



**GO-Global *For Windows***   
**Security Aspects**

## Introduction

GraphOn's GO-Global software gives the Windows Server operating system the capability to publish 32-bit Windows® based applications to remote client desktops, terminals and web-browsers running on PC and non-PC desktops. GO-Global has a number of integrated security features and takes advantage of other embedded security functionality which will be outlined in this document.

## Basic Installation & Default Settings

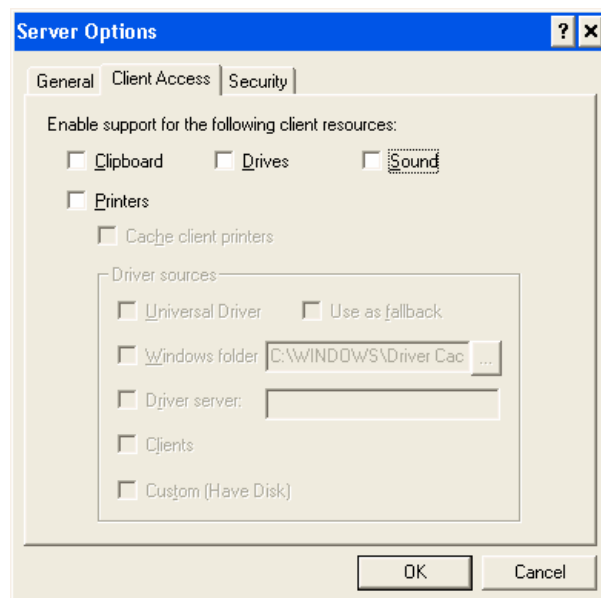
GO-Global is installed by running a single executable (ggw-xxx.exe). The InstallShield Wizard checks for existence of the following server platforms: Windows NT, 2000 and 2003. If an existing GO-Global installation is found, the application software will be updated. The installation menu subsequently installs a GO-Global display driver.



Once the software is installed, a reboot is required to initialize the registry settings and the new display driver.

The GO-Global server settings are all configured from the Cluster Manager **Server Options** menu. The Cluster manager is the primary Administration tool used to manage all GO-Global settings.

To enable a base-level of system settings, *all GO-Global options are disabled or turned off by default*. In addition, no default applications are published by GO-Global. Following the installation, the Administrator must utilize the Cluster Manager to add applications or enable support for such things as local drives, local printers or session encryption.



## Application Protocol

Founded in the early 1980's, GraphOn was an early adaptor of remote access technology and innovated low-bandwidth connectivity using COM ports over serial lines. During those years GraphOn developed a proprietary protocol called RXP (Rapid-X Protocol). The protocol is adaptive, uses multiple layers of compression and is optimized to handle low-bandwidth communications. The proprietary nature of the protocol gives it a layer of security when compared to open-source protocols or even better known "closed" protocols such as ICA.

## GO-Global Data Port

By default, GO-Global servers accept inbound RXP sessions via TCP port 491. For added security, some administrators like to change this port number. This port can be changed to reflect any acceptable port as defined by the company's security policy.

GO-Global uses a TCP port vs. UDP ports because TCP is more efficient and reliable while UDP is inherently less secure than TCP. Generally speaking, the use of UDP packets doesn't guarantee any data communication in either direction which makes UDP's primary use better suited toward broadcasting messages but not ideal to client-server applications such as GO-Global.

The actual TCP port number, 491, is a low number and referred to as a "Well Known Port Number" which is officially assigned and managed by the IANA. As innovators of remote access solutions, developers at GraphOn were able to get a low TCP number assigned which can only be used by system (or root) processes or by programs executed by privileged users. By comparison, other remote access vendors use both TCP and UDP port 1494 which is a registered port to be used by "ordinary user processes or programs executed by ordinary users." For additional reference, see <http://www.iana.org/assignments/port-numbers>.

From a security perspective, having a low TCP number is generally seen as more trusted and perceived to pose a lower security risk. As an example, the Department of Defense (DoD) expressly forbids the use of port 6000 because of a potential risk to security. Since Graphon's Go-Global does not use port 6000 or any other port that is restricted on DoD firewalls it clearly offers a secure alternative.

## Encryption

GO-Global offers integrated DES (Data Encryption Standard ) encryption with 40-bit key strength. This SSL encryption (known as secure socket layer) is the same encryption that web browsers use to protect credit card orders over the internet. The encryption key is not as strong as others but it is fast, reliable, an industry standard and it offers a secure option for using GO-Global application software. GO-Global for Windows will be upgraded to utilize 256-bit AES encryption in the near future.

## Using a VPN with GO-Global

Third party Virtual Private Networking (VPN) software can be used to create a secure, encrypted "tunnel" from the client device to the GO-Global servers. This software utilizes the user's local ISP and the Internet to connect to the corporate office. Once this secure connection is established, a private tunnel is created that connects the local user to the corporate network. The local user can access the corporate network as if he was attached to the network locally. All traffic that flows back and forth is encrypted by the VPN software. Through this VPN tunnel, the user can launch GO-Global sessions. The RXP protocol itself is not encrypted directly; rather, it is encrypted by the VPN software automatically.

