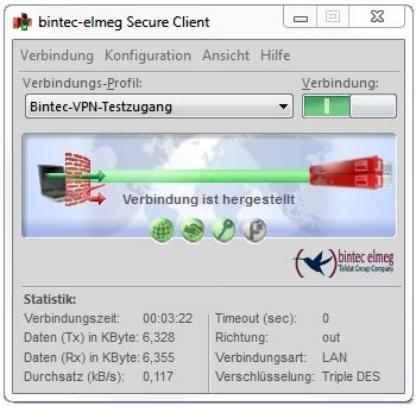
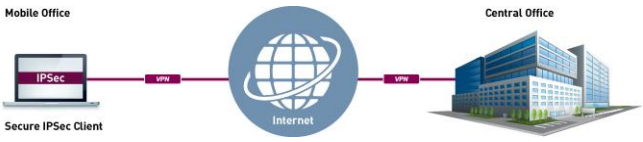
IPSEC VPN CLIENT

IPSec VPN Client für den professionellen Einsatz - ideal für Digitalisierungsboxen





Materialnummer	40295619 (2355186)
Verkaufsstart	01.12.2015
UVP (CRM-T)	75,95 €
IPSec VPN	IPSec nach RFC 2401-2409
Konfiguration	Einfache Bedienbarkeit durch grafische Benutzeroberfläche mit integriertem Installationsassistenten
WLAN Konfiguration	Integrierte WLAN-Konfiguration
Integrierter Dialer (RAS)	Integrierter Dialer für ISDN, GSM, UMTS und LTE mit Budget Manager
Client Monitor	Grafische Benutzeroberfläche zur Verbindungssteuerung und -überwachung
Unterstützte Betriebssysteme	Windows 10, Windows 8.x, Windows 8 (auch TabletPC; kein Windows RT 8.x), Windows 7, Windows Vista, Windows XP (bis v 2.32)- alle 32/64 Bit
Unterstützte Sprachen	Deutsch, Englisch, Französich und Spanisch
Seamless Roaming	VPN Verbindung bleibt auch beim Medien-Wechsel bestehen
HotSpot	Automatische Hotspot Erkennung
Sicherheit	IPv6-fähige dynamische Personal Firewall; Datenverschlüsselung (Encryption); FIPS 140-2 zertifiziert
Anzahl Lizenzen	1 / keine parallele Installation möglich

Highlights

- Sicheren Fernzugriff auf Unternehmensdaten für mobile Mitarbeiter und vom Homeoffice aus
- Integrierte Personal Firewall für den Schutz des Systems des Endanwenders
- Unterstützt IPSec over TCP, NCP Path Finder-Technologie
- Unterstützt Windows 10, 8.x, 7 und Vista
- Hoher Bedienkomfort durch grafische Benutzeroberfläche
- Einfache Installation über Wizard und Assistent

IPSEC VPN CLIENT

Weitere Besonderheiten

- **Online & Offline Aktivierung**: Die Aktivierung des Clients kann direkt online (Internet Zugang von dem entsprechenden PC aus erforderlich) oder offline (Internet Zugang auf einem anderen PC erforderlich) durchgeführt werden.
- **Deaktivierung:** Die Lizenzen des Clients dürfen zeitgleich nur auf einem System aktiviert und verwendet werden.
- Wenn eine Lizenz nicht mehr am System genutzt wird, kann diese deaktiviert werden und anschließend auf einem neuen System wieder aktiviert werden (ab V3.0).
- **Integrierter Dialer (RAS):** Integrierter Dialer für ISDN, GSM, UMTS und LTE mit Budget Manager
- **Client Monitor:** Grafische Benutzeroberfläche zur Verbindungssteuerung und -überwachung
- **System Logging** Einfache Diagnose dank umfangreicher und detaillierter Logging-Informationen
- **Seamless Roaming:** Die VPN Verbindungen bleiben auch bei der Änderung des Verbindungsmediums (LAN/ WAN/Mobilfunk) bestehen.
- **IPSec VPN:** IPSec nach RFC 2401-2409
- **IPSec Algorithmen:** AES (128,192, 256 Bit), 3DES (168 Bit), Blowfish (128-448) RSA (1024 oder 2048)
- **IPSec Hashes**: MD-5, SHA-1, SHA-256, SHA-384, SHA-512 und DH-Gruppen 1, 2, 5, 14-18
- **IKE Versionen:** IKEv1 und IKEv2 - mit Pre Shared Keys und Zertifikaten (X.509)
- **IPSec IKE Config Mode:** IKE Config Mode ermöglicht die dynamische Zuweisung der Client IP Konfiguration (IP-Adresse, DNS und WINS Server)
- **IPSec Dead-Peer-Detection:** Sorgt für eine kontinuierliche Überwachung der IPSec-Verbindung
- **IPSec NAT-T:** Unterstützung von NAT-Traversal (NAT-T) für den Einsatz auf VPN-Strecken mit NAT
- **IPSec Zertifikate (PKI):** Unterstützung von X.509-Zertifikaten
- **IPSec PKI Standards:** Entrusts Smart Cards: PKCS#11, für Verschlüsselungs-Token TCOS 1.2 und 2.0, Smart Card Reader Interfaces CT-API und PC/SC, PKCS#12, CSP
- **IPSec Certificate Revocation List:** EPRL - End-entity Public-Key Certificate Revocation List (CRL), CARL - Certification Authority Revocation List, (ARL), OCSP - Online Certificate Status Protocol
- **IPSec über TCP (NCP PathFinder):** IPSec Fallback auf TCP, z.B. 443 (HTTPS), basierend auf der NCP Path Finder Technologie, zur Überwindung von Firewalls bei Sperrung von IKE Port 500.
- **FIPS inside:** Der Client verfügt über einen kryptografischen Algorithmus nach FIPS-Standard (zertifiziert nach
- FIPS 140-2). Die FIPS Kompatibilität ist gegeben, wenn folgende Algorithmen für den Aufbau und die Verschlüsselung der IPSec-Verbindung genutzt werden.
- **FIPS Inside Algorithmen:** Verschlüsselungsalgorithmen: AES 128, 192, 256 Bit oder Triple DES; - Hash Algorithmen: SHA1, SHA256, SHA384 oder SHA512 Bit - DH Gruppe: Gruppe 2 oder höher
- Medientypen LAN, WLAN, XDSL, ISDN, GSM, UMTS, LTE, inklusive automatischer Medientyperkennung
- **DynDNS:** Abfrage der aktuellen IP-Adresse über einen öffentlichen DynDNS-Server
- **Stateful Inspection Firewall:** Sateful Inspection Firewall für IPv4 und IPv6, richtungsabhängige Paketfilter mit Überwachung des jeweiligen Verbindungsstatus, Applikationsfilterung
- **Friendly Net Detection:** Automatisches Erkennen von sicheren und unsicheren Netzwerken, aktiviert abhängig davon Firewall-Regeln
- **Passwort-Schutz :** Passwort-Schutz für Profil-Management und Konfiguration verhindert unberechtigten Zugriff auf die Konfigurationseinstellung

Lieferumfang

- Brief mit Seriennummer und Aktivierungscode der Lizenz
- Download-Hinweis (www.bintec-elmeg.com)