

Common Security Questions about GoToMyPC



© 2002 Expertcity, Inc. All Rights Reserved. Confidential Property of Expertcity, Inc.

Common Security Questions about GoToMyPC

GoToMyPC Technology Overview

Encryption and Authentication

Security and Privacy

GoToMyPC Corporate Plan Information

GoToMyPC Technology Overview

- Q: What GoToMyPC software do I need to install on the host and client computer?
- A: From an administrative perspective, GoToMyPC software installation is easy to manage. There is no need for you to manage or maintain distribution shares or CD-ROM-based software. Through the online Administration Center, you invite users to download the GoToMyPC software. Users download a 1.75 MB file and perform an easy, one-time installation on the host computer. The client computer requires no software to be preinstalled by you or the user. When users connect to their host computers, GoToMyPC downloads a small (448K) Viewer plug-in to the client computer. This software is downloaded to a temporary folder on the client computer and is automatically deleted once the session ends.
- Q: Why do my users need to keep their host computers turned on to use GoToMyPC?
- A: GoToMyPC is designed to use your existing infrastructure and corporate Internet connection. Once installed on the host computer, the software runs as a service and waits for a connection request from the client. The host computer makes periodic, short HTTP requests to the server to poll for new information. This outgoing connection is what enables GoToMyPC to work with most firewalls, and therefore requires that the computer remain turned on and connected to the Internet.
- Q: How do you protect the host computer during a session from access by hackers and other intruders?
- A: In addition to protecting the data through industry-standard encryption, GoToMyPC uses several methods to protect access to the host computer:
 - End-to-end authentication with a challenge/response mechanism.
 - Multiple passwords through the secure Web site, including a unique access code.
 - Strong passwords: 8 character alphanumeric passwords required. Special characters are allowed and the passwords are case sensitive.

- Limited log-in attempts.
- Inactivity time-out on the Web site.
- User notification that the host computer is being accessed.
- Administrator notification of access via online administration tools.
- Q: How do you prevent someone from viewing or controlling the host computer while a remote session is in progress?
- A: Protecting physical access to the host computer during a session is an important consideration for remote access. GoToMyPC protects the host computer through screen blanking and keyboard/mouse input blocking features. Most configurations of GoToMyPC allow the user to blank the screen of the host computer while connected in a GoToMyPC session. In addition, user can lock the host computer's mouse and keyboard while connected in a GoToMyPC session.
- Q: Does GoToMyPC require a static IP address?
- A: No. Unlike other remote control and remote-access products, the GoToMyPC protocol design is compatible with dynamic and static IP addresses. GoToMyPC automatically detects the IP address, so your users do not need to configure any software settings.
- Q: How does GoToMyPC work through my firewall?
- A: GoToMyPC adjusts itself to your firewall so administrators generally do not need to change or open ports in the organization's firewall. GoToMyPC does not open any new ports that an intruder could exploit, or open any new firewall holes. All connections are made by using outgoing TCP ports that are often left open for Web browsing (ports 80, 443 and/or 8200). Unlike other remote-access products, GoToMyPC does not accept incoming connections that could allow intrusions. GoToMyPC encapsulates all traffic inside standard HTTP wrappers, ensuring compatibility with firewalls that inspect payload.
- Q: Will GoToMyPC work with a Network Address Translation (NAT) device?
- A: Yes. Because GoToMyPC uses outgoing HTTP requests, it is compatible with the dynamic IP addresses generated by network and port address translation (NAT/PAT) devices that block incoming sessions.
- Q: Which port numbers does GoToMyPC use, and can I change the port numbers?
- A: GoToMyPC uses one of the several ports that are usually left open for users to access the Internet (port 80 or 443). This means that administrators generally do not need to configure firewalls to allow GoToMyPC connections. If your organization uses a proxy that restricts traffic through port 80 or 443, you may open port 8200 for GoToMyPC

connections. Expertcity provides a Connectivity Test Wizard that administrators may use to optimize their GoToMyPC connection ports.

