



Remote Access Security

Security is essential when accessing home and office computers remotely. Learn how GoToMyPC provides reliable, industry-leading security that keeps your files, applications and information safe from harm.

GoToMyPC enables secure remote access to any Internet-connected Mac or PC. Keyboard, mouse and display updates are transmitted over a highly compressed, encrypted stream, yielding an experience that's like being there.

Applications supported by GoToMyPC include:

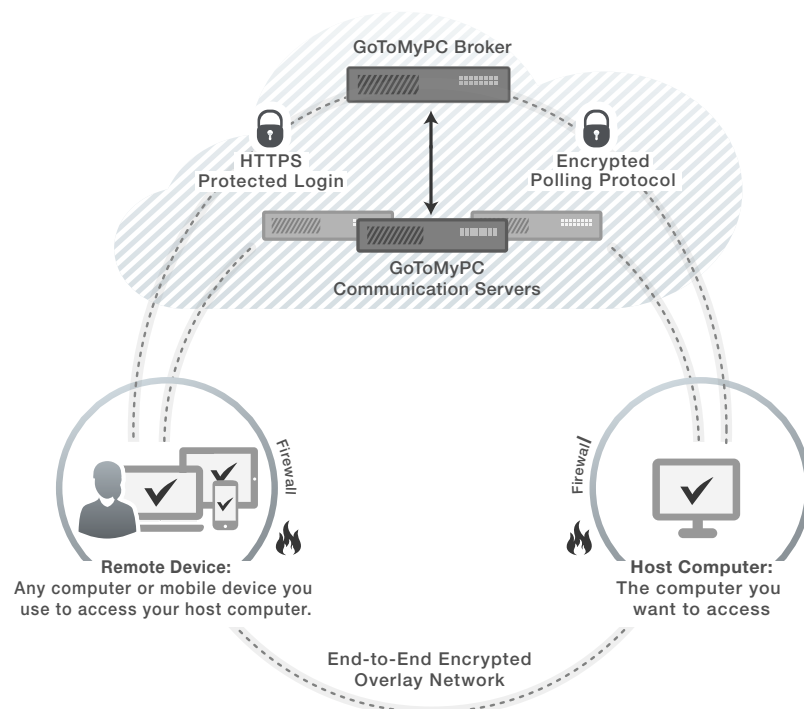
- **Screen sharing:** Launch a resizable viewer from any browser or mobile device to enable interactive access to any desktop application (even those that are not web based).
- **File transfer:** Easily transfer files between the host and local client computer.
- **Remote printing:** Print from your host PC to a printer wherever you are.
- **Mobile access:** Access your Mac or PC from your iPad, iPhone or Android device.

GoToMyPC is a hosted service composed of five components:

- **Computer:** A small footprint server is installed on the computer to be accessed: Typically, this

is a home or office computer with always-on Internet access. We call it the host computer. This server registers and authenticates itself with the GoToMyPC broker.

- **Browser:** From the remote, or client, computer, the user launches a web browser, visits the secure GoToMyPC website, enters a user name and password and clicks a connect button for the desired computer, sending an SSL-authenticated, encrypted request to the broker. Alternatively, the user can load the GoToMyPC app on a tablet or smartphone, enter his or her account details and click connect to initiate the request.
- **Broker:** The broker is a matchmaker that listens for connection requests and maps them to registered computers. When a match occurs, the broker assigns the session to a communication server. Next, the client viewer — a tiny session-specific executable — is automatically loaded by our automatic launcher tool.
- **Communication Server:** The communication server is an intermediate system that relays an



opaque and highly compressed encrypted stream between the client and host computers for the duration of each GoToMyPC session.

