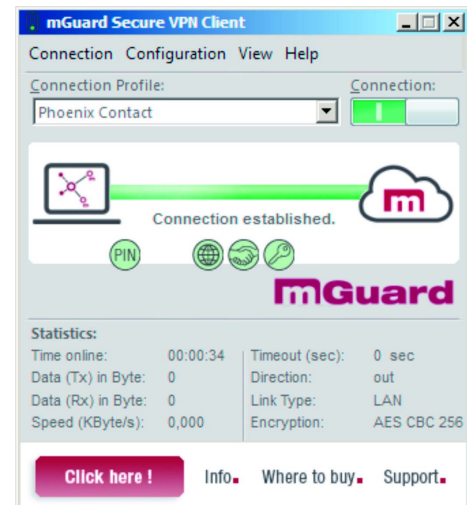


# MGUARD SECURE VPN CLIENT

## VPN software client

Data sheet  
107026\_en\_01

© PHOENIX CONTACT 2017-03-22



## 1 Description

The VPN software client is a software application for connecting PCs to a virtual private network (VPN). The client expands the private network by means of a public, unsecure network, such as the Internet. This ensures that resources from remote networks can be accessed both securely and transparently.

As a result, data can be transferred reliably between the client and the mGuard system. The IPsec protocol ensures the confidentiality, authenticity, and integrity of all data.

With a single click, the client automatically selects the ideal transfer medium, starts connecting to the Internet, and establishes the VPN tunnel. A centrally defined parameter lock prevents users from making accidental changes to the configuration data.

The client supports both mobile and stationary applications. It is compatible with all mGuard VPN applications and mGuard Secure Clouds, as well as ADSL and mobile communication routers from Phoenix Contact.

## Features

- For desktops, laptops, or tablet PCs running Windows 10, Windows 8.x, or Windows 7
- Compatible with the complete mGuard system
- Compatible with ADSL and mobile communication routers from Phoenix Contact
- Maximum security with IPsec protocol on Layer 3
- Supports current certificates such as x509.v3
- Secure data transmission with 128/192/256-bit AES encryption
- Extended authentication compared to switches and access points in accordance with IEEE 802.1x
- Free 30-day trial version available to download



Make sure you always use the latest documentation.  
It can be downloaded from the product at [phoenixcontact.net/products](https://phoenixcontact.net/products).

## 2 Ordering data

| Description                          | Type                            | Order No. | Pcs./Pkt. |
|--------------------------------------|---------------------------------|-----------|-----------|
| License for mGuard Secure VPN Client | MGUARD SECURE VPN<br>CLIENT LIC | 2702579   | 1         |

## 3 Technical data

| System requirements                   |                                                                                       |
|---------------------------------------|---------------------------------------------------------------------------------------|
| Supported operating systems           | Windows 10, Windows 8.x, Windows 7 (32 bit and 64 bit)                                |
| Supported VPN remote peers            | mGuard Secure Cloud                                                                   |
|                                       | FL MGUARD ... VPN                                                                     |
|                                       | TC MGUARD ... VPN                                                                     |
|                                       | TC ROUTER 3002T...                                                                    |
|                                       | TC DSL ROUTER X500 A/B                                                                |
| VPN (virtual private network)         |                                                                                       |
| VPN (virtual private network)         | IPsec (layer 3 tunneling)                                                             |
|                                       | RFC-compliant                                                                         |
|                                       | IPsec proposals can be determined by the IPsec gateway (IKEv1 / IKEv2, IPsec Phase 2) |
|                                       | Event log                                                                             |
|                                       | Communication in tunnel only                                                          |
|                                       | MTU-size fragmentation and reassembly                                                 |
|                                       | Dead peer detection (DPD)                                                             |
|                                       | NAT traversal (NAT-T)                                                                 |
|                                       | IPsec tunnel mode                                                                     |
| Encryption                            |                                                                                       |
| Symmetrical operation                 | AES 128/192/256 bit, Blowfish 128/448 bit, Triple DES 112/168 bit                     |
| Dynamic operation for exchanging keys | RSA up to 2,048 bit, seamless rekeying (PFS)                                          |
| Hash algorithms                       | SHA-256, SHA-384, SHA-512, MD5, DH group 1, 2, 5, 14 ... 18                           |
| Cryptography module                   | Embedded, certified in accordance with FIPS 140-2 (certificate #1051)                 |



