

GoToMyPC™

GoToMyPC:

A Secure
Remote-Access
Solution

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

Introduction	-----	3
Security from the Ground Up	-----	4
Secure Facility	-----	4
Secure Network	-----	4
Secure Platform	-----	4
Secure Administration	-----	4
Scalable and Reliable Infrastructure	-----	5
Protecting Customer Privacy	-----	5
Published Privacy Policy	-----	5
Disclosure of Customer Information	-----	5
Access to Customer Information	-----	5
Ensuring Traffic Privacy	-----	5
Security Policy Administration	-----	6
Secure Management Interface	-----	6
Inviting New Users	-----	6
Suspending or Canceling User Accounts	-----	6
Secure Service Installation	-----	6
Digitally Signed Applications	-----	6
Firewall Compatibility	-----	7
Guarding Computer Access	-----	7
Protecting Confidential Data	-----	7
Advanced Encryption	-----	7
Strong Encryption Keys	-----	8
Protection Against Message Replay and Modification	-----	8
Defeating Man-in-the-Middle Attacks	-----	8
Authenticated Access	-----	8
Long, Complex Passwords	-----	8
Limited Number of Login Attempts	-----	8
Multiple, Nested Passwords	-----	8
End-to-End Authentication	-----	9
Inactivity Timeouts	-----	9
OS-Level Access Control	-----	9
Guest Invitation	-----	9
Limited Invitation Period	-----	9
Granting Access Required	-----	10
Share Control or View-Only Option	-----	10
Monitoring Access Within an Organization	-----	10
Monitoring Usage	-----	10
Detailed Session Logs	-----	10
Access Notifications	-----	10
Conclusion	-----	11

Introduction

GoToMyPC enables secure browser-based access to any Internet-connected Windows PC. 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. Applications supported by GoToMyPC include:

Screen Sharing: Launch a resizable viewer from any browser to enable interactive access to any desktop application (even those that are not Web based).

Guest Invite: Collaborate with colleagues by granting temporary access to a GoToMyPC-enabled desktop.

File Transfer: Transfers files, folders and directories between computers faster and more easily.

Chat: Dialog between local and remote users during collaboration or help desk access.

Remote Printing: Print from the host Viewer to your local client printer.

Java Viewer: Connect to your PC using any computer - Mac or PC - with almost any operating system, including Mac, Windows and Unix.

Under the covers, GoToMyPC is a hosted service, composed of four components:

Computer: 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.

Browser: 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 computer, sending an SSL-authenticated, encrypted request to the broker.

Broker: A matchmaker that listens for connect requests, mapping them to registered computers. When a match occurs, the broker assigns the session to a communication server. At this point, the client viewer - a tiny session-specific executable - is automatically loaded by the browser's Java Virtual Machine.

Communication Server: An intermediate system that relays an opaque, highly compressed, encrypted stream from client to server.

Protecting the integrity of the corporate network and the privacy of sensitive data is of utmost concern to any enterprise. Security is an essential ingredient when extending Internet-based remote access to corporate teleworkers and travelers. GoToMyPC Corporate was developed with these key security issues in mind, as illustrated in Figure 1 and described throughout this paper.

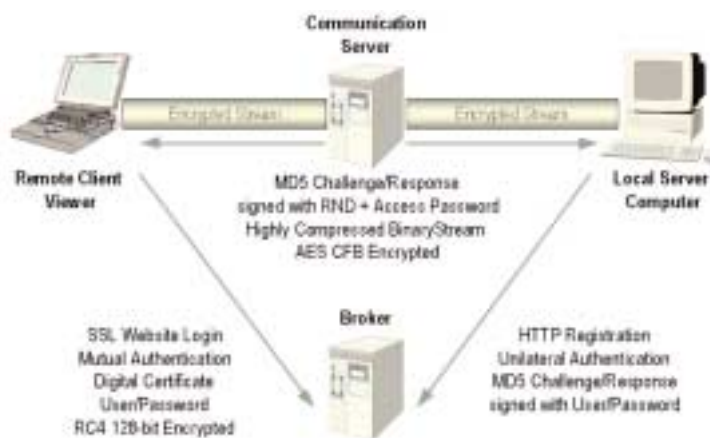


Figure 1: GoToMyPC's Security Architecture

Security from the Ground Up

Expertcity delivers GoToMyPC using an ASP model designed expressly to ensure robust, secure operation.

Secure Facility

All GoToMyPC Web, application, communication and database servers are hosted in a highly secured data center. Physical access to servers is restricted. The entire site sits in a locked cage, monitored by cameras. Expertcity's NOC in Santa Barbara is similarly protected by premises security.

