GoToMyPC®

Citrix GoToMyPC Corporate Security FAQs

Common security questions about Citrix GoToMyPC Corporate

Q: What are the GoToMyPC Corporate software components that I need to install on the host and client computers?

A: From an administrative perspective, Citrix® GoToMyPC® Corporate 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 GoToMyPC Corporate Administration Center, you invite users to download the GoToMyPC Corporate software. You can restrict the maximum number of host computers each user can create. Users download an executable file and perform an easy, one-time installation on the host computer. Alternatively, administrators can perform a remote installation or upgrade of the host-side software. The client computer requires no software to be pre-installed by you or the user. When users connect to their host computers, GoToMyPC Corporate downloads a small Viewer plug-in to the client computer.

Q: Why do my users need to keep their host computers turned on to use GoToMyPC Corporate?

A: GoToMyPC Corporate 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 maintains a persistent connection to the poll server for new information.

Q: How do you protect the host computer from access by hackers and other intruders?

A: In addition to protecting the data through industry-standard encryption, GoToMyPC Corporate uses several methods to protect access to the host computer:

- End-to-end authenticated key agreement with the Secure Remote Password (SRP) protocol
- Password-protected access to secure website
- Host computer access protected with an additional per-host access code
- Strong passwords: Eight-character alphanumeric passwords required; special characters are allowed and the passwords are case sensitive
- Optional two-factor authentication using One-Time Passwords or RADIUS two-factor authentication (RSA SecurID integration)
- Limited log-in attempts and lockout rules configurable by an administrator
- Inactivity time-out on the website and Viewer
- User notification that the host computer is being accessed; in-session notification on the website; and a viewable record of failed log-in attempts
- Administrator notification of access via online administration tools and reports; administrator can end remote-access connections immediately if necessary

Q: How do you prevent someone from viewing or controlling the host computer while a user is remotely connected to it?

A: Protecting physical access to the host computer while the user is remotely connected is an important consideration when selecting a remote-access service, and GoToMyPC Corporate provides optional features to enhance its built-in security. Most computer configurations allow the user to blank the screen of the host computer while remotely connected to it. A user can also lock the host computer's mouse and keyboard while connected. If no activity is detected in the user's host computer for a configurable period of time, the Viewer on the client computer will automatically time out. After the connection has ended, GoToMyPC Corporate can automatically lock the host computer for certain operating systems. You can enforce the use of these security settings through the GoToMyPC Corporate Administration Center.

Q: Does GoToMyPC Corporate require a static IP address?

A: No. Unlike other remote-control and remote-access products, the GoToMyPC Corporate protocol design is compatible with dynamic and static IP addresses. GoToMyPC Corporate automatically detects the IP address, so your users do not need to configure any software settings.

Q: How does GoToMyPC Corporate work through my firewall?

A: GoToMyPC Corporate adjusts itself to your firewall, so you generally do not need to change or open ports in your organization's firewall. GoToMyPC Corporate 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 Corporate does not accept incoming connections that could allow intrusions. GoToMyPC Corporate encapsulates all traffic inside standard HTTP wrappers, ensuring compatibility with firewalls that inspect payload.

Q: Will GoToMyPC Corporate work with a Network Address Translation (NAT) device?

A: Yes. Because GoToMyPC Corporate 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 Corporate use, and can I change the port numbers?

A: GoToMyPC Corporate uses one of the several ports that are typically left open so that users can access the Internet (port 80 or 443). This means that you generally do not need to configure firewalls to allow GoToMyPC Corporate connections. If your organization uses a proxy that restricts traffic through port 80 or 443, you may open port 8200 for GoToMyPC Corporate connections. Citrix Online provides a Connectivity Test Wizard that you may use to optimize your GoToMyPC Corporate connection ports.

Encryption and authentication

Q: How secure is the connection between the host and client computers?

A: GoToMyPC Corporate 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 Citrix Online servers. Users can generate optional One-Time Passwords to provide further protection.

Q: What encryption method do you use?

A: GoToMyPC Corporate 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 Corporate 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 Corporate generates unique, secret encryption keys for each connection using fully contributory, mutually authenticated key agreement.

Q: Can I change or improve the GoToMyPC Corporate security settings or encryption method?

