



SECURE MOBILE ACCESS USING SSL VPNs

September 2005

**Prepared by Peter Rysavy
<http://www.rysavy.com>
1-541-386-7475**

Executive Summary

Remote access has become increasingly complex. It's no longer about traveling executives wanting access to e-mail or data while on the road, but rather about employees, partners, and customers demanding access from a wide range of environments and Internet-capable devices. Increasingly, mobile workers want access to corporate resources from mobile devices, such as smartphones and wireless PDAs. These devices are powerful mobile computers with the ability to access a wide variety of information on your network, through both Web and client/server applications. Businesses today face the challenge of effectively securing mobile access and providing access only to those resources appropriate for particular users and devices. Aventail offers an SSL VPN with features specifically designed for mobile devices that address common challenges faced by organizations. The Aventail® Smart SSL VPN, which incorporates the Aventail Secure Mobile Access Solution:

- Uses industry-proven methods for user authentication and data encryption.
- Supports mobile access for both handheld devices and notebook computers on a single security platform, unlike competing approaches that require two independent mobile access architectures.
- Accommodates the specific needs of mobile device users by providing a user interface tailored for small devices.
- Customizes access to information so that it is appropriate for the particular device used for access.
- Provides two forms of access with one form allowing any device with a Web browser to access information and the other form providing a small client that can be downloaded via a Web session, which enables full client/server interaction.
- Includes a comprehensive management and administrative tool that allows you to control access with a high degree of granularity.

With the Aventail SSL VPN, one security architecture protects all forms of remote access, including access from handheld devices and notebook computers. If you are already using mobile devices that have their own communications architecture for applications such as push e-mail, however, you can use Aventail Mobile solutions to extend the range of applications and data available.

Introduction

The ways that mobile and remote workers are accessing corporate resources continues to expand. Remote access used to consist mostly of dial-up connections. Now, remote access encompasses a wide range of networking options, including home networks, public Wi-Fi networks, and 3G cellular networks. At the same time network connectivity options are increasing, the types of mobile devices used for access are expanding as well.

Company-issued laptop computers were once the primary means of remote access, but now workers also want access to corporate resources from home systems, public terminals, and a variety of mobile devices, such as wireless PDAs and smartphones. Although organizations provide many such devices for their employees, it has become common for individual users to purchase their own mobile devices for both business and personal use.

Practically every mobile phone now has a micro browser, which can potentially be used to access corporate resources. In addition to access provided by mobile phones, more powerful smartphone and PDAs today offer complete multi-tasking operating systems, have highly capable browsers, include full-featured e-mail clients, and can support sophisticated client/server transactions. The leading mobile device platforms include Linux, Windows Mobile, Palm OS, RIM Blackberry, and Symbian.

The challenge enterprises face is how to most effectively secure communications from all of these different devices, address the multiplicity of networks used, and tailor resource access according to user identity and the security level of both the device used for access and the given access environment. Any security solution must also include stringent authentication methods, use proven encryption algorithms, limit what enterprise resources can be accessed from particular devices, and provide an effective and immediate means of disabling access in the event that a user loses his or her mobile device.

As an organization, there are a number of mobile access options available to you, each with their strengths and weaknesses. This white paper discusses some of the most common remote access approaches and shows that—for many companies—an advanced SSL VPN architecture can accommodate the widest range of devices used for accessing the network. Supporting virtually any type of mobile device requires that specific provisions be made in the SSL VPN to accommodate access from handheld devices. Currently, the Aventail Smart SSL VPN, which includes Aventail Mobile technology, is the only SSL VPN that incorporates such provisions.

Mobile Device Capabilities

To understand when to apply a particular remote access approach, it is helpful to consider the most common types of mobile devices and to understand their capabilities. Unlike the notebook computer platform that has become a relative commodity, smaller form-factor devices are still very much a work in progress, with a wide range of capabilities, multiple operating systems, significant variations in form factors, and differing user interfaces.

Convergence of device types is unlikely as the devices themselves are designed to satisfy a wide range of specific usage models. For example, some individuals want devices that function primarily as a phone, which can also be used for occasional data transmission—perhaps to monitor incoming e-mail, but rarely to compose or send e-mail messages.

These users might prefer a form factor that is most similar to a standard phone, but that includes a microbrowser. Other users may need greater data access and would prefer a PDA-like device that has a keyboard and the ability to run client/server applications.

The following table summarizes the typical device options available today.

