



Your Checklist: Seven Steps to Secure and Seamless Field Mobility



Introduction

Now more than ever, companies are deploying mobile applications to drive competitive advantage and increase profitability. Only in the U.S. more than 47 percent of the workforce is mobile, spending more than eight hours per week away from their workstation or desk, according to statistics released by the Bureau of Labor Statistics in 2006. IDC predicts that nearly 75 percent of the U.S. workforce will be mobile by 2011.

Beyond remote e-mail access and point-specific wireless applications, today's enterprises are mobilizing core business solutions with strategic enterprise value. The business advantage is enormous, but the mobilization of the workforce also exposes organizations to increased risk and a new set of challenges unique to the wireless world.

Virtual Private Networks (VPNs) based on Internet Protocol security (IPsec) and Secure Socket Layer (SSL) have long been used to provide secure remote access to the enterprise network for employees and consultants working remotely. However, traditional VPN technology has its roots in wired computing and does not perform well in a wireless environment with limited bandwidth and unstable connections. A new generation VPN based on Transport Layer Security (TLS), called the mobile VPN, has instead evolved to handle both the requirements of the wired and wireless world.

This white paper examines the unique challenges of the wireless world and the reasons why a mobile VPN is more capable of handling remote access in a true mobile scenario than the old VPN technologies.

The Third-Generation of Mobility

With mobile workforce enablement and wireless technologies now being mandated as a critical business priority, IT organizations must rapidly advance to third-generation mobility.

Whereas first- and the second-generation mobility technologies were focused on e-mail access and wireless point-solutions, third generation mobility demands an ubiquitous mobile workflow that is seamlessly integrated into existing business processes and backend systems — allowing transparent wireless access to all enterprise applications from any network without requiring system modifications or new hardware. At the same time, next-generation mobility demands bulletproof security and effortless compliance with audit trail requirements mandated by Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standards (PCI DSS), and other regulations.

Security Is the Missing Link

Most companies have invested heavily in IT security for their office employees and laptop users, but mobile workers using smartphones or mobile computers have been neglected. A majority of mobile devices do not comply with government regulations or organizations' internal IT security policies and are often the network's weakest link. In fact, fewer than 10 percent of companies currently deploy mobile security suites even though such security suites have been shown to be highly effective in stemming data loss, according to Gartner Group research.

As businesses demand more information to be made available to their field employees, mobile devices are becoming more vulnerable to hackers and other threats. A security breach is not only damaging to a company's reputation, but can lead to financial loss through lawsuits, regulatory fines, and customer retention failures.

Organizations need to approach wireless security with the same sense of urgency they give to securing their wired infrastructure, and they need to understand the unique challenges of the wireless environment.

The Third-Generation VPN

In today's mobile world — where bandwidth is limited, connections are unstable, roaming is common, battery life is critical, and security is urgent—it's imperative to deploy a VPN solution that stands up to the most demanding wireless challenges. Beyond just another VPN, a third-generation VPN is based exclusively on TLS — and is optimized specifically for low-bandwidth networks and mobile devices. It offers all the functionality of the SSL and IP Sec VPNs, but was built from the ground up for third-generation mobility and offers seamless security for any mobile device and application.

Your Checklist: Seven Steps to Secure and Seamless Field Mobility

This white paper examines the criteria that an IT department should consider when evaluating a wireless security solution for its mobile workforce, allowing these employees to work without fear and leverage the company's wireless investment to its fullest potential.

1. Does the solution support the three fundamentals of security?

When evaluating different security solutions for field force mobility, you want to ensure that the solution addresses the three fundamentals of security: authentication, encryption, and data integrity.

• **Authentication**

Authentication allows the recipient to identify the sender and trust that the sender actually sent the message. A strong security solution should support two-factor or multifactor authentication so that both the sender and the recipient are verified before exchanging data.

Authentication Methods

These are some of the authentication methods available:

- Domain username/password
- Client certificates
- RADIUS challenge/response
- RSA SecurID single-time password
- Smart cards
- Biometrics





- **Data Encryption**

Data encryption requires scrambling of transmitted data with a secret key to unlock or decode the encryption. To decrypt and read encrypted data, access to the secret key is required. Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES) offer the highest level of security and are used by government and financial sectors.

- **Data Integrity**

Integrity refers to the validity of data. Integrity can be compromised by malicious altering on the part of a hacker, through transmission errors, or because of a hard disk crash.

A trustworthy security solution should validate that data has not been modified during transit, and it should automatically eliminate any changed data packages.

