GO-GLOBAL®

Administrator Guide

6.3.3

[2025.07.17]

COPYRIGHT AND TRADEMARK NOTICE

CONTACT INFORMATION

GraphOn Corporation
189 North Main Street, Suite 102
Concord, NH 03301 USA
sales@graphon.com
graphon.com

CONTENTS

CHAPTER I Introduction **1**

Introducing GO-Global 1

GO-Global Features 1

New Features 6

System Requirements 7
- GO-Global Host 7
- GO-Global Client 8
- Browsers 8
- Port Requirements 9
- GO-Global Protocol Requirements 11

CHAPTER II GO-Global Licensing **12**

Overview 12

On-Premises Licenses 14
- License Creation 14
- Activating GO-Global 14
- Adding Seats — On-Premises Perpetual 15
- Adding Seats — On-Premises Subscription 16
- License Upgrades and Rehosts 16
- License Database 17
- Multiple Host Environments 17
- High Availability 18
- Using On-Premises Licenses in Cloud Environments 22
- Emergency On-Premises Licenses 23

Cloud Licenses 24
- License Creation 24
- Activating GO-Global 25
- Adding and Removing Seats 26
- License Upgrades and Rehosts 26
- License Management 26
- Cloud License Activation via PowerShell 27
- Multiple Host Environments 29
- High Availability 31
- Emergency On-Premises Licenses 38

CHAPTER III Configuring the Host **40**

Installing the GO-Global Host 40
- Activating GO-Global with an On-Premises License File 40
- Activating GO-Global with a Cloud License 41
- Upgrading to GO-Global 6.3 from Earlier Versions 42
- Activating GO-Global using an On-Premises Trial license 44
- Installing a Perpetual, On-Premises License 44
- Using GO-Global's Integrated Web Server 45
- Installing the Web Files on a System other than the Host 46
- Hosting Web Files from a Directory other than the Default Directory using IIS 46
- Running GO-Global through Apache HTTP Server 47

Enabling Internal and External Users to Open Secure Connections to a Host 48
Server Roles and the Configuration Tab 49
Application Host Managers and License Servers 49

Downgrading GO-Global 50

Managing Applications 51
Installing Applications 51
Publishing Applications 51
Sharing a Link to a Published Application 52
Editing the Web Server Address 54
Editing the Host Address 55
Editing the Virtual Directory 55
Editing the Protocol 56
Running the Application Outside the Browser 56
Enabling Access for Remote Users 57
Setting Default Link Properties 57
Duplicating an Application 57
Editing an Application's Properties 58
Assigning Application Launch Parameters to Users or Groups 60

CHAPTER IV Running GO-Global 62

AppController 62
User names 63

GO-Global Web App 65
Running the GO-Global Web App 65
Running the GO-Global Web App with AppController 66
Accessing the Host or Relay Load Balancer Directly from the Internet 68

macOS App 68

GO-Global Startup Parameters 70

Modifying the Logon HTML Page 73
Changing the Default Logon HTML Page 74
Specifying URL Parameters 75

Connecting with WebSockets 75

Web Files 80
Creating a URL Alias 80

Resizing the Client Window 81

Modifying the Session Window of the Web App 81

Uninstalling AppController 82

Automatic Client Updates 82

CHAPTER V Administering User Accounts 85

Administering User Accounts 85
Setting Up User Profiles 86
Setting File Permissions 86

Setting up a Network Printer 87

CHAPTER VI GO-Global Admin Console 88

GO-Global Admin Console 88

Managing Sessions and Processes 89
Terminating a Session 89
Ending a Process 89
Shadowing a Session 90

Sending Messages to Users 91

Managing GO-Global Licenses 93

Session Reconnect 95
Setting the Session Termination Option 96
Disconnecting a Session 97

Shared Account 99

Client Time Zone 100

Client Clipboard 100

Client Sound 101

Client Serial and Parallel Ports 101

Client File Access 102
Remapping Client Drives 103
Hiding Client Drives 104
Hiding Host Drives 105