- **Direct Connections:** Once the user is authenticated and connected, GoToMyPC attempts to establish a direct connection between the client and host, bypassing the GoToMyPC communication server whenever possible to increase the connection speed and improve in-session performance. The Direct Connections feature instructs both the client and host to listen for a limited time for incoming connections and also to attempt outgoing connections to each other; whichever signal arrives first establishes the connection. The client and host then proceed to execute an SRP-based authenticated key agreement and establish an end-to-end secure connection that is not susceptible to “man-in-the-middle” attacks. Should the direct connection be blocked or interrupted, the previously established connection through the communication server maintains remote access service. The Direct Connections feature is always enabled for GoToMyPC and GoToMyPC Pro accounts and optional for GoToMyPC Corporate.

Protecting the integrity of users' data and the privacy of sensitive information is of utmost concern to anyone. Whether you're using GoToMyPC for business or personal use, security is essential.

Security from the ground up

Citrix delivers GoToMyPC using an SaaS model designed expressly to ensure robust and secure operation while integrating seamlessly with a company's existing network and security infrastructure.

Secure facility

All GoToMyPC web, application, communication and database servers are hosted in highly secured worldwide datacenters. Physical access to servers is restricted. The Citrix network operations center (NOC) in Santa Barbara, California, is protected with strict security measures.

Secure network

Citrix access routers are configured to watch for denial of service (DoS) attacks and to 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 back-end databases.

Secure platform

Citrix servers run on hardened Linux servers with the latest security patches installed. Servers have been penetration tested, and system logs are continuously audited for suspicious activity.

Secure administration

Citrix servers are administered over a private T1 linking the secure datacenter to the Citrix NOC in Santa Barbara. Secure Shell (SSH) supports authenticated and encrypted remote log-in access by the Citrix NOC staff. An intermediate server handles and authenticates all SSH connections, thereby avoiding open ports and ensuring very tight access control.

Scalable and reliable infrastructure

The Citrix 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 Citrix web servers. For optimal performance, the GoToMyPC broker load balances the client/server sessions across geographically distributed communication servers.

Protecting customer privacy

Citrix understands about the importance of privacy. Citrix has a strong privacy policy that prohibits unauthorized disclosure of personal or business information to any third party.

Published privacy policy

The Citrix published privacy policy is included in every GoToMyPC service agreement. This policy identifies the information gathered, how it is used, with whom it is shared and the customer's ability to control the dissemination of information. Citrix 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

To deliver service, Citrix must collect certain user information, including first and last name, email address and account-level passwords for GoToMyPC. Unless expressly authorized, Citrix will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed upon services. With its users' express consent, Citrix sends service update messages to its users at the email addresses they provided when requesting the service.

Even when GoToMyPC is accessed from a public computer, 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 the time of registration, 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 information in the history cannot be used to access the account or any computer without a complete set of credentials, including the user's login and password, the computer's access code and (optionally) a one-time password.

Access to customer information

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

GoToMyPC session logs are used by Citrix 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 and credential privacy

Although GoToMyPC communication servers relay traffic between the client browser and host computer, these packets are encrypted. Citrix cannot decipher this traffic because it does not possess the access code used to generate encryption keys. Even if a hacker were to gain access to Citrix servers, computer access codes are not stored there and individual session traffic is not recorded, so live-session traffic cannot be compromised.

Digitally signed applications

Software is installed by visiting the GoToMyPC website and launching a signed Java applet or our automatic launcher tool. The server software is permanently installed on the host computer, but the client does not require any permanently installed viewer software.

Most security parameters are pre-set and do not need to be configured by end users. Users can also enable additional security measures, such as blanking the computer screen and locking the keyboard during or after sessions, or generating one-time passwords to prevent keystroke capture attacks. Users are always responsible for setting their own passwords and computer access codes, thereby ensuring end-user privacy.

Firewall compatibility

GoToMyPC is firewall friendly. Sessions are initiated only through outgoing HTTP/TCP to ports 80, 443 and/or 8200. Because most firewalls are already configured to permit outgoing web traffic, you do not have to bypass or compromise your corporate or branch office firewall or your remote worker's firewall to implement secure remote access with GoToMyPC.

Many other solutions require servers to receive incoming packets at a public IP address. The GoToMyPC host establishes a persistent TCP connection to the GoToMyPC broker (poll. gotomypc.com) that allows it to be notified if any connect requests have been received.

