

Secure, Seamless Connectivity to Mobile Workers



SafeMove mobile virtual private network (MVPN) solution enables easy and secure access to the corporate internal network, ensuring an unparalleled user experience making it an effective solution for all mobile workers.

Connectivity

SafeMove's Mobile IP Client establishes and maintains network connections with the minimum of effort so users enjoy a fully productive, LAN-like experience wherever their work takes them.

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 Ethernet, WLAN, GPRS, Edge or 3G, 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.

Hotspot Login Assistant – The new and improved 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 Mobile IP and IPsec connection automatically switches to using the access network, giving a secure, seamless connection.

Hotspot Firewall Traversal – This feature enables the client to access networks that block standard VPN and Mobile IP. Some hotspots and guest networks have firewalls that block UDP port 434 utilized by standard

SAFEMOVE IN BRIEF

- > Zero-click connectivity
- > Seamless roaming
- > Session persistence
- > Productivity
- > Cost-savings
- > Reachability
- > Solid security
- > Standards-based
- > High availability/Load balancing
- > Fine-grained access control
- > Integration to enterprise infrastructure



Mobile IP. By instead using TCP port 443 – the standard HTTPS port – the SafeMove client can seamlessly access also such problematic networks.

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.

Security.

SafeMove meets the industry’s highest information security requirements so that remote access can be provided with confidence yet without negatively impacting ease of use.

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

Encryption – All data communication is encrypted using a FIPS 140-2 certified cryptographic module that meets the latest international security standards for public and private sector organisations.

Anti-Virus Quarantine – The AV Quarantine feature detects when your device’s anti-virus software is not up to date and sets the personal firewall to limit access to receive AV updates only. Once updated, access to the enterprise network is restored.

Access Control - SafeMove’s new 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.

Manageability.

A standards-based approach combined with a flexible architecture and a comprehensive management console mean SafeMove is ready for the most challenging environments yet surprisingly easy to deploy and manage.

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.

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

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. This keeps communications and data roaming costs within acceptable limits and can result in significant savings.

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.

For more information contact our sales: safemove.sales@birdstep.com or visit our website at www.birdstep.com.

SUPPORTED PLATFORMS:

Clients:

- > Microsoft Windows XP Service Pack 3 (32-bit)
- > Microsoft Windows 7 (32-bit and 64-bit) (Service Pack 1 recommended)
- > Microsoft Windows Vista (32-bit) Service Pack 2
- > Nokia smart phones with operating system versions of S60 3.1, S60 3.2 and S60 5th edition.
- > Windows Mobile devices with Windows Mobile version 6.5 or 6.1.

Servers:

- > CentOS 5.7 (x86 32-bit)
- > RedHat Enterprise Linux 5 Update 4