Video Replay 105

File Open Redirection 106
Opening Files on the Client 107

URL Redirection 108

Smart Card Document Signing 108

Monitoring Host Activity 110
Viewing Session Information 110
Viewing Process Information 111
Searching Sessions and Processes 111
Refreshing the Admin Console 112
Setting the Refresh Rate 112
The Status Bar 113
Setting the Broadcast Interval 113
Setting the Sign In Time Limit 114

Session Startup Options 114
Applying Group Policy 114
Displaying Progress Messages 115
Logon Scripts 116
Setting Resource Limits 119
Specifying the Maximum Number of Sessions 119
Specifying the Minimum Physical and Virtual Memory 120

Session Shutdown Options 120
Specifying the Session Limit 120
Specifying the Idle Limit 120
Specifying the Warning Period 121
Specifying the Grace Period 122

Windows Compatibility Assurance 122
Runtime Incompatibility Detection 125

GO-Global Updates 125
Installing a GO-Global Update 126
Reviewing Pending and Installed Updates 126

Managing GO-Global Hosts from Client Machines 128

Keyboard Shortcuts for the Admin Console 129

CHAPTER VII Load Balancing **130**

Load Balancing 130
Load Balancing Requirements 131

Independent Hosts 132

Relay Load Balancers 133

Dependent Hosts 135
Taking a Dependent Host Offline 136

Farm Manager 137
Farm Manager Resource Requirements 137

Farm Host 139

Configuring a Third-Party Load Balancer 139
Load Balancer Affinity/Stickiness Options 142

Starting a GO-Global Session from a Browser 142

Taking a Farm Host Offline 144

License Server Configuration 144

Administering Relay Load Balancers and Dependent Hosts on Different Networks 146

Host Selection 147

Application Host Manager Recovery 149

Manually Copying Configuration Settings From one Host to Another 153

TLS Configuration with Third-Party Load Balancers 153
Application Host Manager Considerations 155
Troubleshooting TLS Issues Between Application Hosts & Application Host Managers 155
Terminating TLS at the GO-Global Hosts 157

TLS Configuration with Relay Load Balancers and Dependent Hosts 160

CHAPTER VIII Authentication **163**

Standard Authentication 163

Integrated Windows Authentication 164
Granting Launch and Activate COM Rights to Standard Users 166
Password Caching on the Host 166
Password Caching on the Client 167

Password Change 170
Changing Passwords at Next Logon 170
Prompting Users to Change Passwords Before Expiration 171
Prompting Users to Change Passwords After Expiration 172
Password Change and Integrated Windows Authentication 172

Two-Factor Authentication 173
Resetting User Verification Codes 176

OpenID Connect Authentication 177
Matching Active Directory Users to Identity Provider Accounts 180
Storing User names in Alternate Fields 181
Granting Launch and Activate COM Rights to Standard Users 183
Kerberos Authentication Within Sessions Started Via OIDC Authentication 184

CHAPTER IX Security Options **187**

Security Options 187
Modifying the Host Port Setting 187
Encrypting Sessions 188
Notifying Users of a Secure Connection 190

Selecting TLS Protocol 190

Strong Encryption Certificate Wizard 192

Obtaining a Trusted Server Certificate 194
Using an Intermediary TLS Certificate on iOS and Android 196
Resolving TLS Issues 197

Session Reconnect 198

CHAPTER X Branding **199**

Branding 199
Branding the Sign In Dialog 199
Branding the Two-Factor Authentication Dialogs 201
Branding the Program Window 205
Branding the AppController Web Interface 209

CHAPTER XI Printing **213**

Printing 213

Designating Access to Printer Drivers 214

Printer Configuration 216

Printers Applet 217
Adding and Removing Printers 217
Setting the Default Printer 218
Editing Default Printer Settings 218
Printing a Test Page 219
Changing a Printer's Driver 220
Resetting Printer Settings 220

Mapping Printer Drivers 221
Exporting Printer Settings to a File 223
Creating a Default Printer Setting File for a Mapped Printer 223