The host will attempt to keep the connection open by sending TCP "keep alive" packets approximately every 60 seconds. This makes GoToMyPC completely compatible with application proxy firewalls, dynamic IP

addresses and network/port address translation (NAT/PAT).

Please note that some firewalls may block Direct Connections, or give you a warning message asking for your permission to allow it, because it creates an incoming connection at one point. This does not limit GoToMyPC's compatibility with firewalls, though; if Direct Connections is blocked or interrupted, the connection will simply automatically continue through the communication server via outgoing signals. GoToMyPC users also have the option to disable Direct Connections if they so desire.

Also, because GoToMyPC is firewall friendly, you can use it with computers at your company without creating a headache for your IT team. Companies can control GoToMyPC traffic by simply blocking traffic sent to the GoToMyPC broker's IP address. Upon request, Citrix will filter GoToMyPC connections made to a company's network address block, ensuring that only company-authorized computers can be accessed by company-authorized users. This permits a company's visitors to use GoToMyPC to reach their own offsite computers while preventing unauthorized use of GoToMyPC to access a company's own computers.

Guarding computer access

To be accessed remotely, your computers must have the GoToMyPC software installed and running on them. Installing GoToMyPC requires physical access to the computer. It is not possible to remotely activate GoToMyPC or use a Trojan to "plant" it on a computer.

Computers are added by visiting the GoToMyPC website from each computer. The user — the computer's owner — must enter his or her user name, account password and a computer

access code that only he or she knows. It is impossible for someone to reset the computer access code without supplying the user name and account password used to register the computer. Optional one-time passwords and 2-step verification can be used to provide an additional level of authentication. This eliminates compromise due to keystroke logging, which can be an issue when using GoToMyPC on a public 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 host computer, including screen images, file transfers, copy/paste operations, keyboard/mouse input and chat text, is protected with end-to-end 128-bit Advanced Encryption Standard (AES) encryption.

Advanced encryption

GoToMyPC uses 128-bit Advanced Encryption Standard (AES) in Counter Mode (CTR). In early 2001, after an extensive four-year evaluation process, the National Institute of Standards and Technology (NIST) selected AES as a successor to DES. Originally known as Rijndael, AES was selected because of its computational efficiency, modest memory requirements, flexibility, simplicity and, of course, security.

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. These are derived using a zero-knowledge, public-key-based protocol called SRP. (See below.) The access code verifier resides on the computer in encrypted format and is never transmitted to or stored on Citrix servers. Would-be hackers cannot intercept

or generate the keys necessary to decode encrypted data.

Protection against message replay and modification

Screen sharing and file-transfer packets include a sequence number to prevent any attempted message replay attack. These packets carry highly compressed binary data that are framed in a proprietary protocol and encrypted with AES. An attacker cannot modify these packets without it being detected by the recipient.

Authenticated access

The GoToMyPC confidentiality between the browser client and host computer 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 host computer. Access controls further ensure that only authenticated parties can gain access to authorized resources.

Mobile security

All of the security protocols made for using GoToMyPC on a desktop or laptop apply equally to using GoToMyPC on a mobile device. In the event that you lose your phone or device, no one can use the app to access your remote computer without your personal GoToMyPC access code.

Strong passwords

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

Limited number of log-in attempts

GoToMyPC limits the number of times any user can attempt to log in sequentially. This measure also helps to protect against password-guessing attacks. By default, after 3 authentication failures, access to the user's account and computer are temporarily deactivated for 5 minutes.

Multiple passwords

GoToMyPC uses multiple, nested passwords to keep outsiders away. Cryptographic techniques are used to ensure that sensitive data — user names and passwords — are never sent in plaintext. For an additional level of protection, users can use one-time passwords.

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 user name and password that is exchanged over SSL.