2. Is the solution based on a standard security protocol?

Several VPN solutions meet the three fundamentals of trustworthy security. However, a VPN that is based on a standard security protocol

is always preferred, since it has been tested and validated. Proprietary technology exposes the company to unknown risks and may increase the risk of a security breach.

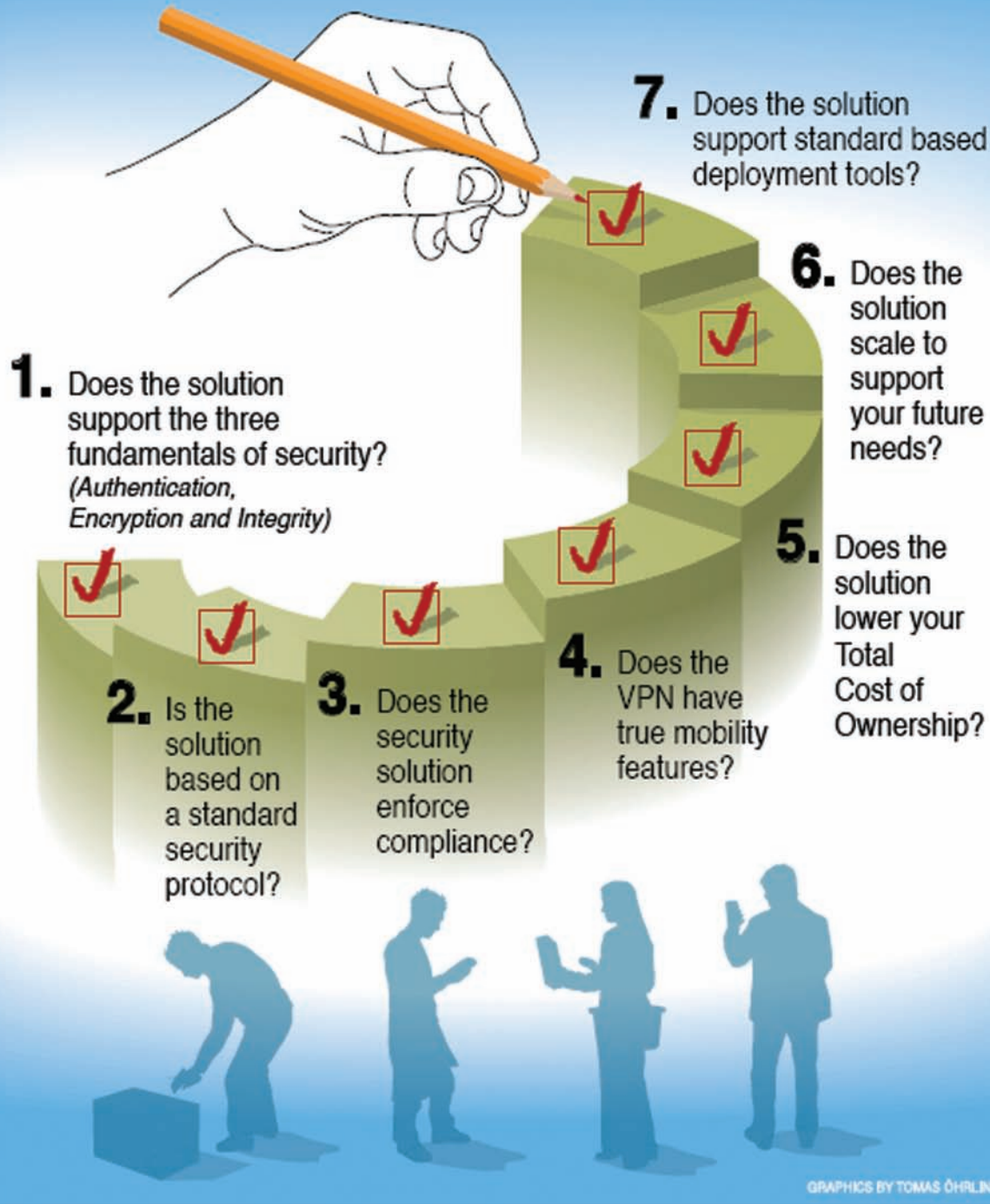
3. Does the security solution enforce compliance?

With a growing mobile workforce, the ability to manage and control wireless devices is essential. IT administrators must have the ability to establish, enforce, and update mobile device settings to ensure regulatory compliance with regulations such as SOX, HIPAA, and PCI DSS.

Accordingly, it is important that the VPN supports Network Access Control (NAC), ensuring that connecting devices are authorized to access the network and are compliant with the company's security policy. Devices that don't comply can be quarantined, thereby protecting networks from unauthorized access and virus attacks.