A: No. The strong security controls and AES encryption is pre-set, so your users cannot unintentionally compromise or weaken your network security. Organizations find that the GoToMyPC Corporate 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: GoToMyPC Corporate 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, which would require not only knowledge of the access code, but reverse-engineering of the host or viewer.

Q: Does GoToMyPC Corporate work with two-factor authentication?

A: Yes. Two-factor authentication provides security by requiring something you know (such as a password) and something you possess (such as a key fob). As optional security features, GoToMyPC Corporate offers One-Time Passwords and integrates with SecurID from RSA Security, Inc.

Q: Do you record or store the files users remotely access on their host computers?

A: For privacy reasons, GoToMyPC Corporate does not store or record user actions (such as files accessed). However, you can obtain information about a user's GoToMyPC Corporate activity, such as the connection time, duration of the connection, the host computer IP address, last log-in time and failed access attempts. In addition, you can optionally integrate session information into an existing reporting infrastructure by recording data into the Windows Event Log.

Q: How secure is the GoToMyPC Corporate website?

A: Users must authenticate themselves on the GoToMyPC Corporate website 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 website — a feature that is particularly important when using public computer terminals. To protect against attacks, GoToMyPC Corporate temporarily blocks access to the site for five minutes if a user makes three attempts to log in with incorrect log-in information. You can customize the lockout periods for users, including setting hard lockouts requiring administrator intervention.

Q: Which certificate authority do you use to issue certificates?

A: The GoToMyPC Corporate certificate authority is VeriSign, a trusted digital-certificate provider. All GoToMyPC Corporate programs are digitally signed.

Q: How do my users receive the certificate?

A: The VeriSign certificate is embedded at the beginning of every GoToMyPC Corporate 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 never seen by Citrix Online and is never stored anywhere. When the user sets the access code, the host computes an SRP verifier (a one-way function of the access code that cannot be used in its place). The user's knowledge of the access code and the host's knowledge of the verifier allow them to authenticate each other and agree on unique secret encryption keys.

Q: Must users change their GoToMyPC Corporate passwords and access codes periodically, and are users allowed to repeat passwords and access codes that they used previously?

A: By default, GoToMyPC Corporate does not require that users change their passwords and access codes at predetermined times, and users can re-use previous passwords. However, you can enforce an organization's security policies by using the GoToMyPC Corporate Administration Center to create password-related rules. For example, you can set passwords and access codes to expire at specified intervals and prevent the re-use of previously used passwords.

Security and privacy

Q: How does GoToMyPC Corporate protect the privacy of my data?

A: GoToMyPC (Citrix Online) has a strong privacy policy and will not disclose any of your personal information to third parties. Although Citrix Online servers broker all transmissions, personal data is fully encrypted the entire time. Citrix Online 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 Citrix Online servers, the data for individual connections could not be accessed or compromised.

Q: What data do you collect about each session?

A: 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 connection, the duration of a session, the IP address of client computer and failed log-in attempts. If guest invitations are used, you can view when the invitation was sent, the connection duration, the guest computer IP address and the guest email address. In addition to this basic information that you can view, GoToMyPC Corporate 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 Corporate have access to files or data on my organization's computers?

A: No. GoToMyPC Corporate and Citrix Online 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 Citrix Online servers, your organization's computers or data could not be accessed or compromised because all data streams are end-to-end encrypted using keys only known to the host and the Viewer.

Q: What data is left behind on the client computer after a user has disconnected from the host computer, and can users block cookies and still use GoToMyPC Corporate?

A: The client computer retains the GoToMyPC Corporate Viewer program in a temporary folder but does not store any data from the host computer. Neither the program files nor the log files contain personal settings or information useful to users or intruders. GoToMyPC Corporate uses a 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, and may be blocked by users if they desire. The data left behind with the cookie poses no privacy threat, even if GoToMyPC Corporate 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 Corporate does not require the use of a firewall. Unlike Virtual Private Network (VPN) remote access, a home computer running GoToMyPC never becomes an actual part of the corporate network. Therefore, security breaches such as a virus infection pose less of a threat to your network with GoToMyPC Corporate.

Q: How do you prevent hackers from randomly guessing a password?

A: GoToMyPC Corporate has security features that make it difficult for hackers to randomly guess a password. The GoToMyPC Corporate website has a feature that blocks access to the site for five minutes if a user makes three attempts to log in with incorrect log-in information (these periods and a hard

lockout are configurable by an administrator). 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. To provide further password security, users can generate One-Time Passwords.