Secure Network

Expertcity's access routers are configured to watch for denial of service (DoS) attacks and log denied connections. Multi-layer perimeter security is provided by a pair of firewalls: one between the Internet and Web servers, another between the GoToMyPC broker and backend databases. The security of this architecture has been independently confirmed by penetration tests and vulnerability assessments, conducted by an outside organization.

Secure Platform

Expertcity servers run on hardened Solaris 8 with the latest security patches installed. The entire service delivery platform is SunToneSM certified for quality and reliability. Servers have been penetration tested and system logs are continuously audited for suspicious activity.

Secure Administration

Expertcity servers are administered over a private T1 linking the secure data center to Expertcity's NOC in Santa Barbara. Secure Shell (SSH) supports authenticated, encrypted remote login access to Expertcity's NOC staff. To avoid opening ports and ensure very tight access control, an intermediate server handles and authenticates all SSH connections.

Scalable and Reliable Infrastructure

This infrastructure is both robust and secure. Redundant routers, switches, server clusters, and backup systems are used to ensure high availability. For scalability and reliability, switches

transparently distribute incoming requests among Expertcity Web servers. For optimum performance, the GoToMyPC broker load-balances client/server sessions across geographically distributed communication servers.

Protecting Customer Privacy

Expertcity understands that any enterprise outsourcing service delivery is concerned about privacy. Expertcity has a strong privacy policy that prohibits unauthorized disclosure of personal or corporate information to any third party.

Published Privacy Policy

Expertcity's published privacy policy is included in every GoToMyPC service agreement. This policy identifies information gathered, how it is used, with whom it is shared and the customer's control over dissemination. Expertcity is a TRUSTe licensee, adheres to established TRUSTe privacy principles and has agreed to comply with the TRUSTe oversight and consumer resolution process.

Disclosure of Customer Information

In order to deliver service, Expertcity must collect certain user information, including first/last name, email address, and account-level passwords for GoToMyPC. Unless expressly authorized, Expertcity will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services. For example, email addresses are used only to send service update messages, with the user's express consent. Upon request, Expertcity will also enter into a formal non-disclosure agreement (NDA) with any customer.

Even when GoToMyPC is accessed from a public PC, data left behind poses no privacy threat. GoToMyPC uses an optional cookie to track traffic patterns and retrieve registration information. This cookie holds a unique number, generated at registration time, but does not contain any personally identifiable information or passwords. Users can block this cookie, if desired. After a session ends, browser history indicates that GoToMyPC was accessed - but history cannot be used to access the account or any computer without a login/password.

Access to Customer Information

Expertcity NOC staff are the only individuals with access to Expertcity servers - limited access is granted on a need-to-know basis for the express purpose of customer support. Even Expertcity developers do not have access to Expertcity's production servers.

GoToMyPC session logs are used by Expertcity to maintain quality of service and assist in performance analysis. GoToMyPC tracks domain names, browser types and MIME types for traffic management. However, this data is gathered in the aggregate and is never correlated with an individual user or company account.

Ensuring Traffic Privacy

GoToMyPC Corporate account administrators have access to summary usage records associated with their company's account, but not to the traffic exchanged during individual remote access sessions.

In fact, although GoToMyPC communication servers relay traffic between client browser and computer, these packets are encrypted. Expertcity cannot decipher this traffic, because it does not possess the access code used to generate encryption keys. Even if an attacker were to gain access to Expertcity's servers, individual session traffic is not recorded and live session traffic cannot be compromised.

Security Policy Administration

GoToMyPC Corporate provides a secure online Administration Center to control which employees are permitted remote access and to block unauthorized access or features.

Secure Management Interface

The Administration Center is accessible from any Web browser. To reduce unauthorized login attempts, the Administration Center URL is not published. Once an organization establishes a GoToMyPC Corporate account, the administrator is provided with access instructions. The GoToMyPC server is authenticated with an X.509 digital certificate. The administrator sub-authenticates by username/password. Thereafter, SSL with 128-bit RC4 encryption protects all management traffic from disclosure or modification in transit.

Inviting New Users

Only the administrator is authorized to create new user accounts. The administrator simply logs into the Administration Center and supplies a list of email addresses. A customizable mail message is sent to each invited user, containing instructions and a one-time self-activation URL. The new user visits this URL, defines his or her own password, then adds computers to his or her own account. This approach streamlines large-scale deployment, while retaining enterprise control over remote access authorization.

Suspending or Canceling User Accounts

The Administration Center can also be used to check the activation status for individuals and groups. Controls are available to temporarily suspend or permanently cancel any user's account. Mail messages are sent to affected users, indicating the suspension or cancellation, and future client browser or computer login attempts with this account are denied.

Secure Service Installation

GoToMyPC software installation and update procedures were designed with enterprise security in mind.

