



SSL Mobile VPN — AirBEAM Safe



SSL Mobile VPN

FEATURES

FIPS 140-2 compliant

Meets stringent federal guidelines for security as established by the National Institute of Standards and Technology

WTLS (Wireless Transport Layer Security)

Provide secure wireless communications on the Internet, including Web browsing, email, instant messaging and access to corporate data

Provide wired-level network security for handheld and laptop computers, smartphones, printers, payment terminals and more

The SSL Mobile VPN (AirBEAM Safe) allows enterprises to leverage the power of mobility without compromising security. This virtual private network (VPN) allows enterprises to provide workers who are on-the-move inside and outside the enterprise walls with easy-to-use secure wireless access to the Internet, corporate intranet and applications — from any device over any wireless or wired network. True end-to-end security is delivered through a comprehensive feature set, which includes 3-factor authentication, encryption, integrity monitoring, log file records and policy management tools. The SSL Mobile VPN runs in the background over any network, transparent to users while providing a robust always-on persistent connection. No matter where your users are — from sales personnel and managers out in the field to associates on the retail sales floor and healthcare workers in a hospital — your workers can access the Internet, host-based business applications and send and receive email and instant messages, all with the same level of security as a wired network.

Worry-free security for wireless devices

Two- and three-factor strong authentication provides worry-free mobility, especially critical in the retail and healthcare industries, where compliance with government regulations is required to protect sensitive financial and personal data. Authentication support includes Windows Domain Username/password, soft certificates, RADIUS challenge/response, RSA SecurID single-time password and smartcards. Client and server side authentication ensures that the mobile device is authorized on your network and connected to an authorized device. The FIPS 140-2 compliant solution offers strong 256-bit AES encryption to protect data in transit. Integrity checks ensure that data was not altered while in transmission, preventing devices from sending or receiving information that contains a rogue packet. IT can ensure that all mobile devices are compliant with the company's standard security policies via Network Access Control (NAC) — and non-compliant devices can be quarantined, protecting the network from unauthorized access attempts and attacks.

**WLAN and WWAN support:
Wi-Fi, 3G, EDGE, GPRS,
EVDO, CDMA, WiMAX
and satellite**

Provides secure communications for a wide range of users inside and outside the enterprise walls

**Windows Mobile 6.0/5.0/2003,
Windows CE 3.0/4.X/5.X,
Windows 2000 Professional,
Windows XP Professional,
Windows Vista Professional,
MS-DOS, DR-DOS and
embedded systems**

Flexibility to support a broad range of mobile devices, including mobile computers, smartphones and laptops, as well as fixed devices such as printers, payment terminals and scales

**256-bit AES encryption;
RSA key-exchange, SHA-1
integrity checking and
support for standard PKI**

Provides robust industry standard encryption to protect data in transit

**Supports Windows
Domain username/
password, client
certificates, RADIUS
challenge/response,
RSA SecurID single-time
password, smartcards
and biometrics**

Provides strong authentication to ensure that users are authorized and connected to authorized servers

Broad device support

The SSL Mobile VPN offers support for a wide range of platforms, including mobile devices such as handheld mobile computers, smartphones and laptops as well as printers, payment terminals and scales. This flexibility enables the enterprise to deploy a single VPN solution to support all devices, simplifying and reducing the cost of securing wireless connections as well as eliminating the need to run cables to connect printers and other peripherals. This secure wireless connection provides enterprises with the flexibility to easily and cost-effectively reconfigure the enterprise environment as needed — for example, re-locating payment terminals in a retail store during peak holiday times — reducing operating costs as well as providing the business agility to respond easily to changing business needs.

Broad network support

Regardless of network, you can count on Motorola's SSL Mobile VPN to deliver a level of security equivalent to the wired network. Comprehensive network support includes wireless LAN (WLAN) as well as wireless WAN (WWAN), WiMAX and satellite, providing users outside the four walls with an easy direct connection to headquarters or other remote and branch offices. And regardless of the bandwidth of the network, advanced data compression improves throughput, delivering superior performance.

Designed for mobile devices

The SSL Mobile VPN is designed from the ground up for mobile devices. Unlike wired VPNs, the application has a very small memory footprint and requires minimal processing power. As a result, battery life is preserved for communications, helping enterprises provide full-shift mobile access to mobile workers and reducing the need to invest in and maintain a larger battery pool.