End-to-end authentication

Whenever a browser client connects to the host computer, they also authenticate each other, using a shared secret known only to the end user and the accessed computer. This access code is never seen or stored by Citrix. As long as the user keeps his or her access code secret, only he or she can successfully launch a GoToMyPC connection to that computer. GoToMyPC uses the Secure Remote Password (SRP) protocol standard for end-to-end authenticated key agreement between the viewer and host.

This patented, well-reviewed protocol provides outstanding cryptographic strength, performance and resilience against a wide range of potential attacks. For more information, visit <http://srp.stanford.edu/>.

To enable one-time passwords authentication, the user clicks a button to generate a list of passwords from the computer to be accessed. When initiating future connections, a user who supplies the correct access code will be prompted for a numbered password from this list. Each password is used for just one connection, and the user can cancel or regenerate the list at any time. One-time passwords are an easy-to-use method to achieve stronger authentication without requiring added infrastructure.

Two-step verification

Two-step verification is a proven security method, widely used in many online services. It is based on something you know (a password) and something you have (like a phone).

Users have the option of enabling 2-step verification for GoToMyPC. This feature sends a unique authentication code via SMS to the user's phone whenever he or she attempts to log in. The user then enters this code into the website or mobile app to gain access. GoToMyPC can be set to remember computers or devices the user frequently uses so that the prompt does not reappear.

Inactivity time-outs

Users walk away from public computers without logging out and leave home computers unattended. GoToMyPC addresses these threats by applying inactivity time-outs. Users are automatically logged out of the GoToMyPC website if their SSL connection is inactive for 15 minutes. Users can also configure the viewer to time out after a set period of inactivity. 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 computer to be accessed in a screen-locked or logged-out state. When GoToMyPC connects, the remote user must enter a user name and 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 choose to use desktop sharing for collaboration with colleagues, customers and clients. Guest access can be useful, but it must be implemented securely. The GoToMyPC user may grant a third party temporary access to any of his or her own GoToMyPC-enabled computers, without disclosing the account or computer password.

Limited invitation period

When permitted, users can invite others to access their computers using GoToMyPC. By right-clicking the MYPC icon in the system tray, the user can issue an email invitation that expires after one, two or three hours. The user 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 guest's specified address containing a one-time access URL the guest will follow to get to the GoToMyPC website.

Granting access required

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

Shared 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 end the GoToMyPC connection at any time by disconnecting the guest.

Access notifications

Whenever a client connects to a computer running GoToMyPC, a notice appears on the computer's screen. This notification makes sure that the computer's owner is always aware of the GoToMyPC connection, preventing a "lurker" from silently watching local desktop activity. In addition, the GoToMyPC website displays a session-in-use notification during an active connection. Upon each browser client login, the user is always notified of his or her last log-in attempt. This notification reassures the user that no unauthorized access has taken place during the interim. In addition, users can view

their own connection histories, including the number of failed log-in attempts, to confirm that there has been no suspicious activity.

Administering GoToMyPC Corporate accounts

Security is essential when extending Internet-based remote access to remote and mobile employees. However, to ensure low total cost of implementation (TCI), secure remote-access solutions must integrate smoothly with each organization's existing security infrastructure and require little IT support or per-user configuration. Our enterprise product was developed with these key security issues in mind.

GoToMyPC Corporate provides a secure online administration center from which administrators can control the employees who are permitted remote access and can block unauthorized access or features.

Secure management interface

The administration center is accessible from any web browser. Once an organization establishes a GoToMyPC Corporate account, the administrator is provided with access instructions. A top-level administrator can grant access to a second tier of plan administrators to facilitate large GoToMyPC Corporate deployments. All website connections are protected using SSL with a minimum of 128-bit symmetric encryption and a 1024-bit authenticated key agreement. If the browser does not support a strong cipher suite, the user will be redirected to a page that explains how to upgrade the browser. The GoToMyPC server is authenticated with an X.509 digital certificate. The administrator authenticates by username/password.