Client Printer Naming Customization 227
Adjusting the Printable Area 228

PDF Conversion and PDF Printing Libraries 228

CHAPTER XII Mobile App Console **230**

Mobile App Toolbar Editor 230

Creating Custom Toolbars 231

Log Files 237

CHAPTER XIII Advanced Topics **238**

GO-Global Host Performance Counters 238

Configuration Requirements for Delegation Support 240

Mapped Drives 243

Multi-Monitor Support 244

Specifying the Maximum Color Depth for GO-Global Sessions 244

Enabling Image Compression 246
Modifying the fontContrast Property 246
Setting a Printer Configuration Wait Time 247
Disabling the Password Expiration Warning 247
Key Reporting Method 248
Obtaining the Name of the Client Computer 250
Application Script Support 251
Mix Windows Support 252
Publishing Applications to Users and Groups 253
Published Application Registry Values 254
Publishing an Application Using Registry-Based Group Policy 255
Unpublishing an Application Using Registry-Based Group Policy 256
Advanced Session Process Configuration 258
Reducing Session Start Time by Disabling User Profile Initialization 263
Running the Windows Desktop in Background of GO-Global Sessions 263
Registering System Processes 264
Proxy Tunneling 265
Proxy Tunneling via the HTTP CONNECT Method 266
Support for Internet Protocol Version 6 267
GO-Global healthCheck Request 267
Performance Auto-Tuning 271
How Performance Auto-Tuning Works 272
Silent Installation 273
Extracting AppController MSIs 273
Running a Silent Targeted Installation 274
Automating the Configuration of GO-Global 275
Log Files 276
Selecting a New Location for the Log Files 276
Setting the Output Level 277
Maintaining Log Files 278
Changing Log Files to Text File Format 279
Client Log Files 279
Connection Monitoring 280
Connection Verification 280
Support Request Wizard 281
High Resolution Client Devices 282
Setting the Program Window Close Option 283
Reconnecting to Sessions when the Network Connection is Dropped 284
Dragging Full Windows 285
Automatic Client Keyboard Support 285
Configuring Support for Client Keyboards and/or IMEs 286
Installing Additional Keyboards and IMEs 286
Client Keyboard Mapping Files 288
Keyboard/IME Identifiers Used by GO-Global 288
Configuring Client Keyboard Options 290
Specifying Layout Text Substitutions 290

Setting the Fallback Layout Text 291
Configuring Multiple Input Locales 291
Localizing Messages 292
Language Codes 293
Web Client Language 293
AppController Language 293
Specifying a Language for Host-Side Generated Text 294
Setting Resolution on Mobile Clients 295
APPENDIX 297
RapidX Protocol (RXP) 297
Encryption and Exportation Regulations 298
GO-Global Settings 299
Third-Party Components 300
Known Limitations 301

CHAPTER I

Introduction

1

Introducing GO-Global

GO-Global is the simple and secure application virtualization solution that extends the reach of existing Windows applications to corporate networks or the web. With GO-Global, authorized employees, business partners, and customers can securely access applications from anywhere, regardless of connection, location, client platform, or operating system.

GO-Global Features

- **Network and Web Accessibility.** GO-Global provides access to Windows applications from GO-Global Hosts via the network or through Web access.
- **Cross-platform Compatibility.** GO-Global provides access to any Windows application from virtually any client platform. Applications can be run from desktop computers such as Mac, Windows, and Linux, and from iOS and Android mobile devices. Windows-based applications deployed through GO-Global look, feel, and function as if they were running on a Windows operating system, regardless of the client platform.
- **Client File Access.** GO-Global supports seamless integration of client drives, including hard disk and mapped network drives. This allows users to access files stored on the client computer and to save files locally.

- **Host Monitoring.** GO-Global provides real-time monitoring of individual GO-Global Hosts, control of individual clients and processes, and logout and shutdown for individual users.

- **Session Shadowing.** The session shadowing feature allows multiple users to view and control a single session and its applications. This feature allows help desk personnel and system administrators to help troubleshoot and debug user problems. Session shadowing may also be used for live collaboration.

- **Load Balancing.** Load balancing distributes user sessions across multiple GO-Global Hosts. When load balancing is enabled, users can reconnect to a disconnected session running on any one of the load-balanced hosts.

- **Session Reconnect.** With session reconnect enabled, GO-Global maintains client sessions on the server without a client connection. If a user deliberately disconnects from the server, or if the client's connection is lost due to network problems, the user's session and applications remain running on the server for the length of time specified by the administrator. If a client's connection to a host is broken, the client will automatically attempt to reconnect to the host.

