

# GoToMyPC™

GoToMyPC:

Making Life Simpler for  
Teleworkers and Travelers

**expertcity®**

© 2001 Expertcity, Inc. All Rights Reserved.  
Confidential Property of Expertcity, Inc.

5385 Hollister Avenue Santa Barbara, CA 93111 Voice: 805.690.6400 Fax: 805.690.6471

## GoToMyPC: Making Life Simpler for Teleworkers and Travelers

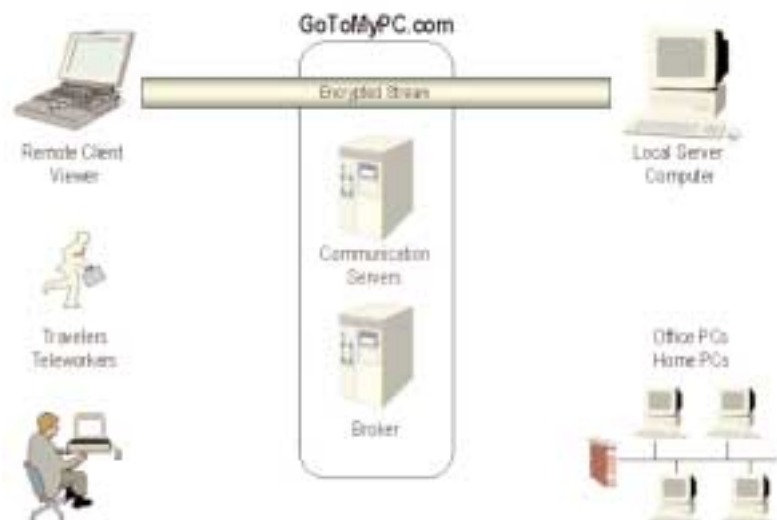
Today, providing teleworkers and travelers with remote access to corporate networks is no longer a luxury - it has become a business necessity. Letting employees tap into the office LAN from customer sites, hotels, Internet cafés and airport kiosks can greatly increase business efficiency and productivity. But mobile empowerment has a price, measured in IT administration and network security. GoToMyPC, a new remote-access service from Expertcity, intends to change that.

### Yes, You Can Get There from Here

GoToMyPC is a hosted service that enables secure browser-based access to any Internet-connected Windows PC. The current release supports screen sharing, file transfer, remote printing, guest invite, chat applications and a Universal Viewer, which allows viewing of a Windows PC from a Windows, Mac or Unix PC.

Unlike other solutions, GoToMyPC screen sharing does not require permanent client software or network change. A resizable viewer, launched from any browser with a 56Kbps Internet connection, enables interactive access to any desktop application (even those that are not Web based). Transfer sends and receives files, folders and directories, including those located on LAN-connected fileshares. Chat supports text dialogs between client and host users, useful during help desk access to teleworker PCs. Remote printing allows printing to a client printer from the host computer Viewer. Third parties can also be granted temporary "guest view" access to a GoToMyPC-enabled desktop.

The technology behind GoToMyPC evolved from DesktopStreaming, an Expertcity-hosted customer support service used by large, well-known companies like Sun Microsystems, Gateway, Intuit, and CompUSA. GoToMyPC's client viewer and desktop server are robust Win32 applications, designed from the ground up for efficient, secure communication over any network. Keyboard, mouse, and display updates are transmitted over a highly compressed, encrypted stream, yielding "good as



there" experience over broadband and impressive performance over dial-up.

Figure 1: GoToMyPC Architecture

Under the covers, GoToMyPC is a hosted service, composed of four components (see Figure 1). A small footprint server is installed on the computer to be accessed: typically, a home or office PC with always-on Internet access. This server registers and authenticates itself with Expertcity's GoToMyPC broker. For network address and firewall independence, the server initiates all communication with the broker, issuing HTTP "pings" to check for new connect requests.

On the client side, the remote teleworker or traveler launches a browser, visits Expertcity's secure Web site, enters username/password, and clicks on a "connect" button for the desired server, sending an SSL-authenticated, encrypted request to the broker. Of course, for security reasons, only computers configured with this username are displayed.

The GoToMyPC broker is a matchmaker - it listens for connect requests, mapping them to registered computers. When a match occurs, the broker assigns the session to a communication server. The client and server are supplied with the communication server address and a unique session ID. At this point, the client viewer - a tiny session-specific executable - is automatically loaded by the browser's Java Virtual Machine.

The communication server relays an opaque, highly compressed, encrypted stream from client to server. The client and server mutually authenticate each other, using a shared secret (a computer access code) known only to them. For scalability, reliability, and optimum performance, the broker load-balances sessions across a pool of geographically distributed communication servers.