Q: Are users automatically disconnected after a period of inactivity?

A: If no further activity is detected for 15 minutes, the user is automatically logged off the GoToMyPC Corporate website. This feature provides security for users who forget to log off public computer terminals. In addition, both you and your users can configure the Viewer to time out after a period of inactivity.

Q: How secure is the File Transfer feature?

A: As with the data that is shared between screens during the remote-access connection, file-transfer data is also encrypted using 128-bit AES encryption. This prevents intruders and hackers from obtaining sensitive documents or data. With GoToMyPC Corporate, 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. You can disable the File Transfer feature for specific users or groups if desired.

Q: How secure is the Guest Invite feature?

A: Remote connections initiated via the Guest Invite feature have the same strong security and protection as does any GoToMyPC Corporate connection, and you can disable guest access if necessary. However, with Guest Invite, GoToMyPC Corporate 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 Corporate 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 a limited period of time. If the guest does not connect within the time period specified, 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 such features as File Transfer, Guest Invite, Clipboard Sharing and Remote Printing to protect my network and confidential information?

A: Yes, you can configure access to meet your unique organizational or security policies. You can enable or deny access to File Transfer, Guest Invite, Clipboard Sharing and Remote Printing to specific users or groups.

Q: How secure is the GoToMyPC Corporate data center?

A: GoToMyPC Corporate 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 Corporate 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 Citrix Online's Security Policy.

Q: How secure is the GoToMyPC Corporate architecture?

A: The GoToMyPC Corporate architecture is designed for security and reliability. For security, GoToMyPC Corporate has an SSL-encrypted website and end-to-end AES 128-bit encryption of the data stream. In addition, the access code is never transmitted or stored on GoToMyPC Corporate servers. Other security features include lockout protection, inactivity time-out 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 Corporate access to authorized people in my company?

A: To give your information systems staff more control of GoToMyPC Corporate access in your organization, you can use the Authorization Management Service or Signature Protocol feature. AMS limits or prevents inbound or outbound GoToMyPC activity from IP address ranges that you designate. This enables GoToMyPC Corporate customers to limit access to only authorized GoToMyPC Corporate accounts. Any organization not currently a GoToMyPC Corporate customer can use the free AMS service to block GoToMyPC Corporate access throughout the organization. The Signature Protocol feature enables administrators to prevent non-permitted GoToMyPC access by limiting host computers within a network to a specific GoToMyPC Corporate account.

Q: How do I restrict computers from being remotely accessed via GoToMyPC Corporate?

A: In addition to limiting the maximum number of host computers users can create, you can maintain control over the computers on each end of the remote connection by optionally requiring the authorization of host and client computers through a unique identifier. By authorizing the setup of host computers in advance through an approval process, you can control the computers that can be remotely accessed. The security of your corporate network can be protected further by requiring authorization in advance for specific client computers.

Q: Can I restrict remote access to specific files, applications or services on a host computer?

A: The same access policies you have applied to your corporate network apply to GoToMyPC Corporate users. Once connected to a host computer, users have the same access rights to files and applications as if they were sit-

ting at their host computers. For additional security, you can define the days and times users are permitted to remotely access their host computers with GoToMyPC Corporate.

Contact us

To learn more about GoToMyPC Corporate 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/corp.

CITRIX® | online

Citrix Online Division
6500 Hollister Avenue
Goleta, CA 93117
U.S.A.
T +1 805 690 6400
info@citrixonline.com

Media inquiries:
pr@citrixonline.com
T +1 805 690 2969

Citrix Online Europe
Middle East & Africa
Citrix Online UK Ltd
Chalfont Park House
Chalfont Park, Gerrards Cross
Bucks SL9 0DZ
United Kingdom
T +44 (0) 800 011 2120
europe@citrixonline.com

Citrix Online Asia Pacific
Suite 3201
32nd Floor
One International Finance Center
1 Harbour View Street
Central, Hong Kong SAR
T +852 100 5000
asiapac@citrixonline.com

About Citrix Online
Citrix Online solutions enable people to work from anywhere. Our products include GoToAssist® for remote support, GoToManage™ for IT management, GoToMeeting® for online meetings, GoToMyPC® for remote access, GoToTraining® for interactive online training and GoToWebinar® for larger web events.

08.09.10/B-31523/PDF