- **Performance Counters.** Performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a server. GO-Global Host performance counters allow administrators to monitor server activity from any machine with network access to a GO-Global Host.

- **Proxy Tunneling.** Proxy tunneling allows users to connect to GO-Global Hosts on the internet via proxy servers.

- **Group Policy Support.** Using Microsoft's Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options.

- **Time Zone Redirection.** This option allows GO-Global sessions to run in the time zone of the client computer, regardless of the time zone that is selected on the GO-Global Host.

- **Backward Compatible Client and Host.** This allows a client to connect to a GO-Global Host when the major and minor versions of the client and server match but the revision (service pack) or build numbers do not.

- **Client Printing.** Users can print to client-accessible printers from applications running on GO-Global hosts. GO-Global's Universal Printer Driver supports nearly all printers on Windows, Mac and Linux clients automatically. The Universal Printer Driver allows users on Windows clients to configure all the settings of their printers (including custom settings) and allows users on non-Windows computers to configure the standard settings of their printers. And when users on non-Windows clients require access to all the settings of their client printers, administrators can configure GO-Global hosts to use native printer drivers.

- **Dynamic Display Resize.** GO-Global automatically adjusts the size of the session's desktop when the user reconnects to the session from a different device or changes the resolution of the client device.

- **High Resolution Display Support.** GO-Global supports high resolution displays. When the GO-Global client is run on Windows, GO-Global automatically uses the client computer's DPI (Dots Per Inch) setting. When the client is run on operating systems other than Windows, GO-Global uses the DPI setting that is specified for the user under the Control Panel's Display applet on the host.

- **Client Sound.** The GO-Global Host streams audio output from applications running in GO-Global sessions to Windows clients.

- **Client Serial and Parallel Ports.** GO-Global allows applications running on the host to access client machines' serial and parallel ports. This feature is supported on Windows clients only.

- **Mobile App Toolbar Editor.** Administrators can create custom toolbar buttons and menus that appear at the bottom of the GO-Global Mobile App when a Windows application is accessed from a mobile device. Custom toolbars greatly improve the usability of Windows applications when they are accessed from mobile devices such as iPads, iPhones, and Android tablets.

- **Windows Compatibility Assurance.** Windows Compatibility Assurance gives administrators the option to automatically defer installation of Windows Updates until GraphOn has verified that the updates are compatible with GO-Global. To support this, GraphOn continuously monitors Microsoft's Windows Update service for new updates. When Microsoft releases one or more Windows Updates, GO-Global suspends installation of all Windows Updates on affected GO-Global hosts until GraphOn has verified that newly released Windows Updates are compatible with GO-Global. If an update is incompatible, GO-Global prevents installation of all Windows Updates on the affected hosts until GO-Global has automatically downloaded and installed an update that is compatible with all Windows Update releases. Through this process, Windows Compatibility Assurance minimizes the risk of incompatibilities and relieves administrators of the burdens of managing Windows Updates on GO-Global hosts.

- **Licensing Summary.** A tab in the Admin Console lists the GO-Global licenses that are available to a host and displays each license's Product Code, number of seats, maintenance expiration date, and status. In addition, GO-Global notifies administrators when license expiration dates are approaching or have been exceeded.

- **GO-Global Web App.** Developed with JavaScript and HTML5, the GO-Global Web App is a zero-install client that allows users to run Windows applications from popular web browsers on Windows, Mac, and Linux computers.

- **Third-Party Load Balancer Support.** Third-party load balancer support lets administrators centrally manage hosts and sessions that are accessed via third-party load balancers. Using the Farm Manager and Farm Host roles, administrators can configure settings on all hosts in a farm at once, and they can manage and shadow sessions running on any host in the farm. In addition, these roles enable end users connecting to GO-Global Hosts via third-party load balancers to start sessions on one device (e.g., a computer in an office), disconnect, and then reconnect to their sessions from a different device (e.g., a home computer). GO-Global automatically reconnects users to their sessions, even when the load balancer fails to connect a user to the host on which the user's session is running.

- **AppController.** AppController is a next-generation replacement of the GO-Global App that can be started from a computer's desktop, a mobile device, or a web browser.

