GoToMyPC Corporate Advanced Firewall Support Features

Citrix® GoToMyPC® Corporate features Citrix Online’s advanced connectivity technology. We support all of the common firewall and proxy configurations found on corporate LANs today. There is usually no need to adjust your network or firewall. Our software makes smart, secure use of your existing firewall and proxy configurations. And, with our comprehensive set of additional security features, you can take a flexible approach to balancing maximum performance with modern network security.

The intended audience for this document:

- Network Administrators desiring assistance with the setup of GoToMyPC Corporate in environments where it does not function optimally upon the initial setup.
- Network Administrators looking to maximize the performance of GoToMyPC Corporate by tuning their environment.
- Security Administrators needing to understand the communication behavior of GoToMyPC Corporate to evaluate any impact on network security.

Briefly, let’s revisit the main purpose of your network’s firewall and proxies:

- Firewalls prevent intruders from communicating directly with machines on the inside where they might exploit vulnerabilities.
- Firewalls prevent compromised machines on the inside from contacting arbitrary services on the outside to leak information or attack further machines.
- Firewalls may scan and filter incoming documents for viruses and other attacks.
- Proxies are similar to firewalls in the way they filter, but they additionally provide an audit trail of accessed Web resources.
- Proxies reduce bandwidth usage through caching.

Our lightweight software components dynamically analyze your firewall/proxy setup and conditions and find the best paths for connectivity. In establishing this connectivity, Citrix Online’s communication technology does not open any new communication channels that an intruder could exploit, nor does it require any new “holes” to be opened in the firewall. It does not accept any incoming connections and it does not establish VPN-like network links that other software could hijack. Security is built in from the system architecture to the protocols. The following sections will detail how our communication technology works and will show you how you can best achieve the behavior and performance that you require.
**THE SOFTWARE COMPONENTS AND THEIR NETWORK CONNECTIONS**

GoToMyPC Corporate requires connectivity with Citrix Online’s servers to operate. The types of connections required to operate broadly fall into two categories:

- Long-lived JEDI connections (JEDI is the name of our streaming connection protocol) to the servers for receiving notifications and for streaming real-time data. Each JEDI connection uses one persistent TCP/IP socket.
- Periodic short HTTP requests to the server for control information.

**GoToMyPC Corporate Uses These Connections As Follows:**

- The GoToMyPC Corporate service running on a host PC uses persistent JEDI connections to Citrix Online’s Web server to check for connection requests.
- The GoToMyPC Corporate host and the Viewer use standard HTTP GETs and POSTs to Citrix Online’s communication server to control the session and to push chat text back and forth, and they use a JEDI connection to the comm server for screen-sharing data as well as for keyboard and mouse event.
- The file transfer module uses a JEDI connection to the comm server to transmit files.

**FIREWALL NAVIGATION/Negotiation**

All of the various modules of Citrix Online software use identical communication code. Upon startup, each module always performs a number of communication initialization tasks to find the best network path to Citrix Online’s servers. In environments with firewalls and/or proxies, the challenges are twofold: first, to detect and locate the appropriate firewall/proxy, and second, to determine the best protocols with which to speak to or through that firewall/proxy.

Specifically, the initialization tasks perform the following actions:

1. Collect all available proxy information and compile a list of potential proxy addresses. Proxy information is collected from:
   - User settings in Internet Explorer, Netscape and Firefox.
   - Automatic proxy configuration files indicated in the browser settings and stored on the LAN.
   - The connections used by any currently active browser.
   - A Citrix Online software registry entry used to keep track of previously discovered proxies.
2. Open connections to Citrix Online’s servers using:
   a. Direct TCP connections to ports 80, 443 and 8200 of Citrix Online’s servers
   b. Indirect connections to Citrix Online’s servers via the proxies detected in the initialization tasks detailed above.
3. Test the successfully opened connections by performing a few requests on each connection. The test depends on the module:
   - Modules needing standard HTTP perform a few simple HTTP requests.
   - Modules needing a JEDI connection perform a sequence of custom streaming requests.

During the testing of connections via a proxy, the proxy may return authentication requests, i.e., require that the user authenticate himself/herself to the proxy to gain access to the Internet. Citrix Online’s software supports both Basic and NTLM proxy authentication methods.
After the software has determined the best connection route to use, it can use HTTP, JEDI or JEDI/SSL. The SSL variant of the protocol is used to navigate certain firewalls and proxies, and not for encryption. Our encryption always uses the 128-bit AES cipher. For HTTP, GETs and POSTs are made as either direct requests to Citrix Online’s servers or standard requests via an HTTP proxy. For JEDI connections, direct connections to Citrix Online’s servers are made, or, if a proxy is involved, the HTTP/1.1 CONNECT method is used.

DNS (Domain Name System) resolutions may not be available in all environments. This means that Citrix Online’s software cannot resolve poll.gotomypc.com to the corresponding IP address. For these cases, hostname resolution information is stored in the registry. The most convenient method for setting and modifying these entries is using the Wizard as described later.