Encryption and Authentication

- Q: How secure is the connection between the client and the host computers?
- A: GoToMyPC encrypts all data including screen images, file transfers, keyboard and mouse input and chat text. To read an encrypted file, users must have access to a secret key, which prevents data from being intercepted and decoded. GoToMyPC security and encryption is built in and cannot be weakened by users or intruders. For additional security, the access code for the host computer is never transmitted it is stored only on the host computer and is not stored on Expertcity servers.
- Q: What encryption method do you use?
- A: GoToMyPC has end-to-end, 128-bit Advanced Encryption Standard (AES) encryption built in. AES is a strong industry-standard encryption method, and was recently adopted by the U.S. government as its encryption technique. All traffic between the GoToMyPC browser client and host computer is highly compressed and encrypted to thwart packet sniffers, which are programs or devices that monitor data traveling over a network. GoToMyPC generates unique, secret encryption keys for each connection by deriving them from the computer access password and a large random bit sequence.
- Q: Can I change or improve the GoToMyPC security settings or encryption method?
- A: No. The strong security and AES encryption is preset, so your users cannot unintentionally compromise or weaken your network security. Companies find that the GoToMyPC authentication, encryption and security features make it one of the most secure remote-access products on the market.
- Q: How do you prevent man-in-the-middle attacks?
- A: A man-in-the-middle attack occurs when an attacker interferes with the initial public key exchange by substituting a counterfeit public key for the genuine key. GoToMyPC prevents man-in-the-middle attacks by implementing AES in Cipher Feedback (CFB) mode. This makes it very difficult for intruders to generate valid modified packets. Attackers attempting to substitute keys or packets would need to know the session key and the current state of the AES engine.
- Q: Does GoToMyPC work with two-factor authentication such as RSA SecurID?
- A: Two-factor authentication provides security by requiring something you know (such as a password) and something you possess (such as a token card). GoToMyPC does not currently provide two-factor authentication, but is working to support methods such as SecurID from RSA Security, Inc.

- Q: Do you record or store users' remote-access sessions?
- A: For privacy reasons, GoToMyPC does not store or record user sessions or actions (such as files accessed). However, administrators can obtain basic information about sessions conducted by users such as the connection time, duration and the host computer IP address.
- Q: How secure is the GoToMyPC Web site?
- A: Users must authenticate themselves on the GoToMyPC Web site with a user name and password exchanged using Secure Sockets Layer (SSL) protocol. If an SSL session is inactive for 15 minutes, the user is automatically logged out of the Web site a feature that is particularly important when using public computer terminals. To protect against attacks, GoToMyPC temporarily blocks access to the site for five minutes if a user makes three attempts to log in with incorrect login information.
- Q: Which certificate authority do you use to issue certificates?
- A: The GoToMyPC certificate authority is VeriSign, a trusted digital certificate provider. All GoToMyPC programs are digitally signed.
- Q: How do my users receive the certificate?
- A: The VeriSign certificate is embedded at the beginning of every GoToMyPC download. The certificate is issued by VeriSign and will appear if Java is enabled on the computer.
- Q: Where and how is the access code stored for the host computer?
- A: The access code is stored in the host computer registry with 128-bit AES encryption (AES). This access code for the host computer 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.
- Q: Must users change their GoToMyPC passwords and access codes periodically?
- A: GoToMyPC does not require that users change their passwords and access codes at predetermined times. However, your corporate security policies may dictate periodic password changes, and administrators can request that users change their GoToMyPC passwords regularly. In addition to the protection afforded by GoToMyPC's security, your organization retains control over desktop security policies, such as the password expiration.
- Q: Can users repeat passwords and access codes that they used previously?

A: Yes, users may re-use GoToMyPC passwords. Organizations can enforce their security policies through their existing desktop security policies.