In the event of an audit, the company must prove compliance, and it is therefore a necessity that the VPN solution offers a complete record of all network events, including a time stamp and information about the connecting device, and the user ID.

Your Checklist: Seven Steps to Secure and Seamless Field Mobility



Field Mobility Users

Field mobility users are defined as any group of employees, contractors, or partners whose primary or exclusive workplace is in the field and whose success depends on using smartphones, laptops, and other mobile devices to access enterprise applications outside the four walls of an office.

These users include:

- Business executives
- Sales representatives
- Consultants
- Service technicians
- Truck drivers
- Utility inspectors
- Police, Fire, and EMT

Now that the basics of security have been explained, this white paper will focus on the specific challenges of a wireless environment and what impact they have on the security solution. It is in this area that third-generation mobile VPNs, based on TLS protocol, provide considerable advantages as compared to traditional SSL and IPsec VPNs.

4. Does the VPN have true mobility features?

Field mobility with remote access via WiFi hotspots, WiMAX, GPRS, 3G, EDGE, and other wireless networks from a small mobile device or a laptop, presents a new set of challenges that do not exist in a wired networking environment.

First- and second-generation VPNs are based on SSL and IPsec. Both technologies offer strong security, but with roots in wired networking, they do not offer the mobility features required for an effective field mobility application.

The third-generation VPN is a mobile VPN that is based on the TLS protocol and it is optimized for wireless networks and mobile devices. It offers the same level of security as the SSL and IPsec VPNs, but was built from the ground up for true mobility and offers all the wireless functionality that makes a field mobility deployment successful.

Some of the most critical challenges to consider in a wireless environment are:

- **Roaming**

One of the key factors for a successful field mobility deployment is that the security solution must offer a seamless user experience as the user moves around. Seamless roaming helps users remain continuously connected as they cross network boundaries and use different radio access networks.

Automatic roaming is essential as the device switches networks, moves in and out of coverage, and hibernates.

The Currently deployed SSL and IPsec VPN technology, with roots in wired networking, is not up to the challenges of the wireless world and will have a negative impact on productivity. It does not offer seamless roaming and the user will therefore be forced to log in and reauthenticate every time the device loses the connection.

The new generation mobile VPN is built from the ground up for the wireless world and offers seamless, secure roaming among networks with no interruptions for the user. The device automatically switches networks, creating an always-connected scenario for the user and the application. Individual or user group based policies can be used to limit or prioritize among available connections.

- **Session Persistence**

Unstable connectivity is common in the wireless environment, and mobile devices will sometimes lose the connection or hibernate to save battery power. Session persistence with transaction recovery is therefore critical to a successful implementation.



The First- and second generation VPNs do not handle the unstable wireless connectivity well. They will prompt users to log in and authenticate every time the device loses the connection or hibernates and data may be lost if the signal disappears — with a significant negative impact on productivity and tremendous user frustration.

In contrast, the mobile VPN offers session persistence without the need to reauthenticate or restart the application after a lost signal, change of network type, or hibernation mode.

It also recovers all the data after a lost signal or hibernation mode, ensuring that data is never lost.

- **Data Compression**

With limited bandwidth available, advanced data compression is an important feature that increases the performance of the applications over low-bandwidth networks. Data compression minimizes the the amount of data being transferred, allowing field organizations to lower their data rates, which can be a potential large cost saving for a company with hundreds or thousands of employees.

First- and second-generation VPNs do not support advanced data compression and will not perform well over slow network speeds. The lack in performance will slow down applications and response times, adding user frustration and resulting in negative impact on productivity.

The new mobile VPN supports advanced data compression with up to 60 percent higher throughput than a regular VPN. The increased throughput also allows applications to run effortlessly when accessing data over low-bandwidth networks. This feature considerably improves user experience and productivity. Additionally, it provides cost benefits since less data is being transferred.

- **Limited CPU Power**

Generally speaking, mobile devices are equipped with smaller processors than desktop computers or laptops. Therefore, it is critical that the security solution require minimal processor power so that it does not slow down other applications running on the machine.

The First- and second generation VPN technologies were built to protect wired computers with powerful processors. This kind of security solution requires more processing power and will slow down other applications running on a mobile device.



The mobile VPN is optimized for mobile devices and uses much less processing power than the old VPN technology, which will considerably improve the speed of the device and extend its battery life.

- **Memory Footprint**

Mobile devices such as smartphones, mobile computers, and PDAs have limited memory space. The memory footprint of the security solution is important to ensure that there is memory dedicated to business-critical applications.