Many companies choose to use VPNs for their users to access GO-Global applications from remote locations. In most instances, VPN access to GO-Global applications is chosen because the company already has an existing VPN solution in place for remote access to other applications. They can easily extend their existing VPN environment to support GO-Global session traffic from remote users.

## Proxy Server Tunneling

GO-Global supports Proxy Server Tunneling, also known as "HTTP Connect". This allows a user who accesses the Internet via a Web proxy server to connect to GO-Global Servers on the Internet. Administrators can use this option to "control" and track users as well as implement a well known port and RFC standard.

When using a proxy Server, keep in mind that by default, all traffic is denied on all networks on the server (using Microsoft's ISA server for example). The GO-Global Server should be configured to accept connections on port 443 only.

## Application Security and User Authentication

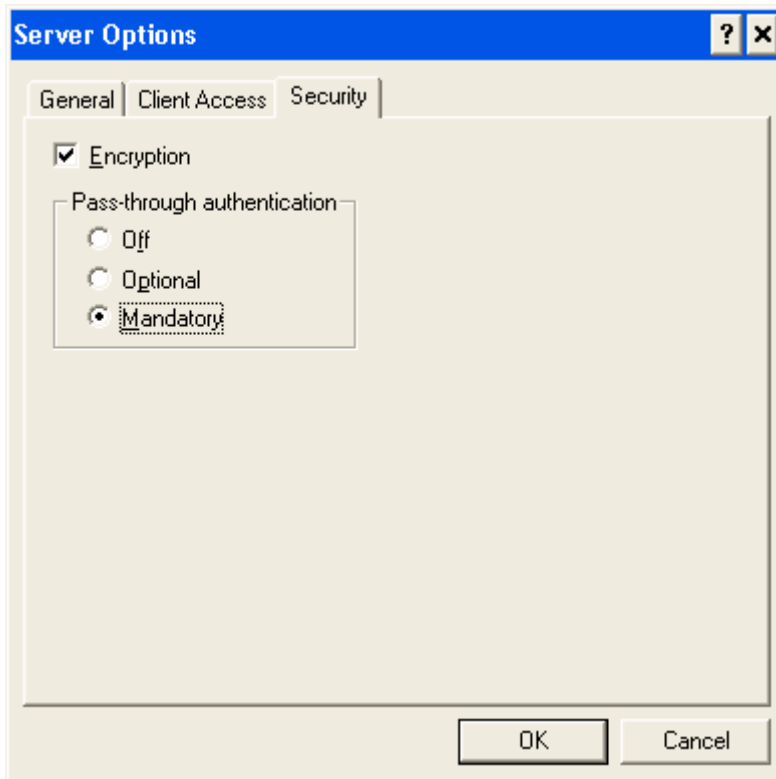
A software application is only as secure as the Operating System it is installed on. In the case of GO-Global, the server software does not install or maintain its own database of users or applications, but rather inherits all aspects of user and data security from the Windows Server OS. Security settings for the user and application are done at the Windows OS level and are passed to GO-Global during the log-in process. It is recommended to use Windows group policies rather than individual application permissions which will ease user management and increase application security.

It is also important to note that GO-Global provides application publishing only. This means that the user has direct access to the application but not the Windows desktop. For instance, a user can have a desktop application shortcut that brings them directly to the remote application. The application appears as if it is running natively on the local desktop. Other remote access applications rely on passing the user through a desktop log-in process. In contrast, the GO-Global user does not rely on a remote Windows desktop or a secondary Start button to launch their application. In most instances, a user *only* requires access to the remote application and not another desktop. There is no incentive for the user to "browse around".

Keeping the user contained within a direct application-server connection provides an added level of security.

## Pass-through Authentication

Network security can be enhanced by turning on Pass-through authentication within the GO-Global Cluster Manager. When using this option to gain additional security, it is recommended to choose the "Mandatory" setting. This option allows forces network authentication and does not allow local user accounts to access the GO-Global server.



Force network authentication with pass-through authentication

## Enterprise Licensing

The use of server based licensing offers yet another layer of application security. Some applications provide user-based licensing but server based (enterprise) licensing is deemed more secure because it relies on central management. This provides the user with automatic access to additional licenses (as needed) and the Administrator with more management control.

GO-Global licensing can be configured so it can be locked down for a given application, a specific server, or a network domain. In addition, any number of redundant license servers can be implemented.

## **GO-Global and Web server Lockdown**

If your GO-Global server is running IIS on a Microsoft platform, the Microsoft IIS security lockdown tool provides an automated, easy to use way to lock down your web servers. You can download the IIS lockdown tool for no charge from Microsoft's website. ([www.microsoft.com/technet/security/tools/locktool.asp](http://www.microsoft.com/technet/security/tools/locktool.asp))

## ***References***

Luotonen, Ari, "Tunneling TCP based protocols through Web proxy servers," August 1998, (online at: <http://www.web-cache.com/Writings/Internet-Drafts/draft-luotonen-web-proxy-tunneling-01.txt>).

"Internet Assigned Numbers Authority", IANA, April, 2005  
<http://www.iana.org/assignments/port-numbers>

Brian Madden, "Citrix MetaFrame XP Security Design", November 2002 (online at <http://www.brianmadden.com/content/content.asp?ID=96>)