### **Reduce Administrative Costs**

GoToMyPC enables secure remote access quickly, seamlessly, almost effortlessly. Other VPN solutions try to duplicate a worker's office desktop on a home PC or laptop by tethering remote hosts to the corporate LAN over IPsec, L2TP or PPTP tunnels. GoToMyPC leverages a worker's existing office desktop by providing secure user-to-PC access. With screen sharing and sufficient bandwidth, employees can have exactly the same desktop environment, whether working at the office, at home, or on the road.

On the client side, even the most basic PC or Mac or any workstation running Unix can be used as a remote monitor, keyboard and mouse. Because it requires just a browser, GoToMyPC can even run on public PCs. On the server side, the worker's existing PC does all the heavy lifting - providing CPU, memory, disk, enterprise applications and native access to the corporate LAN. Screen sharing eliminates the need to install enterprise application and VPN client software on remote PCs, significantly reducing client administration complexity and cost.

With a hosted service like GoToMyPC, there's no need to operate a private RAS pool or install a VPN access concentrator. Like traditional VPNs, GoToMyPC can leverage the public Internet to slash recurring telecommunications costs associated with remote access. However, many IPsec, L2TP, or PPTP VPNs - including those outsourced to managed security providers - require a gateway device to be installed at the edge of the enterprise network. Installing a VPN gateway can be tricky, requiring changes to existing enterprise network addresses, routes and firewall rules.

GoToMyPC is an end-to-end solution, designed to completely avoid enterprise network impact.

Other VPN solutions fail to recognize that network-independence is important to both client and server. Travelers working at a customer or business partner office, staying in a hotel with broadband Internet access or using a public PC often find these environments hostile to IPsec clients, but not GoToMyPC. Its protocol design is compatible with dynamic and static IP addresses, network and port address translation (NAT/PAT) and firewalls that block incoming sessions.

### **Keep It Secure**

Today, some workers use products like pcAnywhere to get around LAN security by dialing directly into office PCs. GoToMyPC eliminates this temptation by using the Internet, securely.

With GoToMyPC, there is no need to punch holes through corporate firewalls. All connections are initiated by the client and server, using outgoing TCP ports frequently left open: 80, 443, and/or 8200. GoToMyPC encapsulates all traffic - even encrypted packets carrying proprietary protocol - inside standard HTTP wrappers, ensuring compatibility with firewalls that inspect payload. IPsec, L2TP - even SSL-based services like uRoam and eTunnels - usually require firewall adjustments. Instead, GoToMyPC adjusts itself to the firewall. However, enterprises that want firewall control over GoToMyPC can do so easily, using IP-level filters for Expertcity servers.

GoToMyPC uses multiple, nested passwords to keep outsiders away. The broker authenticates itself with a digital certificate; it also digitally signs all Java applets and software. Clients authenticate themselves by username/password, exchanged over SSL, with a three-strikes rule (account disabled for five minutes after three failed login attempts). When servers register with the broker, each is assigned a unique random number. Servers authenticate themselves by signing their number with MD5 and username/password. Thereafter, the broker and servers exchange MD5 challenge/response messages, based on a sequence known only to the pair.

For added privacy, whenever a client connects to a server, they also authenticate each other, using a shared secret known only to the end user and the accessed computer, never seen or stored by Expertcity. Each endpoint generates a large random number, and digitally-signs that number with the computer's access code. This exchange also forms the basis for generating 128-bit session keys used to encrypt data.

GoToMyPC provides data confidentiality with a highly compressed encrypted stream that ensures confidentiality without sacrificing performance. GoToMyPC implements 128-bit Advanced Encryption Standard (AES) in Cipher Feedback Mode (CFB). AES was selected due to its computational efficiency, flexibility, simplicity, and security; it will soon become the US government's designated cipher for protecting sensitive information.

Desktop streaming and file transfer packets include a sequence number to prevent message replay attacks. These packets carry highly compressed binary data, framed in a proprietary protocol, encrypted with AES. A hacker cannot modify these packets without corrupting them. Because it is possible to modify encrypted text without corrupting it, chat packets also carry a signed MD5 hash to ensure message integrity.

Any third party (man in the middle) attempting to inject or replay packets would have to know both the session key and the current state of the AES engine. Lack of clear text makes it exceedingly difficult to "guess" the encryption key through traffic analysis. And of course, each key is good for just one session.