With memory footprint requirements as low as just 70 Kb, the mobile VPN does not consume valuable storage space from other applications. The efficient use of memory space allows the third generation mobile VPN to operate seamlessly and smoothly.

Critical Mobility Features

The wireless world presents unique challenges that are not critical in the wired computing world. A true mobile VPN solution must meet the following requirements:

- Seamless roaming among different networks
- Session persistence
- Advanced data compression
- Limited usage of CPU power
- Small memory footprint
- Minimal battery consumption

3G Mobility: Mobile Workflow

First-generation mobility

Remote e-mail access

Second-generation mobility

Point-specific mobile applications
(e.g., field service electronic forms)

Third-generation mobility

Ubiquitous mobile application access and mobile workflow

3G VPN: Optimized for Wireless

First-generation VPN

IPsec

Second-generation VPN

Secure Socket Layer (SSL)

Third-generation VPN

Transport Layer Security (TLS) / Mobile VPN

The traditional VPNs use several hundred percent more memory space than a mobile VPN, based on TLS, and are therefore not efficient to deploy on a mobile device with limited memory space.

- **Battery Consumption**

The security solution's impact on the battery consumption is another important factor to evaluate. In field applications, battery life is critical, and it is important that the battery lasts for the entire workday. The ability for the device to hibernate to save battery power without losing the VPN connection has a large impact on the operating time and thus becomes important.

Due to the lack of ability to hibernate without losing the network connection, traditional VPN technologies, such as SSL and IPsec, will considerably shorten the operating time of the device. With no ability to recharge, this can have a negative impact on both productivity and customer satisfaction.

A true mobile VPN provides session persistence and data recovery, allowing the device to hibernate when it is not being used. This considerably prolongs the operating time from each battery charge to the next, and extends the total life of the battery.

The mobility features of a mobile VPN does not only provide a much better user experience, but they also return real cost advantages compared to the old VPN technology. The third generation mobile VPN offers considerable cost benefits that will lower your total cost of ownership (TCO).

2. Does the solution lower your TCO?

In the end "money talks," and therefore the total cost of ownership always will have a large impact on the purchase decision. These are some of the cost benefits of the third-generation mobile VPN solution compared to the first- and second-generation VPNs.



Mobile VPN Cost Advantages

- Secures all fixed and wireless computers with one VPN, resulting in considerably lower management and maintenance costs.
- Allows the use of existing servers, with no need for additional hardware.
- Application transparent — no expensive software changes.
- Simple to use — no extra cost for training or support.
- Improves the throughput by up to 60 percent, which will help reduce data fees.
- No time-consuming extra log-in procedures or lost data if the device lose the connection, roams or hibernates.

The third-generation mobile VPN:

- Allows you to efficiently manage and secure all your devices that need remote access, including desktop computers, laptops, smartphones, and PDAs, with one solution — and with only one open port in the firewall. With only one VPN solution to manage, it will dramatically lower your costs for maintenance and support.
- Is software based, allowing for easier updates and maintenance of the VPN software.
- Has a small server footprint and does not require any additional hardware to be installed. The software can be installed on existing servers and supports virtualization.
- Is application transparent and does not require any costly software changes. The third-generation VPN provides a security platform that can be leveraged for any existing or future applications.
- Increases productivity thanks to session persistence and seamless roaming, which can add up to a considerable time savings over the course of a day.
- Supports advanced data compression with up to 60 percent increased throughput over wireless networks. This both improves productivity and reduces the amount of sent data, helping organizations to lower their fees for data traffic.
- Uses less battery power, prolonging the operating time from each battery charge as well as the lifetime of the battery.

- Is transparent to the user and does not require any training, nor will it generate costly support calls.

6. Does the solution scale to support your future needs?

Whether your field organization consists of a couple of service technicians or thousands of field sales representatives, you want to ensure that the field mobility platform can scale with your organization's needs whenever you add more users or allow them to access new applications.

To make the best enhancement to your system, you must first evaluate whether your mobility solution needs to support only Web-based applications and access to e-mail, or if access to CRM, ERP, and multiple applications is important. Many security solutions can provide access to e-mail and Web-based applications, but few grant transparent and seamless access to your mission-critical enterprise back-end systems, such as CRM and ERP.

The traditional SSL VPN delivers remote network access from a Web browser, which requires adjustments on the application level. A true mobile VPN based on wireless TLS provides application transparency and will not demand any modification of the software. The application-transparent mobile VPN offers greater flexibility. The mobile VPN is easy to scale as new business demands access to more applications and systems.