Digitally Signed Applications

Software is installed by visiting Expertcity's Web site and launching a signed Java applet. Companies that prefer to block Java or prohibit users from installing software can launch the server or client from a file instead. The server is permanently installed, but the client does not require any permanently installed software.

All GoToMyPC programs are digitally signed. GoToMyPC software automatically keeps itself

up-to-date. However, no component is ever installed or updated without checking signatures. This prevents "Trojan horses" from masquerading as legitimate GoToMyPC software.

There are no security parameters configured by end users - the only values supplied are login, account password, and computer access password. This prevents misconfiguration, ensuring that company-specified secure remote access policies are always enforced.

Firewall Compatibility

GoToMyPC is firewall friendly. It generates only outgoing HTTP/TCP to ports 80, 443 and/or 8200. Because most firewalls are already configured to permit outgoing Web traffic, you don't have to bypass or compromise your corporate, branch office or teleworker firewall to implement secure remote access with GoToMyPC.

Many other solutions require servers to receive incoming packets at a public IP address. The GoToMyPC server sends an outgoing HTTP "ping" to the GoToMyPC broker at regular intervals, checking to see if any connect requests have been received. This makes GoToMyPC completely compatible with application proxy firewalls, dynamic IP addresses, and network/port address translation (NAT/PAT). However, companies that need to can control GoToMyPC traffic by simply filtering on GoToMyPC broker IP address.

Guarding Computer Access

Computers within your network must have the GoToMyPC server installed and running on them in order to be accessed remotely. Installing GoToMyPC requires physical access to the computer. It is not possible to remotely install or use a Trojan to "plant" GoToMyPC on a computer.

Computers are added by visiting Expertcity's Web site from each computer. The user - the computer's owner - must enter his or her login, account password and a computer access password that only he or she knows. It is also impossible for someone to reset the computer access password without supplying the login and account password used to register the computer.

Protecting Confidential Data

GoToMyPC uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the GoToMyPC browser client and computer, including screen images, file transfers, copy/paste operations, keyboard/mouse input and chat text, is protected with end-to-end 128-bit AES encryption.

Advanced Encryption

In early 2001, after an extensive four-year evaluation process, the National Institute of Standards and Technology (NIST) selected the Advanced Encryption Standard (AES) as a successor to DES. Originally known as Rijndael, AES was selected due to its computational efficiency, modest memory requirements, flexibility, simplicity, and, of course, security. AES is expected to become the US government's designated cipher for protecting sensitive information by mid-2001. It is also expected to become the default, mandatory cipher for IPsec ESP, TLS, and many other secure tunneling protocols. But why wait? GoToMyPC implements 128-bit AES in Cipher Feedback Mode (CFB) today.

Strong Encryption Keys

Even a strong cipher is vulnerable if it does not use strong, confidential encryption keys. GoToMyPC generates unique secret keys for each connection, derived from the computer access password and a large random bit sequence. The access password resides on the computer in encrypted format, and is never transmitted to or stored on Expertcity servers. Would-be hackers cannot intercept or generate the keys necessary to decode encrypted data.

Protection Against Message Replay and Modification

Desktop streaming and file transfer packets include a sequence number that allows the receiver to detect and report an attempted message replay attack. These packets carry high-compressed binary data, framed in a proprietary protocol, encrypted with AES. A hacker cannot modify these packets without corrupting them.

Chat packets carry text, also encrypted with AES. Because it is possible to modify encrypted text without corrupting it, chat packets also carry a signed MD5 hash to ensure message integrity.

Defeating Man-in-the-Middle Attacks

GoToMyPC implements AES in CFB mode. Any third party (man in the middle) attempting to inject or replay packets would have to know not only the session key, but also the current state of the AES engine. Compressed binary payloads make it exceedingly difficult to generate valid modified packets or "guess" the session key through traffic analysis.

Authenticated Access

GoToMyPC confidentiality between client and server builds on the strong foundation provided by authentication. Authentication verifies the identity of every party, from the GoToMyPC broker and communication server to the browser client and computer. This is combined with access controls that ensure only authorized parties can gain access to authorized resources.

Long, Complex Passwords

GoToMyPC requires that every password be at least eight characters long and contain both letters and numbers. These requirements help to prevent accounts from being configured with easily compromised, short, common passwords that are trivial to guess with a dictionary attack. The longer and more complex the password, the stronger the protection.

Limited Number of Login Attempts

GoToMyPC limits the number of times any user can attempt to login sequentially. This measure also helps to protect against dictionary attacks. After three strikes, the account is temporarily deactivated for five minutes.

Multiple, Nested Passwords

GoToMyPC uses multiple, nested passwords to keep outsiders away. Cryptographic techniques are used to ensure that sensitive data - logins and passwords - are never sent in plaintext.