Security and Privacy

- Q: How does GoToMyPC protect the privacy of my data?
- A: GoToMyPC (Expertcity) has a strong privacy policy and will not disclose any of your personal information to third parties. Although Expertcity servers broker all transmissions in the ASP product, personal data is fully encrypted the entire time. Expertcity does not have access to this data or to the access code used to generate the unique encryption keys. Therefore, all data transmitted is completely private. Even if an unauthorized party were to gain access to Expertcity servers, the data for individual connections could not be accessed or compromised.
- Q: What data do you collect about each session?
- A: Basic information is collected about every session, and users and administrators have access to this data. Examples of the collected information include the name of the host computer name being accessed, the start time of a remote-access session, the duration of a session and the IP address of client computer. If guest invitations are used, you can view when the invitation was sent, the session duration, the guest computer IP address and the guest email address. In addition to this basic information viewable by administrators, GoToMyPC collects aggregate data to maintain the quality of service and to assist in performance analysis. Examples of this aggregate information include domain names and browser types. This data is not correlated with individual users or company accounts.
- Q: Does GoToMyPC have access to files or data on my organization's computers?
- A: No. GoToMyPC and Expertcity personnel have no way to access your organization's data because it is fully encrypted. We do not have the access code used to generate the unique encryption keys. Even if an unauthorized party were to gain access to Expertcity servers, your organization's computers or data could not be accessed or compromised because the access code resides only on the host computer.
- Q: Can users block cookies and still use GoToMyPC?
- A: Yes, users may block the cookie if they desire. GoToMyPC uses the cookie to track traffic patterns and retrieve registration information (the "Remember me" option during log in). This cookie does not contain any personally identifiable information or passwords. The data left behind with the cookie poses no privacy threat, even if GoToMyPC is accessed from a public computer.
- Q: Do my users need a personal firewall for their home computers?

- A: Whether your users require a personal firewall for their home computers is based on your organization's remote-access security policies. Although it is prudent to use a firewall in conjunction with any Internet access, GoToMyPC does not require the use of a firewall.
- Q: How do you prevent hackers from randomly guessing a password?
- A: GoToMyPC has security features that make it difficult for hackers to randomly guess a password. The GoToMyPC Web site has a feature that blocks access to the site for five minutes if a user makes three attempts to log in with incorrect login information. In addition, every password must be at least eight characters long and contain both letters and numbers. These long, complex passwords prevent users from compromising security by using short, easy-to-guess passwords.
- Q: Are sessions automatically logged off after a period of inactivity?
- A: If a session is inactive for 15 minutes, the user is automatically logged off the GoToMyPC Web site. This feature provides security for users who forget to log off public computer terminals. The standard Viewer used for most GoToMyPC sessions remains connected until the user ends the session. However, the Universal Viewer (used from Mac, Linux, Solaris and certain Windows computers) logs users off after 15 minutes of inactivity.
- Q: How secure is the File Transfer feature?
- A: As with the data that is shared between screens during the remote-access session, file transfer data is also encrypted using 128-bit AES encryption. This prevents intruders or hackers from obtaining sensitive documents or data. With GoToMyPC, users cannot transfer viruses and worms simply by viewing a host computer. However, whenever users transfer files from computer to computer in a networked environment, it is prudent to use virus protection.
- Q: How secure is the guest invitation feature?
- A: Sessions conducted from a guest invitation have the same strong security and protection as does any GoToMyPC session. However, with guest invitations, GoToMyPC provides additional security:
 - Guest access is one-time only, so previously invited guests do not have continued access to a user's computer. For further security, GoToMyPC allows only one outstanding invitation, and users can cancel the invitation at any time.
 - The invitation that your users send to trusted guests is valid for only a limited period of time. If the guest does not activate the link within the time period, the invitation expires.

