BITTIUM SAFEMOVE® MOBILE VPN

Highly Secure, Always-On & Seamless Connectivity

Bittium SafeMove® Mobile VPN remote access solution provides secure, always-on, and seamless connectivity for government, authority, and other organizations with the highest security requirements. All users enjoy hassle-free, zero-click access to the best available network wherever their work takes them.

Always best connected – SafeMove does passive and active measurements for always selecting the best route.

Zero-click connectivity – SafeMove removes all of the hassle and complexity of getting connected by enabling genuine zero-click access to the best available network. Whether it's 5G, Ethernet, Wi-Fi or SAT, users are connected instantly and automatically.

Seamless roaming – Once connected, moving from one network to another is totally transparent and requires no user involvement whatsoever. SafeMove allows connectivity to be maintained and applications remain in use throughout.

Session persistence – Even during longer gaps in network coverage, the VPN and other application sessions are maintained avoiding the frustration of frequent re-authentication and loss of data.

Post-quantum cryptography (PQC) – SafeMove IPsec VPN supports quantum-resistant cryptographic algorithms to safeguard against the emerging threat of quantum computing. SafeMove adopts the hybrid approach and combines both classical and PQC mechanisms for enhanced security. Currently, SafeMove implements ML-KEM (CRYSTALS-Kyber) for multiple key exchanges in IKEv2. Currently available for Android.

For more information, please contact:
secure@bittium.com

Supported clients

- Microsoft Windows 11 onwards
- Android™ 11 onwards
- iOS 15 onwards

Older Android versions may not support all the latest features of SafeMove® Android Client

Supported servers

- Virtualized server appliance, Bittium SafeMove® server appliances, Red Hat® Enterprise Linux® 8 certified server hardware, public or private clouds

Security approvals

- NATO Restricted for Bittium Tough Mobile™ 2 C solution including Bittium SafeMove® Mobile VPN
- TL IV (Restricted) granted by National Cyber Security Authority (NCSA) in Finland
- Difusión Limitada (Restricted)granted by Centro Criptológico Nacional (CCN) in Spain

Bittium
DEFENCE & SECURITY

Hotspot login assistant – Makes access to Wi-Fi hotspots easy and secure. SafeMove includes an integrated, secure web browser that lets the user log on to access networks requiring web login. When login is complete, the secure connection automatically switches to using the hotspot network, giving a secure, seamless connection.

Intranet detection – SafeMove's Intranet Detection functionality automatically disables tunnelling and encryption when it detects the user is connected using a trusted link (such as wired Ethernet in the corporate network).

Compatibility – A wide range of client device platforms is also supported so that your entire workforce can take advantage of easy, secure connectivity. SafeMove® is based on open international standards such as IPsec, IKE and Mobile IP allowing seamless integration with other systems.

Access control – SafeMove's Access Control Server enables fine grained user access control based on identity, group membership in Active Directory (AD) and/or restricted destinations (IP address range in the corporate internal network).

WAN optimization – The WAN optimization/ payload compression methods supported by SafeMove® reduce the required bandwidth. For compressible data such as text, this can have significant performance benefits especially on the narrowband connections.

Cyber security ready – The quarantine feature detects when your device's anti-virus software is not up to date, firewall is disabled or the patch level is lagging behind and sets the device to limit access to only remediate its security posture. Once updated, access to the enterprise network is restored.

Hybrid cloud ready – Fine grained policy for which traffic to encrypt and tunnel, and which traffic to pass directly to the internet. This can be leveraged to reduce load on the enterprise network as e.g. cloud services and video conferencing need not unnecessarily pass through the enterprise network.

Versatile server options – SafeMove can be run and operated anywhere from small embedded devices and small scale on-premises network systems to large public cloud environments.

High availability, scalability and load balancing – SafeMove's exceptional scalability makes it suitable for large, mission-critical deployments. Servers can be distributed geographically for more efficient network use whilst dynamic load-balancing maintains an even load across all available servers.

Reporting – The SafeMove management console provides a wealth of advanced reports and usage statistics as well as a real-time view of current server activity.

IPv6 support – SafeMove can simultaneously handle both IPv4 and IPv6 traffic, and utilize both IPv4 and IPv6 connectivity.

Authentication – Strong authentication is the key to establishing secure remote access. SafeMove supports the standard Internet Key Exchange (IKEv2) procedure for authentication and allows the use of software certificates as well as two-factor authentication using smart cards or USB dongles, including support for Windows smart card CSP function.

Encryption – All data communication is encrypted using a cryptographic module that meets the latest international security standards for public and private sector organisations.

Always best connected

When a mobile device moves through a wireless networking environment and encounters the following situations, SafeMove maintains connectivity at all times:

1. Normal coverage

2. Coverage from multiple, competing access points

3. No coverage at all for a short while (notspot)

4. Intermittent loss of coverage because of different obstacles (dynamically changing)

No matter what your challenges in mobile working are, SafeMove solves them.

Bittium ▪ Ritaharjuntie 1, FI-90590 Oulu, Finland ▪ Tel. +358 40 344 2000 ▪ **bittium.com**

Bittium
DEFENCE & SECURITY