The GoToMyPC broker authenticates itself to browser clients by supplying a digital certificate, issued by a trusted authority. Clients authenticate themselves to the GoToMyPC broker by supplying an account login/password, exchanged over SSL.

When a computer registers with the GoToMyPC broker, it relies on DNS resolution of the broker's hostname to reach the correct destination. The broker assigns the server a unique random number. The server initially authenticates itself by signing its unique number with MD5 and the account login/password. Thereafter, the broker and server exchange MD5 challenge/response messages, based on a sequence known only to the pair.

End-to-End Authentication

Whenever a browser client connects to a computer, they also authenticate each other, using a shared secret known only to the end user and the accessed computer. This access password is never seen or stored by Expertcity. The client and server each generate a very large random number and digitally sign that number with the access password. This challenge/response provides end-to-end authentication, without transmitting the password. As long as the user keeps his or her access password secret, only he or she can successfully launch a GoToMyPC session to that computer.

Inactivity Timeouts

Users walk away from public PCs without logging out and leave home PCs unattended. GoToMyPC addresses these threats by applying inactivity timeouts. Users are automatically logged out of the GoToMyPC.com Web site if their SSL session is inactive for fifteen minutes. Additionally, host security features allow users to blank the host screen and lock the host keyboard and mouse from accepting input.

OS-Level Access Control

GoToMyPC leverages the OS-level access controls already in place on the corporate LAN. Simply leave the PC to be accessed in a screen-locked or logged-out state. When the 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 computer.

Guest Invitation

Users armed with GoToMyPC may be tempted to use desktop sharing for collaboration with colleagues, customers and clients. Guest access can be useful, but must be implemented securely. GoToMyPC's "guest invite" feature grants a third party temporary access to any GoToMyPC-enabled computer, without disclosing the account or computer password.

Limited Invitation Period

Computer owners can invite others to access their computers using GoToMyPC. By right-clicking on the GoToMyPC launcher, the computer owner can issue an email invitation that expires after one, two or three hours. The owner must supply his or her account login and password to satisfy a broker challenge/response and digitally sign the entire invitation. The broker then sends an email message to the specified address containing a one-time access URL the guest will follow to get to Expertcity's Web site.

Granting Access Required

Once at the web site, the guest clicks on a button to download the GoToMyPC viewer. Because the URL contains a onetime token for dynamic login, the guest is not prompted for an access password. Instead, a pop-up window is displayed on the computer to be accessed, requiring manual authorization by the owner to complete the guest connection. Unauthorized invitations are prevented by requiring the invitation to be generated from the computer itself, by someone with the account-level password.

Share Control or View-Only Option

Two guest access modes are supported: a view-only mode and a full-control mode. In view-only mode, the browser client can draw, but cannot initiate desktop actions or transfer files. Full-control mode offers the same access normally granted to the computer's owner. The local mouse always overrides remote control. The computer owner can of course end the GoToMyPC session at any time by disconnecting the guest.

Monitoring Access Within an Organization

The GoToMyPC Administration Center lets an organization track all connections made by employees and maintain session logs for security audit and accounting purposes.

Monitoring Usage

The GoToMyPC Corporate administrator can view sessions for any given day, including those that are still active. Each session record displays the first and last name of the user, the name of the destination computer, the IP address of the client initiating the session, the session start and stop time, the session duration and the type of session (normal or guest invite).

The Administration Center can also be used to generate reports that cover any range of dates and which sum users, sessions and session time and calculate the average session duration.

These standard reports can be analyzed to spot unusual access patterns, including exceptionally long sessions and unexpected client IP addresses. They also serve as audit trails, making it possible to check to see who accessed a particular computer at a particular time.

Detailed Session Logs

The GoToMyPC broker logs additional information for each session, including the last user access time, type of browser (user agent), download status for the viewer, communication server ID, who closed the session (server/client/broker/timeout), a close error code and the build number of the computer. This information is intended to aid problem diagnosis; access is limited to Expertcity customer support on an as-needed basis.

Access Notifications

Whenever a client connects to a computer running GoToMyPC, a notice appears on computer's screen. This notification makes sure that the computer's owner is always aware of the GoToMyPC session, preventing a "lurker" from silently watching local desktop activity.

Upon each browser client login, the user is always notified of his or her last login attempt. This notification reassures the user that no unauthorized access has taken place during the interim.

Conclusion

Expertcity's recipe is straightforward: Start with a secure hosted service and operational practices that preserve customer privacy. Complement this foundation with secure enterprise-class configuration and monitoring tools to control remote access. Protect remote access sessions with multi-level authentication and state-of-the-art encryption to keep corporate traffic safe. The end result: GoToMyPC Corporate for robust, secure remote access.

Prepared by:

Lisa Phifer
Core Competence, Inc.
lisa@corecom.com