- When an invited guest attempts a connection, your user receives an on-screen notice that someone is requesting access. Users must approve access before a connection can be completed. Users can disconnect the guest at any time.
- Users choose the level of access to grant invited guests. To limit a guest's access to a computer, users may grant view-only control. Alternatively, users can allow full control of the keyboard and mouse.
- Q: Can I turn off features such as File Transfer and Guest Invite to protect my network and prevent remote users from downloading confidential documents?
- A: At this time, you cannot disable specific GoToMyPC features. However, we are working on features for GoToMyPC Corporate that will allow customers to enable specific features by group or by employee.
- Q: How secure is the GoToMyPC data center?
- A: GoToMyPC has data center policies in place at several levels to provide identification and authentication of personnel; access control; and auditing of systems. For example, all GoToMyPC servers are located in a secured data center that has restricted physical and logical access. The access routers are configured to watch for denial of service (DoS) attacks, and multi-layer perimeter security is provided by firewalls. The security of this architecture has been independently confirmed by penetration tests and vulnerability assessments conducted by a third-party organization. Complete data-center security is covered in Expertcity's Security Policy.
- Q: How secure is the GoToMyPC architecture?
- A: The GoToMyPC architecture is designed for security and reliability. For security, GoToMyPC has an SSL-encrypted Web site and end-to-end AES 128-bit encryption of the data stream. In addition, the access code is never transmitted or stored on GoToMyPC servers. Other security features include lockout protection, inactivity timeout and the ability to lock the host keyboard and mouse and to blank the host screen. For reliability, Web-balancing switches monitor the network flow and transparently distribute server requests among all the servers. Redundant switches and routers, clustered servers and backup systems ensure reliability and scalability.
- Q: How can I restrict GoToMyPC access to authorized people in my company?
- A: You might be able to use your company's firewall and DHCP server to restrict access to a specific group of users. First, set up a subset (also known as a pool) of IP addresses on your DHCP server. Configure your authorized GoToMyPC users' connection settings to use this subset of addresses.

Next, configure your firewall or proxy server to allow the subset (pool) of IP addresses access to poll.gotomypc.com. This allows only your specific group of users access to the

GoToMyPC server. The firewall prevents unauthorized users from accessing the GoToMyPC server.

GoToMyPC Corporate Plan Information

- Q: Who is GoToMyPC?
- A: GoToMyPC is a product of Expertcity, Inc., a leading provider of Web-based remoteaccess and customer-support technologies. The company was founded in 1999, and its investors include Sun Microsystems, CNET Networks, Bertelsmann Ventures and SoundView Ventures. The company's screen-sharing technology enables users to view and control a remote computer via the Web, thus enabling remote access.

The company has received numerous awards, including recognition as a Top 100 Site from *PC Magazine* and the Forbes Favorite from Forbes.com Best of The Web and the CNET Editors' Choice award. GoToMyPC has received numerous awards and citations from both mainstream and industry press. In July, CNET awarded GoToMyPC its Editors' Choice pick in the remote control category, where GoToMyPC was pitted against the established market leaders.

- Q: What assurances can GoToMyPC provide regarding security?
- A: The GoToMyPC architecture was created with security and reliability as the primary focus. The company adheres to a security policy that requires strong security and customer privacy mechanisms. The company's enterprise-class configuration and operational practices meet or exceed industry-standard security measures.
- Q: What types of companies are currently using GoToMyPC?
- A: GoToMyPC customers are a cross-section of enterprises from small firms to Fortune 500 enterprises. Expertcity's clients include Gateway, Sun Microsystems, Intuit, Bertelsmann, Nortel Networks, Colgate-Palmolive, EarthLink, Honeywell, Siemens, Best Software, Autodesk, DecisionOne, Witness Systems, Cox Communications, CDW, Talisma, Sage, RightNow Technologies, Cablevision, Peachtree, Allied Mortgage Capital Corporation, eSylvan, MicroWarehouse, Harcourt-Brace, SaskTel, Administaff and SkillSoft.

expertcity_®