FIPS compatibility is always specified if one of the following algorithms is used to establish and encrypt the IPsec connection:

- Diffie-Hellman group: Group 2 or higher (DH from a length of 1,024 bit)
- Hash algorithms: SHA-1, SHA-256, SHA-384, or SHA-512
- Encryption algorithms: AES with 128 bit, 192 bit, or 256 bit, triple DES

## Authentication

|                                  |                                                                                                                                                                            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication methods           | IKE (aggressive and main mode), quick mode                                                                                                                                 |
|                                  | XAUTH for extended user authentication                                                                                                                                     |
|                                  | IKE config mode for dynamically allocating a virtual address from the internal address range (private IP)                                                                  |
|                                  | PFS (Perfect Forward Secrecy)                                                                                                                                              |
|                                  | PAP, CHAP, MS CHAP V.2                                                                                                                                                     |
| IEEE 802.1x                      | EAP-MD5 (extensible authentication protocol) for extended authentication compared to switches and access points (layer 2)                                                  |
|                                  | EAP-TLS (extensible authentication protocol – transport layer security) for extended authentication compared to switches and access points based on certificates (layer 2) |
| Supporting certificates in a PKI | Soft certificates, smart cards, and USB tokens                                                                                                                             |
|                                  | Multi-certificate configuration                                                                                                                                            |
|                                  | Pre-Shared Secrets                                                                                                                                                         |
|                                  | One Time Passwords (OTP)                                                                                                                                                   |
|                                  | Challenge response systems (e.g. RSA SecurID Ready)                                                                                                                        |
| Authentication standards         | X.509 v.3 default                                                                                                                                                          |
|                                  | Entrust Ready                                                                                                                                                              |
|                                  | PKCS#11 interface for encryption tokens (USB and smart cards)                                                                                                              |
|                                  | Smart-card 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 using user certificates in the Windows certificate store                                                                                                           |
|                                  | PIN directive, administrative specification for entering any complex pins                                                                                                  |
| Revocation                       | EPRL (end-entity public-key certificate revocation list, formerly CRL)                                                                                                     |
|                                  | CARL (certification authority revocation list, formerly ARL)                                                                                                               |
|                                  | OCSP (Online Certificate Status Protocol)                                                                                                                                  |

## Networking

|               |                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| LAN emulation | Virtual Ethernet adapter with NDIS interface, integrated, complete WLAN and WWAN support (wireless wide area network, mobile broadband from Windows 7) |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|

## VPN Path Finder

VPN Path Finder

VPN path finder technology, fallback: IPsec / HTTPS (port 443), if port 500 and UDP encapsulation are not possible



Prerequisite: VPN path finder technology at VPN gateway, from mGuard firmware 8.3.

## Line management

Line management

DPD with configurable time interval

Short Hold Mode

WLAN roaming (handover)

Timeout, controlled by time

## Data compression

Data compression

IPCOMP (LZS), Deflate

## RFC compatibility

RFC compatibility

RFC 2401 ... 2409 (IPsec)

RFC 3947 (NAT-T Negotiations)

RFC 3948 (UDP Encapsulation)

IP Security Architecture

ESP (Encapsulating Security Payload)

ISAKMP/Oakley

IKE (Internet Key Exchange)

XAUTH

IKECFG

Dead peer detection (DPD)

NAT traversal (NAT-T)

UDP Encapsulation

IPCOMP (Internet Protocol Payload Compression Protocol)