7. Does the solution support standard-based deployment tools?

The SSL VPN is often referred to as “clientless” since it does not require any client software but only allows limited remote access through the web browser. Both IPsec and TLS VPNs are software based and the software needs to be installed on each device. Easy-to-use standard deployment tools are therefore very important.

With field mobility users spread in many different locations, you want to make sure that the VPN solution supports standardized easy-to-use deployment tools and that it supports MS certificate storage for efficient distribution of certificates. Some security solutions require the use of proprietary deployment tools, which will add complexity, and in most cases, raise the cost for the deployment.

Furthermore, it is important that the VPN is easy to use and preferably seamless to the user. This simplifies the deployment by eliminating time and money spent on end-user training and support calls.

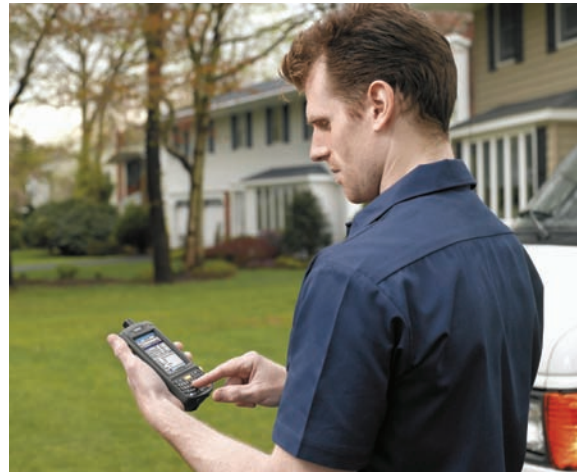
Conclusion

Thus far, security for mobile computers and smartphones have been neglected, but with increasing pressure to get access to mission critical business systems, security must be addressed. Compliance requirements such as SOX, PCI DSS, and HIPAA also demand that companies address this issue to avoid costly regulatory fines and lawsuits.

There are many trustworthy security solutions available, but it will pay off to take the extra time to evaluate and compare different solutions. If field mobility is important to your organization, look for a standardized security solution that offers true mobility features such as session persistence, advanced data compression, and seamless roaming. Make sure you invest in a solution that is scalable and application transparent so that it can meet your future needs in terms of adding more users or applications.

Additionally, a new mobile VPN offers several cost advantages compared to the first- and second-generation VPN technology, such as lower data fees, no additional cost for new hardware or software changes, and lower maintenance costs.

By the seven steps covered in this white paper, you will ensure that you invest in a trustworthy and cost-efficient VPN solution for your fieldbased workforce that will help reduce cost and increase productivity instead of having to pay for costly maintenance contracts and aggravating your IT department and your users.



The AirBEAM Safe Offering

Developed by Columbitech for Motorola Mobile Computers, the AirBEAM Safe/SSL Mobile VPN seamlessly maintains the integrity of the business information that mobile workers access remotely — protecting both your company’s and customers’ sensitive, confidential data.

Beyond just another VPN, it is the third-generation VPN-based exclusively on the TLS protocol, and optimized specifically for low-bandwidth wireless networks and mobile devices.

Because of its wireless roots, AirBEAM Safe/SSL Mobile VPN offers exceptional reliability and performance not only in a wired network environment, but also in today’s dynamic mobile world. It offers seamless roaming and session persistence, which are critical for all mobile users, and the solution is application transparent so it can scale with your future needs. AirBEAM Safe/SSL Mobile VPN uses advanced data compression to provide good performance even over slow network connections, and by reducing the amount of data being sent, organizations can lower their costs for data fees.

Furthermore, AirBEAM Safe/SSL Mobile VPN has a very small footprint and requires minimal processing power, which will help increase the device’s operating time after a battery charge.

AirBEAM Safe/SSL Mobile VPN offers all the advantages of a traditional VPN, but with additional mobility features that will raise productivity and improve the user experience — all for a smaller initial investment and at lower TCO.

More Information

For more information about AirBEAM Safe, visit www.motorola.com/sslmobilevpn





Columbitech, the world's most deployed mobile VPN provider, enables fearless enterprise mobility and unleashes the power of wireless. Its software solution offers seamless security for any mobile device and application, with support for WLAN and public networks, including 3G, 4G, and WiMAX. The Columbitech solution provides transparent access to enterprise applications from any network, without requiring any changes to hardware. More than two million clients are already secured by Columbitech.

© Columbitech, Inc. 2008. All rights reserved.



MOTOROLA

motorola.com

Part number WP-7STEPCHECK. Printed in USA 09/08. 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. ©Motorola, Inc. 2008. 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.