 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

Next Generation Network Access Technology

Data Sheet

NCP Secure Entry Client Windows



Authentication Processes

IKE (Aggressive mode and Main Mode), Quick Mode;
XAUTH for extended user authentication;
IKE config mode for dynamic assignment of a virtual address from the internal address pool (private IP);
PFS;
PAP, CHAP, MS CHAP V.2;
IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication relative to switches and access points (Layer 2);
EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): Extended authentication relative to switches and access points on the basis of certificates (Layer 2);
Support of certificates in a PKI: Soft certificates, smartcards, and USB tokens: Multi Certificate Configurations;
Pre-shared secrets, one-time passwords, and challenge response systems;
RSA SecurID ready

Strong Authentication - Standards

Biometric Authentication (Windows 8.x or higher)
X.509 v.3 Standard;
PKCS#11 interface for encryption tokens (USB and smartcards); smartcard operating systems: TCOS 1.2, 2.0 and 3.0; smart card reader interfaces: PC/SC, CT-API;
PKCS#12 interface for private keys in soft certificates;
CSP for use of user certificates in Windows certificate store PIN policy;
PIN policy; administrative specification for PIN entry in any level of complexity;
Revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL), OCSP.

Networking Features

LAN emulation: Ethernet adapter with NDIS interface, full WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network, Mobile Broadband from Windows 7) support

Network Protocol

IP

Dialers

NCP Internet Connector, Microsoft RAS Dialer (for ISP dial-in via dial-in script) connection manager for international dial-in via GoRemote (formerly GRIC), UuNet, Infonet, MCI (on request)

VPN Path Finder**

NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is not possible

Seamless Roaming**

If a communications medium error occurs, automatic switchover of VPN tunnel to another Internet communication medium (LAN/WWAN/3G/4G) without altering IP address ensures that applications communicating over VPN tunnel are not disturbed and application session is not disconnected. (prerequisite: NCP Secure Enterprise VPN Server)

Next Generation Network Access Technology

Data Sheet

NCP Secure Entry Client Windows



Additional Features	UDP encapsulation, WISPr-support, IPsec-Roaming, Wi-Fi roaming, import of the file formats: *.ini, *.pcf, *.wgx and *.spd, Multi Certificate Support
Transmission Media	Internet, LAN, WI-FI, GSM (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA, PSTN, ISDN
IP Address Allocation	DHCP (Dynamic Host Control Protocol), DNS: Dial-in to the central gateway with changing public IP addresses through IP address query via DNS server
Line Management	DPD with configurable time interval; Short Hold Mode; Wi-Fi roaming (handover); channel bundling (dynamic in ISDN) with freely configurable threshold value; timeout (controlled by time and charges); budget manager (administration of connection time and/or –volume for GPRS/ 3G and Wi-Fi, in case of GPRS/ 3G separated administration of roaming abroad)
APN of SIM Card	The APN (Access Point Name) defines the access point of a mobile data connection at a provider. If the user changes provider, the system automatically takes APN data from the corresponding SIM card and uses it in client configuration
Data Compression	IPCOMP (lzs), deflate
Point-to-Point Protocols	PPP over ISDN, PPP over GSM, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP security architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, RFC 7427: IKEv2-Authentication (Padding-method)
Client Monitor Intuitive, Graphical User Interface	Multilingual (German, English, Spanish, French); Client Info Center; Configuration, connection management and monitoring, connection statistics, log-files (color displayed, easy copy&paste-function); Internet availability test; Trace tool for error diagnosis; Traffic light icon for display of connection status; Integrated support of Mobile Connect Cards (PCMCIA, embedded); The Client Monitor can be tailored to include your company name or support information; Password protected configuration management and profile management, configuration parameter lock; Automatic check for newer software version

Next Generation Network Access Technology

Data Sheet

NCP Secure Entry Client Windows



*) If you wish to download NCP's FND server as an add-on, please click here:

<https://www.ncp-e.com/en/resources/download-vpn-client.html>

***) Prerequisite: NCP VPN Path Finder Technology on the Gateway is required or NCP Secure Enterprise Server

More information on NCP Secure Entry Client is available on the Internet at:

<https://www.ncp-e.com/en/products/ipsec-vpn-client-suite.html>

You can test a free, 30-day full version of Secure Entry Client (Win32/64) here:

<https://www.ncp-e.com/en/resources/download-vpn-client.html>

Option: central management and endpoint security (upgrade NCP Secure Enterprise Client)



NCP PATH FINDER

FIPS 140-2 Inside

Next Generation Network Access Technology