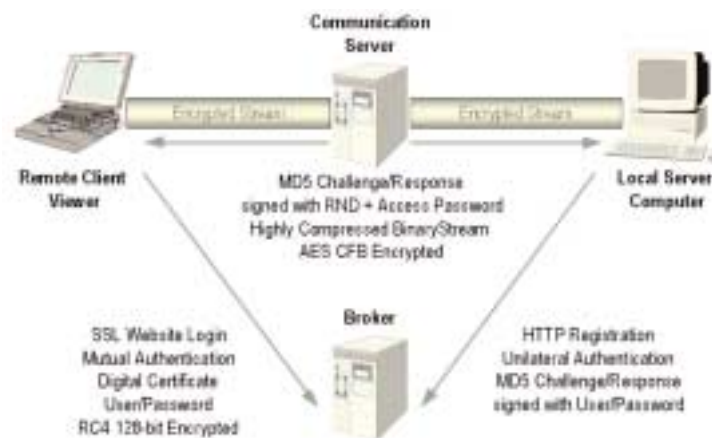


Figure 2: GoToMyPC Uses Authenticated, Encrypted Channel

One of the advantages of providing remote access through screen sharing is the ability to leverage the access controls already in place on the corporate LAN. When GoToMyPC connects, the remote user must enter a Windows login/password to access the computer and be granted file, host, and domain-level permissions associated with his or her account. In other words, the remote user does not have tunneled access to the enterprise network - he or she only has access to a single computer's desktop, and is subject to access controls already in place for that desktop. Host screen blanking and host keyboard/mouse input blocking increase the physical security of the computer being accessed.

It's also important that remote access sessions be terminated after inactivity. Remote users walk away from public PCs without logging out and leave home PCs unattended. GoToMyPC uses inactivity timeouts to help mitigate these threats. Users are automatically logged out of the GoToMyPC.com Web site when their SSL session remains inactive for fifteen minutes.

Expertcity plans several enhancements, including one-time computer access passwords based on S/Key, local computer keyboard/screen lockout during remote access, viewer inactivity timeout and further measures to safeguard against denial-of-service and man-in-the-middle attacks.

### Control Enterprise Access

Want to help a friend or relative diagnose PC problems from the comfort of your own home? Want to check email from your home PC while traveling? GoToMyPC Personal is an easy-to-use, turnkey remote-access solution for residential consumers. Online enrollment and browser-based activation require no computer expertise and can be completed in just minutes.

GoToMyPC Corporate makes this same easy-to-use remote access solution available to corporate end users. However, businesses require enterprise-class administration features. With GoToMyPC Corporate, IT administrators have complete control over secure remote access for groups.

Whenever the administrator modifies a user account, customizable mail messages are automatically generated. For example, when a new user is added (identified by email address), an invitation is sent containing a one-time-use self-activation URL. The user visits the URL, defines an individual password, then adds computers to his or her own account. This approach streamlines large scale deployment, while retaining enterprise control over remote access authorization.

Users add computers by visiting Expertcity's website from the host computer. The default install method requires just one click - a signed Java applet does the rest. Those who prefer to block Java or end users from installing software can install from a file instead. There is virtually nothing to configure - just enter username, account password and an access password (known only to the end user, the owner of the computer). Thereafter, GoToMyPC automatically keeps itself up-to-date.

GoToMyPC Corporate also provides real-time usage monitoring and historical reports. Administrators can view active and completed connections and summarize users, sessions, total time, and average duration over specified intervals. Further connection detail, logged by Expertcity, can be used for problem diagnosis. This kind of central visibility is essential for enterprise deployment.

The goal: keep GoToMyPC easy to use and simple to manage, but provide the ability to implement enterprise-defined security policies at global, group, and user levels.

## **Conclusion**

GoToMyPC is a very attractive solution for individual desktop remote access by trusted "corporate insiders." This service is well suited for extended use by broadband-enabled teleworkers and visiting workers with LAN access. Travelers limited to Internet dial-up can also use GoToMyPC for effective short-term access to PCs on the corporate network.

GoToMyPC over broadband is nearly the same as being back at the office. GoToMyPC over v.90 is fine for checking mail, browsing documents, using telnet or sending and receiving files. Depending upon Internet bandwidth, the application and duration of use, many road warriors will find GoToMyPC a truly effective remote-access solution. Travelers working at a customer or business partner office, staying in a hotel with broadband Internet access, or using a public PC at a conference, Internet café or business center will find remote access with GoToMyPC convenient and familiar.

But convenience need not sacrifice security and control. Enterprises jaded by pcAnywhere-style "back doors" and frustrated by complex VPN deployments may find GoToMyPC more secure, more cost effective, easier to administer and easier to use. GoToMyPC Corporate combines user-friendly desktop sharing with robust authentication, encryption and administrative tools - features that are absolutely essential in any enterprise remote-access solution.

**Prepared by:**  
Lisa Phifer  
Core Competence, Inc.  
[lisa@corecom.com](mailto:lisa@corecom.com)