GO-GLOBAL SECURITY OVERVIEW

INTRODUCTION

The integrity and security of organizational and customer data is of paramount importance to every organization due to the proliferation of hacking attacks and the regulatory requirements for system access controls like the US's Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA), and the European Unions' General Data Protection Regulation (GDPR). As more employees work from home, the security of remote access solutions like GO-Global are subject to additional scrutiny by IT security teams. This document addresses those security-related concerns.

GO-Global leverages the best available security technologies to provide its customers with a multi-layered security system that ensures data security and customer privacy. GO-Global's integrated security features and additional capabilities are detailed below.

GO-GLOBAL SESSION PROTOCOL

GraphOn was an early innovator of client remote access technology. The foundation for GO-Global is a proprietary, low-bandwidth protocol for connectivity over serial lines called RapidX Protocol (RXP). RXP is adaptive, uses multiple layers of compression, and is optimized to ensure the lowest possible bandwidth utilization. Because RXP is closed source, it offers additional defense against attackers, compared to open source protocols such as RDP, where security weaknesses have been found and exploited.

BASIC INSTALLATION AND DEFAULT SETTINGS

GO-Global is easily installed using a single installer executable on the host that will either install or upgrade the GO-Global software. When installation is complete, the host must be restarted to initialize the registry settings and to enable the GO-Global software and drivers.

By design, all configuration options that enable sharing of server or client resources are disabled. Additionally, GO-Global publishes no default applications. GO-Global Host configuration and management are accessed through the **Admin Console** under the **Host Options** menu. Administrators can publish applications, monitor user and host activity, and enable features such as client printing, client clipboard, and encryption using this menu.

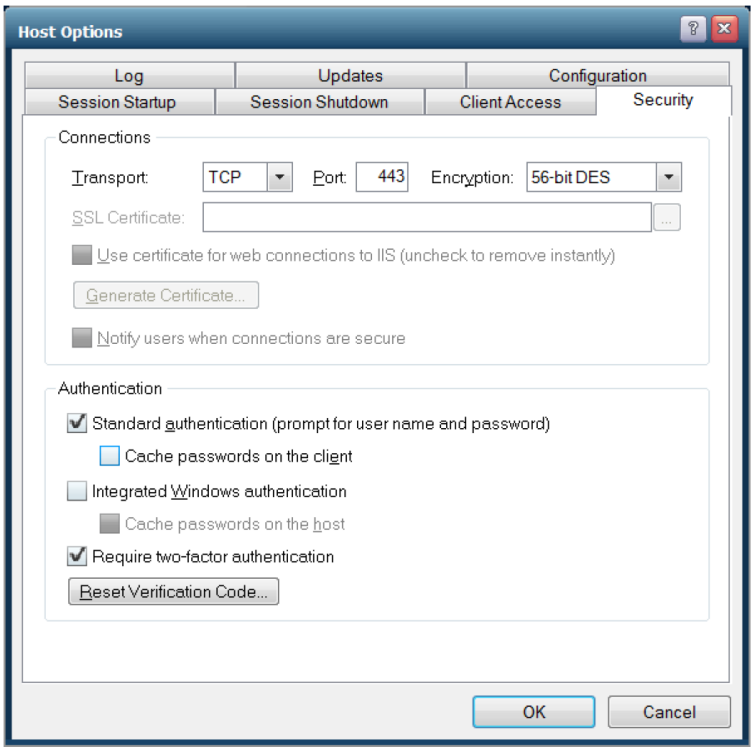

Figure 1. Host Options Menu, Security Tab

CLIENT SESSION ENCRYPTION

By default, GO-Global encrypts sessions using DES (Data Encryption Standard) with 56-bit key strength for all client session connections to protect against basic packet sniffers and clients intercepting raw data communications. It is fast, reliable, and offers an immediate level of security for LAN-based connections via GO-Global.

For internet communications and security-conscious environments, GO-Global offers SSL-based transport with the following encryption algorithms: 128-bit RC4, 168-bit 3DES and 256-bit AES. These higher encryption algorithms require that the administrator applies a signed SSL Certificate on the host, which can be generated using any standard Certificate Authority. Administrators can also generate trusted SSL certificates for GO-Global Hosts through the Security tab of the Host Options dialog of the Admin Console, where the GO-Global Host has a publicly registered DNS address. This allows administrators to enable strong encryption and SSL/TLS security without purchasing a certificate from a third-party Certificate Authority.

For more detail on GO-Global encryption functionality, see GO-Global Tech Note 205.