Once a successful connection has been established, the details are stored as “last known good connection method” in the registry as follows:

HKEY_LOCAL_MACHINE\SOFTWARE\CitrixOnline.com\ConnectionInfo\n
- A list of SOCKS proxies
- A list of HTTP proxies
- Scrambled User ID + password for Basic Proxy Authentication
- A lookup table of Citrix Online server hostnames to their IP addresses

**Additional Considerations Regarding the GoToMyPC Corporate Service**

GoToMyPC Corporate installs as a service and must be installed by a user with administrative privileges. The benefit of this is that GoToMyPC Corporate starts as soon as the PC boots, thus allowing a user to log in remotely. Also, a user can log out remotely and then log in again under the same or a different user ID. Although GoToMyPC Corporate can be set to start manually or at log in, the user must be logged in for the PC to be accessible remotely, and it is impossible to log out and log back in remotely.

**The Wizard Connectivity Tests**

When you want to optimize or analyze the performance of Citrix Online software on your network, or if you need to update the Citrix Online settings in the registry, you can use a small downloadable Wizard to do so. The Wizard will create a detailed report from all of its connection tests and can optionally store some of the optimal configuration info determined by those tests into the registry. Information you might need to store in the registry is your “last known good connection method” and the authentication information needed to get through any proxies that require that.

**Wizard Connectivity Test: [www.gotomypc.com/wizard](http://www.gotomypc.com/wizard)**

The Wizard Connectivity Test works just like the software connections described previously, but the Wizard lets you email a detailed summary of this process to Citrix Online for diagnosis, as well as optionally store some of the results in the registry for automatic use by the other software components. This is what the Wizard performs:

1. Dynamic Proxy Detection
   a. Gather all possible info from system to locate proxies.
2. Ping Tests
   a. Ping possible proxies to discover initial responses.
   b. Try direct connections to our servers on ports 8200, 80 and 443.
3. HTTP Connection Tests
   a. Find out how each proxy is going to treat HTTP variations.
   b. Test connection quality for HTTP.
   c. Discover transparent proxies and their behavior.

4. JEDI Connection Tests
   a. Find out how each proxy is going to treat our JEDI stream.
   b. Test connection quality for JEDI.

5. DNS Test
   a. Test DNS resolutions and, if not available, store our current server IP addresses in the registry.

6. Connectivity Profile Summary
   a. The Wizard then lets you email us the test results for analysis. This is only recommended if connectivity problems are encountered.
   b. Steps for possible performance optimizations are revealed.
   c. Connectivity info is stored in the registry for use by other software components.

You might want to run the Wizard at times of network congestion to help reveal the cause of any performance degradation. If you have an isolated problem, run it on a workstation that is having trouble, then run it on one with no problems for comparison. The minimum requirement for GoToMyPC Corporate to work well is that JEDI must work on at least one of the connections. The Wizard results show this readily, as well as provide information useful for performance tuning or analysis.

**UPDATING CONNECTION INFORMATION IN THE REGISTRY WITH THE WIZARD**

The ability to update connection information in the registry is an important Wizard feature. By using certain data and results from the tests it performs, the Wizard can store some important settings in the registry to assist all future connections. When the Wizard detects changes to connection information, it displays this check box near the end of the test run:

[X] Update settings in Registry

This box will be checked by default if something was discovered during the tests that might be beneficial if made available for use by our other software components. The Wizard registry updates are important when:

- DNS is not available, so we store a lookup table of Citrix Online host names to their IP addresses.
- One or more proxies that require basic proxy authentication are discovered, so we store the authentication info in an encoded format to use for all future accesses.
- In the case of GoToMyPC Corporate, proxy information is not available to the service.
- Of all of the discovered or known proxies, a better/faster one has been found, so we note that this is the new preferred proxy to use.

**TUNING YOUR FIREWALL/PROXY FOR MAXIMUM PERFORMANCE**

The ideal environment for operating GoToMyPC Corporate is one in which direct outgoing connections, without intermediate proxies, can be established to Citrix Online’s servers. If our Wizard Connectivity Test indicates that no such direct route is available, our recommendation is to open up one or more ports for outgoing connections.
To do so, adjust your firewall to allow outbound connections to port 8200. You may limit the destination IP addresses to our servers, e.g., 63.251.224. and 64.94.164., although this is not recommended because additional IP addresses will be added as Citrix Online's service expands.

If you don’t run a proxy (transparent or not) for your average Web surfers on ports 80 and/or 443, and if these ports are open to allow surfing via direct connections, then you will not need to open port 8200 to get maximum throughput. Maximum speed can be achieved by having any one of ports 8200, 80 or 443 open as described.

The next-best connection route is through a fast proxy that can handle HTTP requests without unreasonable delays. This proxy can be transparent, running on ports 80 and 443, or "visible" on some other port such as 8080. To initiate the JEDI protocol for screen sharing, the proxy must allow HTTP/1.1 CONNECTs, which are used by browsers for SSL.

Citrix Online software is very economical with bandwidth thanks to excellent compression and a protocol that forwards data only when necessary. For example, if you stop moving the mouse in a screen-sharing session, the network packets slow to a tiny trickle. On average, each session uses approximately 2KB/sec.

Please contact your Citrix Online representative if you need any additional technical information or assistance.