- **Strong Encryption Certificate Wizard.** The Strong Encryption Certificate Wizard allows administrators to easily generate and apply trusted TSL certificates for GO-Global Hosts, enabling strong encryption and TLS security without purchasing a certificate from a third-party Certificate Authority.

- **Two-Factor Authentication.** Two-Factor Authentication (2FA), also known as Multi-Factor Authentication (MFA) provides an extra layer of security by optionally requiring end users to enter a 6-digit code from a time-based one-time password (TOTP) authenticator app on a device (smart phone, PC, etc.) in addition to their user name and password. This significantly reduces the risk of brute force and dictionary attacks, which is especially critical as more users access corporate work computers while working from insecure home networks. GO-Global's native 2FA feature does not require any external services. It requires that all users have a device with an authenticator app such as Google Authenticator or Authy, or a password manager such as Bitwarden installed.

- **Video Replay.** Video Replay enables applications and browsers running in GO-Global sessions to replay video content on GO-Global clients.

- **URL Redirection.** This feature allows end users to click web links that open in the default browser on the client rather than the default browser on the host, so end users can efficiently access web content and videos running in GO-Global sessions.

- **Branding.** Branding allows customers to replace GraphOn's GO-Global branding on end user interface elements (e.g., Sign In dialog, Program Window, etc.) with the customers' own corporate images, logos, and names.

- **OpenID Connect.** GO-Global support for OpenID Connect (OIDC) enables enterprises and SMBs to provide their users with single sign-on support via OIDC identity providers such as Okta and Active Directory Federated Services (ADFS). For example, it enables users who sign in to an enterprise web application or portal using an identity provider to access GO-Global Hosts from their browsers without having to re-enter their credentials. In addition, it enables users to authenticate to GO-Global Hosts using a wide variety of third-party smart cards and multi-factor authentication devices and products.

  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 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.

- **Administrator Messages.** The Administrator Messages feature allows administrators to send messages to connected users and alert them of system maintenance and other events.

- **File Open Redirection Support.** File Open Redirection streamlines workflow by allowing end users to open specified file types in applications running on the client. Administrators can enable the feature for select file types (e.g., XLSX, PDF, DOCX, etc.) so that when a user attempts to access a file of a specified type from a host application that does not directly support it (e.g., opening an XLSX in Outlook), the file will instead be opened on the client with the relevant client application (e.g., Excel). File Open Redirection supports files that are opened from Windows Explorer. This feature is only supported when AppController is run on Windows and macOS.

- **Integrated Web Server.** GO-Global's Integrated Web Server greatly simplifies browser-based deployments by allowing browsers to connect directly to the Application Publishing Service (APS) on its standard port (491, by default) and download the GO-Global Web App and associated HTML files. This eliminates the need to use a separate web server (e.g., IIS) to enable browser-based access to GO-Global hosts. Administrators no longer need to configure TLS on both the APS and the web server or route traffic to different ports and servers based on the protocol.

New Features

- **Mix Windows Support.** Mix Windows support improves usability by allowing the windows of applications running locally on the client computer to be interleaved with the windows of applications running in a GO-Global session. When users activate the window of an application running in a GO-Global session, only the activated window will come to the foreground. The z-order of windows belonging to other applications running locally and in the GO-Global session will be unaffected.

- **User and Group-Based Application Publishing.** User and Group-based application publishing allows administrators to publish applications to individual users, groups, and organizational units (Ous).

- **Session and Process Search.** With the Admin Console's new Search button, administrators can quickly locate the session and processes of a specific user and eliminate the need for the Admin Console to simultaneously display all sessions and processes that are running on a farm of GO-Global Hosts.

- **Localization Support.** Text that is displayed to end users can be translated into users' native languages. This includes text displayed by GO-Global's Logon and Program Window applications and messages displayed by GO-Global clients (i.e., AppController and the GO-Global Web App and its associated web pages).

- **GO-Global healthCheck Request.** Third-party load balancers and monitoring tools can test the health of GO-Global Hosts by sending a healthCheck request to the Application Publishing Service.

- **New Universal Printer Driver.** GO-Global includes a new Universal Printer Driver that improves print quality and speed and greatly simplifies printing for both users and administrators. Users running AppController for Windows can access and use all the settings of their printers without requiring printer drivers to be installed on GO-Global Hosts.

