OVERVIEW

GO-Global Security

An organization's corporate and customer data integrity and security is of paramount importance due to the proliferation of hacking attacks and the regulatory requirements for system access controls like the United States' Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA), and the European Union's General Data Protection Regulation (GDPR).

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 Microsoft® 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, management, and security-related functions 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, encryption, and authentication using this menu.

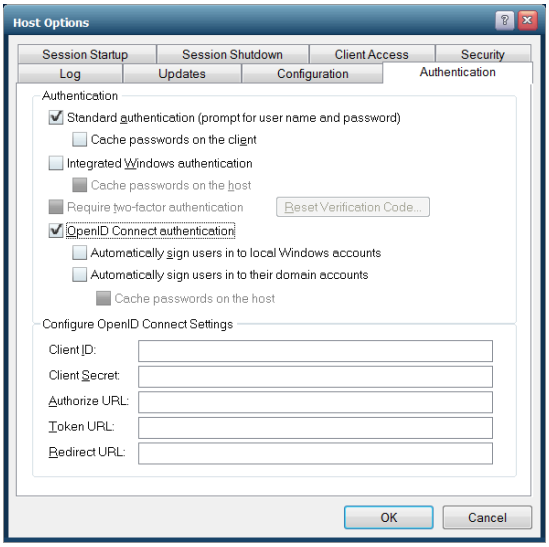

Figure 1. Host Options Menu, Authentication Tab

Continued on next page

GO-Global Security

OVERVIEW

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.

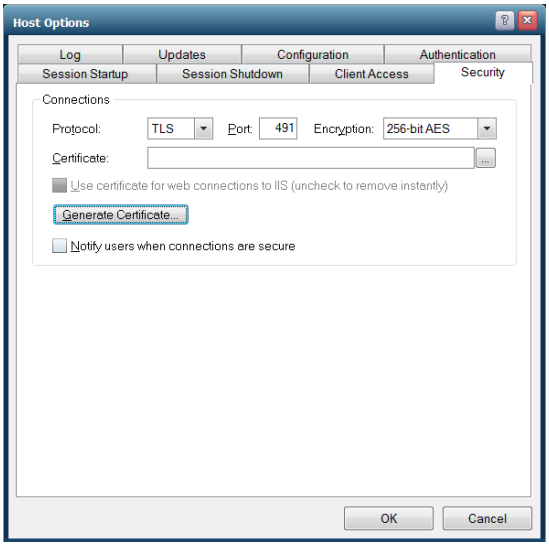

Figure 2. Generating Trusted TLS Certificates for Trusted Hosts

For internet communications and security-conscious environments, GO-Global offers TLS-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 TLS Certificate on the host, which can be generated using any standard Certificate Authority. Administrators can also generate trusted TLS certificates for GO-Global Hosts through the Security tab of the Host Options dialog in the Admin Console, where the GO-Global Host has a publicly registered DNS address. This allows administrators to enable strong encryption and 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.

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, RXP 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.

Continued on next page

GO-Global Security

OVERVIEW

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.

Single Sign-On Support

Single Sign-On (SSO) is a user authentication tool that allows users to log in to and access multiple applications, websites, data, and workstations using one centrally managed set of credentials — a username and password. Overall, single sign-on has made securing identity access and moving to the cloud significantly easier for organizations. Additionally, single sign-on reduces helpdesk calls to retrieve lost or forgotten passwords, which, according to Gartner, make up 30 to 50% of all helpdesk calls.

SSO has historically only been available for web applications. Authentication events within Windows OS occur through Winlogon, the Windows authentication module that performs interactive logons for a session—where a user logs directly onto the operating system with a username and a password. Because Windows requires a user name and password to log on, IT cannot include Windows applications in cloud implementations using single sign-on without a customized Credential Provider.

GO-Global eliminates that requirement with Single Sign-On Support for OpenID® Connect (OIDC), which enables organizations to use IODC identity providers like Okta® and Microsoft® Active Directory Federated Services (ADFS) for single sign-on into GO-Global Windows hosts. With GO-Global, users who sign in to an enterprise web application or portal using an identity provider such as Okta or ADFS can access GO-Global Hosts from their browsers without having to re-enter their credentials, enforcing the organization's authentication policies and reducing lost and forgotten password calls to the helpdesk.

Once a user has authenticated via OIDC, GO-Global gives administrators several options for authenticating the user automatically on Windows. For example, if the identify provider is integrated with the organization's Active Directory, GO-Global can automatically sign the user in to the user's domain account. Alternatively, if Active Directory integration is not required or desired, GO-Global can automatically create a local Windows account for the user.

Continued on next page

GO-Global Security

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 username 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

Integrated Windows Authentication

Administrators can enhance GO-Global end users' network security by disabling Standard authentication (prompt for user name and password) and enabling Integrated Windows authentication on the Authentication tab of the Host Options dialog in the Admin Console. With this configuration, all non-Windows clients are denied access to GO-Global Hosts, so GO-Global end users must log on to their Windows client operating systems with an Active Directory account that the GO-Global Host trusts. Additionally, user accounts local to the GO-Global Host are not allowed access. The user is authenticated as a member of the NETWORK group and access to network resources from the GO-Global Host are restricted.

If an end user requires unrestricted network access from the GO-Global Host, a less secure option is to enable the Cache password on the host setting. This will prompt the GO-Global Host to query the user for a valid user name and password. Passwords are encrypted with the user's security context and stored in the user's profile on the GO-Global Host. With subsequent connections to GO-Global, the end user is automatically logged in, added to the host's INTERACTIVE group, and is granted the same access rights had he logged on to the host console.

Continued on next page

GO-Global Security

OVERVIEW

Application Sandboxing

GO-Global publishes applications individually, but some applications can launch others and access files and registry keys. Administrators who want to prevent that behavior due to security, licensing, or performance concerns can do so using GO-Global's sandbox feature, which allows them to restrict user access to files and programs on a GO-Global Host. These restrictions apply to end users only, not to administrators or members of the Administrators Group.

GO-Global's sandbox allows the administrator to tightly restrict process behavior and deliver a locked-down application to the end user.

GO-Global Client Connectivity and Port Numbers

In TCP/IP networking, a port is a mechanism that allows a computer to simultaneously support multiple communication sessions with computers and programs on the network. A port directs the request to a specific service at that IP address. The packet destination can be further defined by using a unique port number. The port number is determined when the connection is established.

The Internet Assigned Numbers Authority (IANA) defines the unique parameters and protocol values necessary for operation of the Internet and its future development. For additional reference, see http://www.iana.org/assignments/port-numbers.

About GO-Global

GraphOn created GO-Global to enable reliable, secure, multi-user access to Windows applications from any location, device, and operating system. GraphOn GO-Global combines the scalability, performance, and end user feature set of multi-user application publishing products with the easy management of remote PC access products, reducing administration and hardware costs, increasing end-user efficiency, and lowering total cost of ownership. GO-Global is available in multiple subscription license options to fit a wide variety of use cases, so organizations can select the scenario that best fits their needs and lowers their risk.

GRAPHON

GRAPHON CORPORATION
189 North Main Street, Suite 102 • Concord, NH 03301 USA • **sales@graphon.com**