Bittium

Bittium SafeMove® Mobile VPN

Bittium SafeMove® Mobile VPN remote access solution provides always-on, secure and seamless connectivity for field workers. With SafeMove, all field workers can enjoy hassle-free, zero-click access to the best available network wherever their work takes them.

Always Best Connected – Bittium 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 LTE, 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. Bittium 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.

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 certified cryptographic module that meets the latest international security standards for public and private sector organisations.

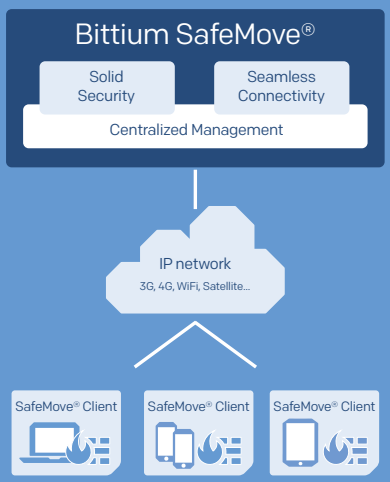
Post-Quantum Cryptography (PQC) – SafeMove IPsec VPN supports quantum-resistant cryptographic algorithms to safeguard against the emerging threat of quantum computing. SafeMove adopts the hybrid approach and combines both classical and PQC mechanisms for enhanced security. Currently, SafeMove implements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

FOR MORE INFORMATION, PLEASE CONTACT:

safemove.sales@bittium.com

SafeMove® in brief

- Always Best Connected
- Zero-click connectivity
- Seamless roaming
- Session persistence
- Solid security
- Fine-grained access control
- Device reachability
- Data compression
- Standards-based



Bittium SafeMove® Mobile VPN

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. The supported WISPr protocol in the Hotspot Login Assistant enables fully automatic and zero-click access to operator hotspot networks.

Hotspot Firewall Traversal – This feature enables the client to access networks that block standard VPN and Mobile IP. Some hotspots and guest networks have restrictive firewalls that prevent the use of VPNs. By instead using TCP port 443 – the standard HTTPS port – the SafeMove® client can seamlessly access also such problematic networks.

Wi-Fi Configuration Provisioning – Windows Wi-Fi/WLAN configuration profiles can be provisioned to SafeMove® clients and it will be centrally managed using the Bittium SafeMove® Manager. Both password protected networks (WPA2) and unprotected networks are supported.

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). This functionality enhances performance and allows zero touch switching between secure VPN and trusted corporate Ethernet.

Ease of Deployment – SafeMove® integrates with a Microsoft infrastructure allowing SafeMove® clients and their corresponding PKI certificates to be deployed through group policies.

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

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). Access Control rules can be configured in the SafeMove® Manager and the feature can be integrated with existing AD settings. This means that only users with a valid and active account in AD are granted access to corporate resources and only those that they are entitled to use.

WAN optimization –This 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. This greatly improves the usability of applications for example in rural areas, where LTE coverage might be spotty or entirely missing. This benefits the mission and business critical users of SafeMove® in public safety, community nursing, utilities and in other field services.

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 and performance requirements on the enterprise network as e.g., cloud services and video conferencing need not unnecessarily pass through the enterprise network. This feature also allows access to resources not available from the enterprise network, such as home network printers.

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. Support for multiple Home Agents eliminates potential bottlenecks and further enhances fault tolerance.

Cost Control – Because SafeMove® constantly monitors which networks are available for connection, use of more expensive bandwidth is kept to an absolute minimum or denied completely. The Roaming policy feature enables the SafeMove® client to detect when Windows Mobile Broadband is roaming in a foreign operator network. The client can then apply a special firewall policy to block certain traffic, e.g. block Windows Update and allow only certain business critical applications, like email. This can lead to significant cost savings and prevent users from inadvertently using costly, volume based data services.

Bittium SafeMove® Appliance – For immediate, out-of-the-box deployment SafeMove® is available as a pre-installed Server Appliance.

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.

Supported Clients:

- Microsoft Windows 10 onrwards
- Android 9 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
- Microsoft Azure, AWS. private clouds

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