Table 1: Range of Capabilities in Today’s Mobile Devices

Most Common Form Factors	Mobile telephone with large display Mobile telephone that opens up like a clam shell with a large display and keyboard inside PDA without keyboard PDA with miniature keyboard
Typical Display Capabilities	160 X 240 pixels

	200 X 640 pixels 240 X 320 pixels 320 X 320 pixels
Operating Systems	Linux Palm OS RIM Blackberry Symbian Windows Mobile Proprietary systems
Application Execution Environment Options	Binary Runtime Environment for Wireless (BREW) Browser based Java Native applications (C++)
E-Mail Capabilities	Browser based Client that supports Microsoft ActiveSync Client that supports Internet protocols (POP3, IMAP) Client that supports RIM Blackberry protocols
Browser Capabilities	Wireless Markup Language HTML xHTML JavaScript SSL

The conclusion that one can draw from the table is that today's mobile devices are powerful, but that considerable variation exists among them. However, they all have two things in common—TCP/IP-based data networking and the ability to provide access to corporate information. Much of the initial focus of mobile access has been on e-mail and remote calendar synchronization, but many companies are now beginning to see the benefit of making additional information available to mobile workers who use handheld devices. Examples of recent offerings include inventory control, client database, customer relationship management, project management, sales force automation, and real estate applications.

However, to be useful and successful, any mobile access system must address specific user needs and requirements of particular mobile devices.

Mobile Device Remote Access Needs

There are several approaches used today for providing mobile access. Before comparing the benefits of these approaches, it is important to understand the needs that each approach must satisfy. These are as follows:

- **Fully Secure.** The remote access system must use industry-proven methods for user authentication and data encryption. Authentication methods must be strong enough to address the possibility of users losing their mobile devices. Encryption must be able to prevent eavesdropping on the radio link, especially when operating over a Wi-Fi connection. Encryption must also protect Internet communications.
- **Common System for All Mobile Devices.** It is highly beneficial for the mobile access system to support both notebook devices and a wide range of handheld devices, including phones and PDAs.
- **Accommodate the Specific Needs of Mobile Device Users.** The system should provide a user interface tailored to the small displays of mobile devices and should only provide access to the subset of corporate information that is relevant to a particular mobile device.
- **Highly Granular and Easy to Manage.** It should be easy for administrators to set granular access control rules, specifying what resources users can access based on policy. This improves the user's experience, as the user only sees relevant information. In addition, it limits exposure in case devices are lost. Management tools should also make it easy to disable access if necessary.
- **Support the Unique Requirements of Wireless Networks.** Wireless connections are not as stable as wireline networks. The mobile access system should tolerate short-term connectivity disturbances.

Mobile Access Architectures

There are a number of different approaches vendors employ for mobile access. In the PDA and smartphone arena, some of the solutions are designed specifically for these particular mobile devices. Examples of vendors using this approach include Extended Systems (Sybase), Good Technology, Intellisync, JP Mobile, RIM, and Seven Networks. The primary emphasis of these systems is to provide push e-mail, where new e-mail messages are automatically sent to the device. A secondary emphasis is calendar and contact database synchronization. These vendors are also working to make other corporate information available to mobile device users, but generally this is done through proprietary methods requiring third-party applications or custom programming. Many of these mobile-specific architectures provide centralized management tools and most offer behind-the-firewall gateways to implement their systems. Some also offer their solutions to cellular operators who implement the gateways in their networks and sell access for additional monthly fees.

While these specific solutions may be beneficial—particularly for companies deploying a very large number of handheld devices where the management aspect becomes paramount—they require network administrators to manage a completely separate mobile access system from the remote system used by telecommuters and notebook computer users.

An alternative approach is to use an IPSec VPN for access from handheld devices. The limitation is that VPN clients are only available for a limited number of mobile devices and

require the installation of client code for access as well as ongoing management and support.

In the SSL VPN architecture, you leverage the SSL security protocol of a standard Web browser, enabling secure access from any device. All smartphones and wireless PDAs have browsers that can communicate with an SSL VPN security gateway that is installed on your network. This architecture can support any form of mobile device. And you only have to manage one access system. Moreover, you do not have to install any client software on mobile devices in order for them to be used for accessing the network.

An Overview of Aventail Mobile

The Aventail Secure Mobile Access Solution is an SSL VPN. It differs from traditional IPSec and other SSL VPN solutions in that it supports remote access from any device. And it also supports internal access from untrusted nodes within the organization, such as a notebook computer connecting to the network via a Wi-Fi connection. The SSL VPN offers the advantage of providing access with only one URL, which specifies the portal interface depending on whether the user is accessing the gateway via a notebook computer, public terminal, home computer, PDA, or smartphone. The administrator also uses the same centralized policy model for managing all of the devices used for access. This is in sharp contrast to many mobile access architectures that are fully separate from laptop-based remote access solutions.

Using the Aventail SSL VPN does not preclude use of other mobile access architectures such as RIM Blackberry. In some scenarios, it makes sense to use both, with the SSL VPN providing access to general-purpose applications and data, and the other solution providing capabilities such as push e-mail.

