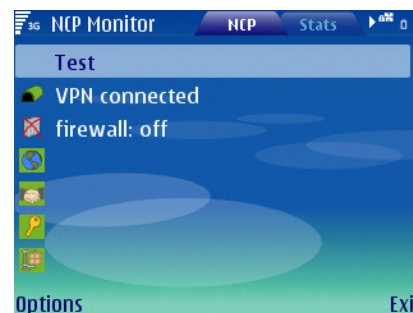


Universal VPN Client software for mobile end devices using the Symbian operating system

- ▶ **Compatibility with VPN gateways from different manufacturers**
- ▶ **Integrated, dynamic personal firewall**
- ▶ **Strong authentication**
- ▶ **Worldwide dial-in via all public radio networks**
- ▶ **End-to-end security principle even at hotspots**
- ▶ **Intelligent connection management for transparent operation, even if the link drops out**
- ▶ **Free 30 day full version**



Universality

NCP Secure Symbian Client is a communications software package for universal use on the company network, based on a Virtual Private Network (VPN). Teleworkers can use their mobile device to access central databases and resources securely from any location. In addition to the NCP Secure Enterprise Server, all VPN gateways based on the IPsec standard and all protocol extensions can be used as remote stations.

In line with NCP's universal product and integrated solutions philosophy, the Secure Symbian Client supports data transfer via all public radio networks. The transfer medium used depends ultimately on the efficiency of the mobile end device and the usage scenario. This could include remote access from a hotspot, in a car, visiting customers or back on the company site.

Security

Comprehensive security measures are required to guard against attack, especially when it comes to mobile data communications. It is needed to guarantee data reliability and to protect the company network from backdoor attacks, for example. The requirement applies especially when a mobile teleworker logs on and off from a hotspot. The NCP Secure Symbian Client sets the standard here, too. It uses every needed security mechanism to implement end-to-end security. The most important, integrated security building blocks in addition to VPN tunnelling are: Data encryption, a dynamic personal firewall, support for OTP (one-time password) tokens, and certificates in a PKI (public key infrastructure). The personal firewall allows the

definition of controllers for: Ports, IP addresses and segments. Friendly net detection provides automatic identification of secure and non-secure networks.

Comfort

„Easy-to-use“ means easy installation and use of client software. The integrated configuration assistant for the configuration PC provides an intuitive, graphic user interface on the mobile end device. The mobile teleworker works in the same way as at his office desk. If the connection drops out during data transfer (e.g. access point change in the WLAN), this has no effect. The user is not affected by it. In the case of email polling/push services, a special connection mode ensures automatic re-establishment of the VPN tunnel to the central VPN gateway. That way, the mobile teleworker can always be reached.

Central management

The NCP Secure Symbian Client is available in „Entry“ and „Enterprise“ versions. Both offer the same performance. The NCP Secure Enterprise Symbian Client can also be managed from a central point and integrated into a comprehensive end point security scenario.

Technical data

System requirements Mobile end device configuration PC	Operating System: Symbian OS from V. 9.0 S60 3rd Edition Operating System: Windows 2000, XP (32/64 Bit), Vista (32/64 Bit); 32 MB RAM Plus: min. 20 MB RAM, Nokia PC Suite
Security features	The Secure Symbian Client supports all IPsec standards as per RFC and also meets the highest security requirements.
Personal firewall	Stateful Packet Inspection; IP NAT (Network Address Translation); differentiated filter rules for: protocols, ports and addresses; Friendly Net Detection (in preparation)
Firewall configuration	Firewall Configuration Plug -In*
Virtual Private Networking (VPN)	IPsec (layer 3 tunnelling), RFC conformity; IPsec proposals can be determined by the IPsec gateway (IKE, IPsec Phase 2); Event log; Block and central tunnelling; MTU size fragmentation and reassembly, DPD; NAT Traversal (NAT-T); IPsec modes: Tunnel mode, Transport mode
Encryption	Symmetrical methods: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamic code exchange: RSA to 2048 bits; Diffie-Hellman groups 1,2,5 Seamless rekeying (PFS); Hash algorithms: SHA1, SHA256, SHA384, SHA512, MD5
Authentication method	IKE (aggressive and main mode), Quick mode; XAUTH for expanded user authentication; IKE config mode for dynamic assignment of a virtual address from internal address book (private IP); PFS; MS CHAP V.2*; Support for certificates in a PKI: Soft certificates (in preparation); Pre-shared secrets; One-time passwords and challenge response systems; RSA SecurID Ready.
Strong authentication	X.509 v.3 Standard; PKCS#12 interface for private key in Soft certificates;
Endpoint Security	Endpoint Policy Enforcement *
Networking features	LAN emulation: virtual Ethernet adapter with NDIS interface or transparent mode
Network protocols	IP
Dialer	Symbian integrated
IP address allocation	DHCP (Dynamic Host Control Protocol); DNS: Selection of central gateway with changing public IP address by searching IP address via a DNS server
Transfer media	WLAN (WiFi), GSM (incl. HSCSD), GPRS, UMTS; Internet; analogue modem (mobile phone via infrared or Bluetooth); usable transfer media depend on end device used
Line management	DPD with configurable time interval; WLAN roaming (hand-over)
Data compression	IPCOMP (lzs), Deflate
Internet society RFCs and drafts	RFC 2401 –2409 (IPsec), RFC 3498, RFC 3947: IP security architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP
Client monitor graphic user interface	Multi-language (German, English); connection stats, log files, trace tool for fault diagnosis; configuration and profile management with password protection
Product versions	NCP Secure Entry Symbian Client NCP Secure Enterprise Symbian Client (central administration*)

* Requirement: NCP Secure Enterprise Management

You can try out a free, 30-day full version of Secure Entry Symbian Client here: <http://www.ncp-e.com/en/downloads/software.html>

IPsec compatibility list: <http://www.ncp-e.com/en/service-support/compatibility/IPsec.html>