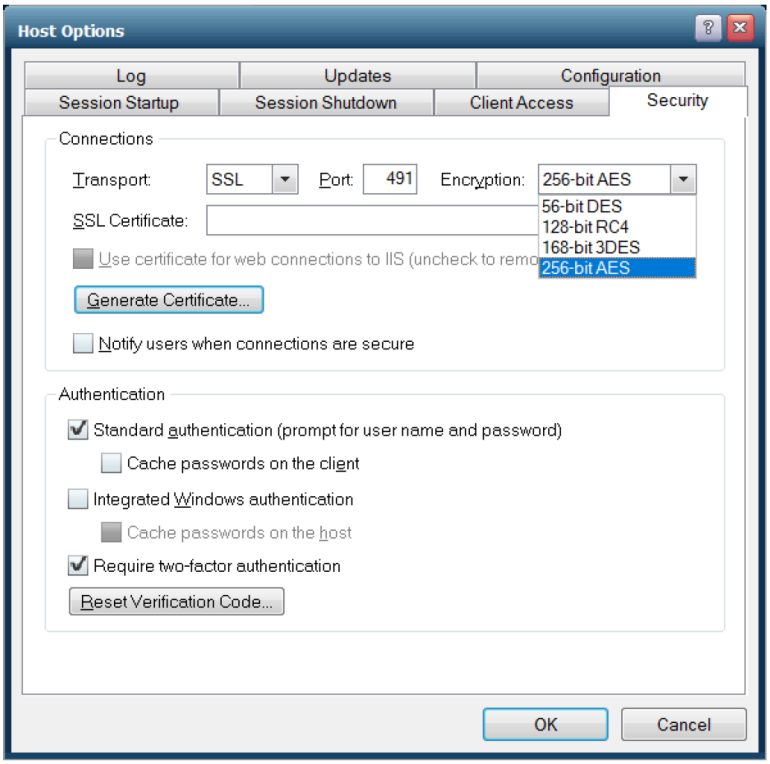

Figure 2. Generating Trusted SSL Certificates for Trusted Hosts

USING A VPN WITH GO-GLOBAL

Administrators using GO-Global can employ Third-Party Virtual Private Networking (VPN) software to create a secure, encrypted *tunnel* from the client device to GO-Global Hosts. The remote end user can launch GO-Global sessions through the VPN tunnel. When using a VPN, GO-Global's proprietary RXP does not need to be encrypted directly, although it can be for an extra level of security. When travelling through a VPN, it is encrypted by the VPN software.

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 Hosts on the internet. When using a proxy server keep in mind that, by default, all traffic is denied on all host ports, so the GO-Global Host 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 on which it is installed. GO-Global does not install or maintain its own user or applications database. Instead, it inherits all aspects of user and data security from the Windows Server operating system. Security settings for the user and application are configured at the Windows OS level and are passed to GO-Global during the logon process.

Additionally, Windows file, folder, share, printer and registry permissions are all respected by GO-Global and are central to the security of any Windows system. Unless end users are given Administrator or elevated privileges, they will not be able to access system folders, corrupt or break the server, or otherwise cause security threats.

GraphOn recommends using Windows Group Policies for all system-side security settings, especially in a load balanced server farm, to ensure consistency across all hosts.

TWO-FACTOR AUTHENTICATION

GO-Global's Two-Factor Authentication (2FA) (also known as "2-step verification") is an advanced authentication feature that provides an extra layer of security by optionally requiring users to enter a 6-digit code from an authenticator app on a smart phone, in addition to their user name and password. This ensures that even if a user's password is compromised, the attacker will still not be able to access the host system without access to the user's unlocked phone. This renders brute force and dictionary password searches useless, which is especially critical as more organizations enable remote working with vulnerable remote desktop clients. 2FA also reduces the burden of forcing a complex password policy.

GO-Global's Two-Factor Authentication requires that all users have a smart phone with an authenticator app such as Google Authenticator or Authy installed.

Figure 3. End User Start Window for Two-Factor Authentication Registration

GO-Global's proprietary RXP was designed to use TCP as it provides reliable data transmission and guarantees delivery. RXP has the registered IANA designation of TCP port 491. This TCP port number, 491, is a low number and can only be used by system (or root) processes or by programs executed by privileged users. By comparison, other remote access solutions 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."

GO-Global Hosts accept inbound client RXP sessions via TCP port 491. For added security, this port can be changed to reflect any acceptable port as defined by a company's security policy, thus making their GO-Global implementation unique and difficult to detect.
Low TCP numbers, such as 491, pose a lower security risk, since a login process is required. The Department of Defense, for example, expressly forbids the use of port 6000 because of potential security risks. GO-Global does not use port 6000 or any other port that is restricted on Department of Defense firewalls.

GraphOn Corporation
6 Loudon Road, Suite 200, Concord, NH 03301 USA sales@graphon.com

[REVISION DATE 2020.08.28]