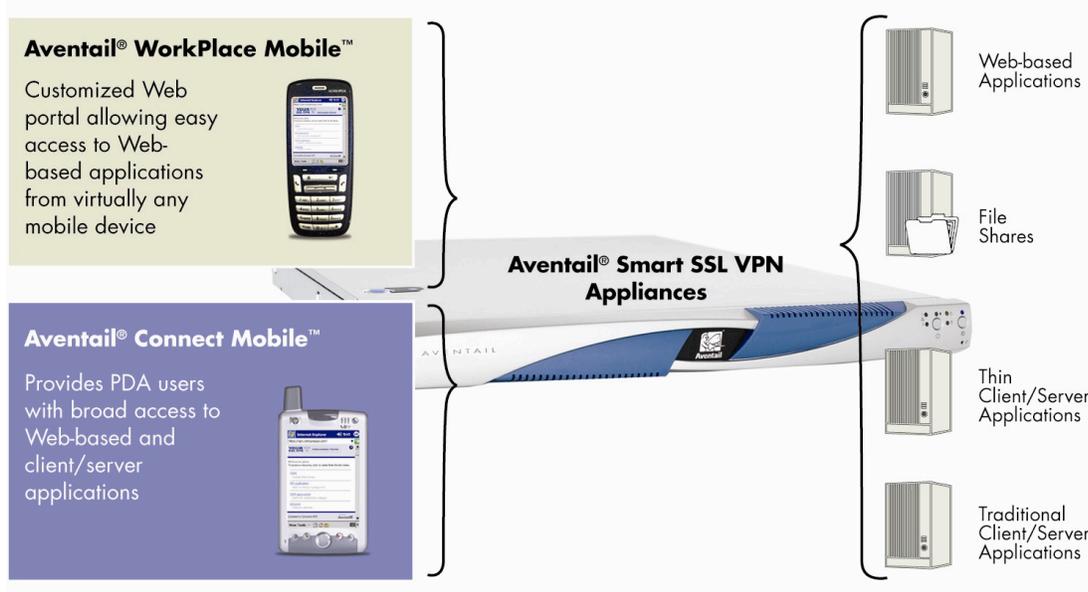
The Aventail SSL VPN provides SSL-based encryption, user-level access control, and stringent user authentication, including RSA SecurID tokens and digital certificates. Mobile devices are only allowed access based on user identity and the security of the device used. In addition, access is limited to named resources and there is no direct connection to the enterprise network.

With the ability to recognize the different capabilities of various mobile devices, the Aventail SSL VPN is tailored specifically for mobile access. It provides two different mobile access options: Aventail® WorkPlace Mobile™ and Aventail® Connect Mobile™. WorkPlace Mobile is a mobile-optimized portal designed for unmanaged devices that provides access for Web-based applications from any mobile device. The portal presents customized content based on user permissions and the type of device used. Palm OS, RIM Blackberry, Symbian, WAP browser, and Windows Mobile devices are all supported.

In contrast, Connect Mobile uses a small Web-deployed client that provides Windows Mobile PDA users broad access to both Web and client/server applications through a proxied connection, preventing direct access to your network. Highly granular control ensures that users only gain access to relevant content. Users who have not previously downloaded the Connect client can do so from the WorkPlace Mobile portal.

The following figure shows the two approaches.

Figure 1: Aventail WorkPlace Mobile and Aventail Connect Mobile



Key elements of any remote access solution include centralized policy and access control. Aventail Mobile technology, which is fully integrated into the Aventail® Unified Policy™ model, makes it easy for administrators to set granular access control rules and to control mobile devices used to access network resources. The administrator can specify the exact resources available to mobile device users.

The end result is a remote access system that accommodates all types of mobile devices. The total cost of this approach is less than other approaches, because it is less time consuming to manage.

In conclusion, the Aventail SSL VPN can provide broad network access from virtually any mobile device that's both simple for users and for IT. With Aventail remote access, your users will be able to work productively no matter where business takes them.

About Aventail

Aventail is the best-of-breed SSL VPN technology company and the authority on secure application access. Aventail delivered the first SSL VPN solution in 1997. And today, Aventail meets the secure communication needs of more than 1 million end users globally. Aventail's family of SSL VPN appliances increases productivity for end users and IT professionals, while maximizing security and lowering costs. Aventail appliances lead the industry in End Point Control, policy management, and transparent, easy-to-use access options to the broadest range of applications. Aventail is the SSL VPN of choice among leading enterprises and service providers worldwide, such as AT&T, DuPont, IBM Global Services, MCI, Office Depot, Sanyo, and TNT. For more information, go to www.aventail.com.