Inviting new users

Only the administrator is authorized to create new user accounts and groups. The administrator simply logs in to the administration center and supplies a list of email addresses. A customizable mail message containing instructions and a one-time self-activation URL is sent to each invited user. The new user visits this URL, defines his or her own password and then adds computers to his or her own account. The administrator can limit the number of computers available to each user and can require explicit administrative authorization of both host computers and client viewer systems. In addition, an administrator can prevent non-permitted GoToMyPC Corporate access by limiting host computers within a network to a specific GoToMyPC Corporate account. These approaches streamline large-scale deployment while retaining enterprise control over remote-access authorization and end-user privacy and accountability.

Suspending or canceling user accounts and connections

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 or group account. Email messages are sent to affected users, indicating the suspension or cancellation, and future client browser or computer log-in attempts with the user's account are denied. In addition, GoToMyPC Corporate administrators can view connection activity in real time and end connections immediately if necessary.

Managing user accounts

GoToMyPC Corporate administrators can configure user account parameters to meet

organizational needs, implement corporate security policies and support privacy mandates. Administrators can limit access by users or groups to specific services such as file transfer, guest invite, clipboard sharing and remote printing. Administrators can also enforce password update frequency and reuse policies, limit time-out periods, lock accounts and computers after authentication failure and mandate use of one-time passwords.

Fine control over these settings allows administrators to match corporate security policies, and customizable multi-level groups enable enterprise-wide policy enforcement and rapid update, even in very large deployments.

SecurID integration

GoToMyPC Corporate integrates seamlessly with a company's existing RSA SecurID infrastructure, without requiring complex configuration or delegation of trust to Citrix servers. This option provides strong two-factor authentication by requiring users to have their own SecurID token in their possession in order to remotely access a host PC. (Mac integration is not yet available.)

To enable SecurID authentication, the computer must be configured with names of the company's own RSA Server(s). Thereafter, a user supplying the correct access code will be required to enter the value currently displayed by his or her SecurID token. That value changes constantly, preventing access by anyone who does not have the token in his or her physical possession.

Monitoring access within an organization

The GoToMyPC Corporate administration center enables an organization to track all

connections made by users, create detailed reports and maintain connection logs for security audit and accounting purposes.

Monitoring usage

The GoToMyPC Corporate administrator can view a report of connections for any given day, including those that are still active. Administrators can also use this tool to end active connections immediately if necessary. Each connection record displays details such as the first and last name of the user, the name of the host computer, the IP address of the client initiating the connection, the connection start and stop time, the connection duration and the type of session (normal or guest invite).

The administration center can also be used to generate and archive reports for specific dates and date ranges that provide details on users, connection time and average connection duration. Administrators can also generate additional reports to evaluate data such as enabled users, the features enabled for each user/group, hours of access, last log-in time or the frequency of failed log-in attempts.

These standard reports can be analyzed to spot unusual access patterns, including exceptionally long connections 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.

Users can view their own connection histories when logged in to the GoToMyPC website. Connection history can also be integrated into an existing reporting infrastructure by sending records to the Windows Event Log on each computer.

Detailed connection logs

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

Conclusion

The Citrix recipe is straightforward: Start with a secure hosted service and operational practices that preserve customer privacy. Protect remote-access connections with multi-level authentication and state-of-the-art encryption to keep users' information safe. The end result: GoToMyPC offers robust, secure remote access that's fast, reliable and simple to use.

Corporate accounts build on this foundation with the addition of secure enterprise-class configuration, administration and monitoring tools. GoToMyPC Corporate can be integrated seamlessly with a company's existing network and security infrastructure and easily scaled as account needs grow, ensuring robust, secure remote access with low total cost of implementation.

Contact us

To learn more about GoToMyPC security, please call us toll-free at 1 888 646 0016 or direct dial +1 805 690 5780. Or, visit our website at www.gotomypc.com.



Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix

Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud services to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of \$2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.

Copyright ©2014 Citrix Systems, Inc. All rights reserved. Citrix, GoToAssist, GoToMeeting, GoToMyPC, GoToTraining, GoToWebinar, OpenVoice, Podio and ShareFile are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

Mac, iPad and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. Android is a trademark of Google Inc.