genuconnect
genuconnect Enterprise

Mobile Work

Facts and Features

Definition

Maximum security and functionality when using laptops or tablets with MS Windows 10 or 11 is provided by genuconnect and genuconnect Enterprise. The VPN Software Clients protect the connections of mobile devices against unauthorized access and scale with growing infrastructure.

While genuconnect Enterprise was developed for secure mobile working in companies, genuconnect enables the processing of classified information up to German VS-NfD, NATO RESTRICTED, and RESTREINT UE/EU RESTRICTED. Changing from genuconnect Enterprise to genuconnect is possible without additional hardware or backend readjustment.

Typical Use

- Highly secure mobile working with laptops and tablets using Microsoft 10 or 11
- Enabling scalable, flexible workplaces in home offices or at multiple locations

Reasons to Choose genuconnect/ genuconnect Virtual

- Secure VPN technology “Made in Germany” for data communication via untrusted networks
- Complete integration in Microsoft Windows
- High scalability: Can be used with more than 100,000 VPN clients
- Compatible with common roll-out mechanisms

Product Differences

genuconnect:

- Approval for classification levels German VS-NfD, NATO RESTRICTED, and RESTREINT UE/ EU RESTRICTED
- Authentication via the user’s smart card
- Randomness enforcement at “VS level”

genuconnect Enterprise:

- Based on genuconnect, enables easy switching to the approved VPN Software Client version
- Two-factor authentication via soft token and password/pin

Service

- Comprehensive training courses
- Customer service directly from the manufacturer

SecurITy made in Germany

System Requirements	
Public Key Infrastructure	PKI for creating and managing the certificates used
VPN endpoint	genuscreen configured as a VPN endpoint in version 8.0 or higher (to use all features, version 8.4 or higher is required)
Remote workstation	Operating system Windows 10 or Windows 11, Pro/Enterprise or LTSC (64 Bit, Intel/AMD)
User	Smart card for the end user's authentication (VPN) keys; one smart card can be used for VPN, e-mail, and disk-encryption keys/certificates

Core Function	
Software based VPN client	Establishes a highly security IPsec/IKEv2 tunnel from any remote workstation to the corporate network
Pre-Logon Access Provider (PLAP) support	Can create the VPN tunnel before the user logs on to Windows, enabling secure network access for authentication services
Smart card authentication	Uses a PKCS#11-enabled smart card for private key storage; the key never leaves the card

Security Model	
Device health & quarantine	The client reports Windows health status to the gateway; non-compliant devices can be placed in a quarantine zone
Trusted Network Detection (TND)	Detects when the client is on a trusted internal LAN and optionally bypasses encryption for direct communication
Captive Portal Browser (CPB)	Minimal-privilege browser that handles captive-portal logins
Automatic authentication	Establish communication in trusted environments with soft token machine certificate without requiring user interaction

Cryptography (Approved Operation)	
PQC support	Hybrid Kyber786+brainpool256
Integrity & encryption	Supports HMAC SHA2 (256/384/512) for integrity and AES GCM/AES CBC (128/192/256) for encryption
Diffie-Hellman groups	Brainpool (P256/P384/P512) and ECP (256/384/521) groups are available for key exchange

Gateway Requirements	
genuscreen appliance	Works with genuscreen ≥ 8.0 (full feature set from 8.4) as the VPN gateway
IKEv2/IPsec ESP	Standard, widely supported VPN protocols with UDP encapsulation (default UDP 4500)
Optional MFA	RADIUS/EAP TLS or EAP MSCHAPv2 can be added on the gateway for multi-factor authentication
DHCP-offered gateways	Gateways can also be supplied via a DHCP option

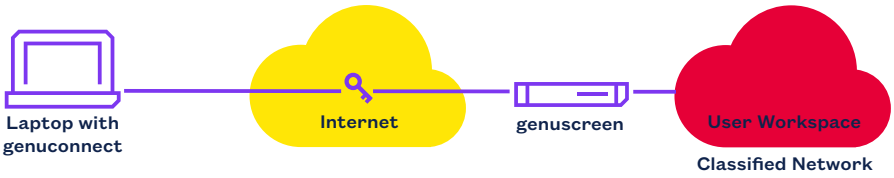
Management & Administration	
Windows GUI	Simple UI showing connection status (gray = idle, green = secure, yellow = restricted/quarantine, red = error)
Profile concept	Each profile can have its own gateway list, certificate handling, and access rules
Central deployment	Distributed as an MSI package; can be pushed via MECM/SCCM or any software distribution system
Auditing & logging	All user connections are logged; Windows Event Log entries are generated automatically
Monitoring	SNMP and Syslog
High Availability (HA)	Connectors can be grouped in active-active mode, load balancing across multiple gateways

Connectivity Options	
Gateway list	One or more VPN gateways can be defined (IP or FQDN)
Captive-portal handling	CPB is automatically launched when a captive portal is detected (e.g., hotel Wi-Fi)
Trusted-network detection	When a trusted internal network is detected, direct communication can be permitted

Certificate Management	
PKCS#11 library integration	Uses a configurable PKCS#11 driver to access smart card certificates
Trusted IKE CAs	A list of trusted certificate authorities is stored on the client for IKE authentication
OCSP revocation checking	Supports online certificate status verification via an OCSP responder on the gateway

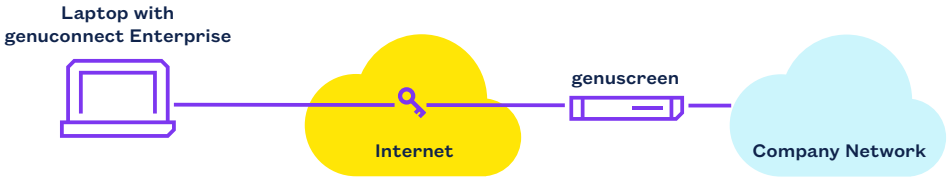
Supported Environments	
Approved operation	genuconnect is approved for classification levels German VS-NfD, NATO RESTRICTED, and RESTREINT UE/EU RESTRICTED

Use Cases



Highly secure connection to internal networks with genuconnect

Employees of government organizations or companies in the classified industry can use genuconnect to establish a highly secure VPN connection to their organization's network and process classified information. Authentication for use of the laptop or tablet is performed easily by means of Windows login or via smart card.



Secure connection to internal networks with genuconnect Enterprise

Employees with access to confidential company information can use genuconnect Enterprise to establish a VPN connection to the company network to process this information securely. Login to the device is protected by 2-factor authentication (soft token and password/pin).

Further Information:

www.genua.eu/genuconnect

www.genua.eu/genuconnect-enterprise

All information in this data sheet is provided for product description purposes only, does not constitute a guarantee, and is not intended to be exhaustive. Technical changes are reserved. Actual performance may vary depending on the operating environment and configuration. Reproduction and/or duplication – including in part and/or in modified form – is permitted only with the written consent of genua.

genua GmbH
Domagkstrasse 7 | 85551 Kirchheim | Germany
+49 89 991950-0 | info@genua .eu | www.genua.eu

0626-03-E