Seamless connectivity — even when roaming

With the SSL Mobile VPN, your users can count on session persistence, providing a continuous VPN session regardless of whether the device enters sleep mode, loses coverage or is switching between networks. As a result, users enjoy seamless security with a single sign-on — even when roaming between the WLAN and the WWAN. User productivity is improved — there is no need to repeatedly log on throughout the day, reopen applications and re-navigate through menus to complete tasks. In addition, data loss attributable to a lost connection is also eliminated. For example, data entered on screen but not yet saved is retained, and interrupted file transfers are resumed without loss of data.

Best-practices robust policy management

Just as policies are used to manage the wired network, the SSL Mobile VPN enables the creation and enforcement of robust policies for individuals as well as groups. As a result, security is further strengthened: user access can be limited to specific applications. Device performance is protected: synchronization with the corporate networks can be enabled only when high-bandwidth network connections are available. Costs are reduced through the prioritization of networks: for example, users in the field that are connected to the cellular network can automatically switch to a lower cost WLAN hotspot or the enterprise WLAN when available.

Robust reporting for cost-effective regulatory compliance

The SSL Mobile VPN log tracks all activities, including malicious log-in attempts and tampered data. All traffic and events are documented, complete with a time stamp as well as user and device identification. Real-time alerts notify management of potential security breaches,

enabling instant action. And the ability to automatically collect this information and quickly generate a report on-demand enables enterprises to cost-effectively meet government regulations, including compliance with Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA) regulations.

Easy to use...easy to deploy...easy to manage

The SSL Mobile VPN brings simplicity to security for end-users and IT administrators alike. There is no user configuration or training required — users can quickly and easily connect via the VPN with just a few clicks. Since only industry standard security is utilized, the SSL Mobile VPN integrates easily with your existing technology architecture. Comprehensive centralized and remote management

capabilities minimize the time and costs associated with deployment and ongoing management. From a central SSL Mobile VPN console or via Motorola's MSP3 (Mobility Services Platform 3), IT can configure, update and monitor VPN servers and VPN clients — no hands-on required. And keeping your software up to date is easy. Motorola offers full service packages that include access to product updates and electronic support information as well as around-the-clock technical support.

For more information on how you can provide your mobile users with wired network level security, please visit us on the web at www.motorola.com/sslmobilevpn or access our global directory at www.motorola.com/enterprisemobility/contactus

5,000 concurrent sessions per server/scalable to 100,000+ clients

Provides the scalability to support the largest enterprise environment

Server support: Windows 2000/2003 and Linux (kernel 2.6.8 or higher)

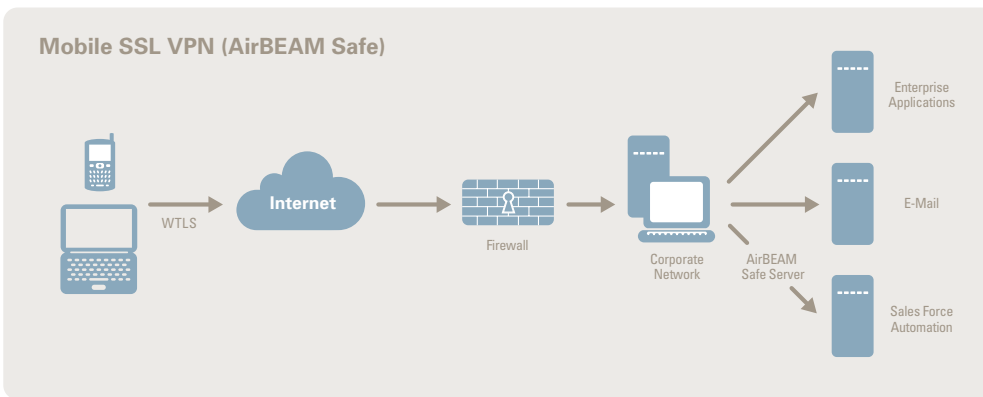
Ability to install on any existing server simplifies and enables rapid deployment

Centralized management (optional)

Optional capability to customize MSP3 via plug-ins to enable centralized and remote management of the SSL Mobile VPN

Gatekeeper

Optional solution component can be installed outside firewall to further increase security and add load balancing and failover



The schematic above illustrates how the Motorola Mobile SSL VPN allows enterprises to easily and cost-effectively enable wireless access to the Internet, corporate intranet and applications — from any device over any wireless or wired network.

SPECIFICATION SHEET

SSL Mobile VPN — AirBEAM Safe



MOTOROLA

motorola.com

Part number SS-SSLVPN. Printed in USA 08/08. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©2008 Motorola, Inc. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.