  In most cases, this eliminates the need to:

  - Install native Windows printer drivers on GO-Global Hosts
  - Find alternatives to Type 4 printer drivers
  - Map printer drivers
  - Configure printer settings on GO-Global Hosts

- **Improved Support for Large Server Farms.** Application Publishing Service enhancements improve the reliability of communication between Application Hosts and Application Host Managers.

System Requirements

GO-Global Host

The GO-Global Host requires one of the following 64-bit Windows operating systems:

- Windows Server 2022 — Standard and Datacenter
- Windows Server 2019 — Standard and Datacenter
- Windows Server 2016 — Standard and Datacenter
- Windows 11 Version 23H2 — Professional and Enterprise
- Windows 10 (latest and prior SAC releases) — Professional and Enterprise
- Windows 10 (latest and prior LTSC releases) — Enterprise

The GO-Global Host is supported on computers that have the latest Windows Updates (released via the Windows Updates service) installed. GO-Global does not support out-of-band (OOB) Windows updates.

Users must be a member of the computer's Administrators group to install and administer the GO-Global Host.

Users must be granted the *Allow log on locally* right.

By default, the GO-Global Host accepts TCP connections on GraphOn's registered port 491. This port can be changed via the Security tab of the Admin Console's Host Options dialog. All firewalls between a GO-Global Host and its clients must allow TCP connections on the port specified in the Admin Console.

GO-Global supports TLS security and strong encryption via OpenSSL version 3.4.1. A TLS certificate is required to enable TLS security.

GO-Global can be installed and run on guest operating systems that are managed by hypervisor products such as VMware ESXi, Microsoft Hyper-V, and Citrix Hypervisor.

The GO-Global Host does not support systems that have Virtualization-based security (VBS) enabled. When VBS is enabled, System Information reports that Virtual-based security is *Running*. If the GO-Global Host is installed on a system where VBS is running, the system will crash or the GO-Global System Extensions Driver will fail to load. For more information or to disable VBS, see Tech Note 224.

GO-Global does not support host installation on a domain controller.

The color depth of the client and host must be greater than 256 — 16 million or greater is recommended.

The memory and CPU requirements of a GO-Global Host are determined by the applications that are published and the number of users accessing the system. In general, a GO-Global Host can support 12 “heavy” users/500 MHz CPU and 25 “light” users/500 MHz CPU. (“Heavy” is defined as a user running one or more large applications with continuous user interaction. “Light” is defined as a user running one application with intermittent user interaction.)

GO-Global supports a maximum round-trip latency of 500 milliseconds.

GO-Global requires a minimum 28.8 kbps modem speed.

GO-Global requires 16 kbps per user network bandwidth.

GO-Global Client

GO-Global supports the following client platforms:

- Windows 11 Professional and Enterprise (64-bit)
- Windows 10 Professional and Enterprise (32-bit/64-bit)
- macOS 13 and later
- Ubuntu 19 and 20 (64-bit)
- Red Hat Enterprise Linux 7 and 8 (64-bit)
- SUSE Linux Enterprise 12 and 15 (64-bit)
- iOS 15 and later
- Android 12 and later on ARM processors, including Chromebooks manufactured in or after 2019

The GO-Global Web App requires 200-600 MB of memory per instance depending on the monitor’s resolution size.

AppController requires 50 MB of disk space and 10 MB of memory per instance.

Browsers

For browsers running in GO-Global sessions, GO-Global supports the following:

- Mozilla Firefox (Latest Extended Service Release)
- Apple Safari 15 and later on macOS
- Google Chrome
- Microsoft Edge

Port Requirements

GO-Global has the following port requirements:

- **Independent Hosts** must allow connections from clients on the TCP port specified under Admin Console | Tools | Host Options | Security.

- **Dependent Hosts** must connect to the Relay Load Balancer on the TCP port specified on the Relay Load Balancer under Admin Console | Tools | Host Options | Security.

- **Relay Load Balancers** must allow connections from clients and Dependent Hosts on the TCP port specified under Admin Console | Tools | Host Options | Security.

- **Farm Hosts** must connect to the Farm Manager on the TCP port specified on the Farm Manager under Admin Console | Tools | Host Options | Security. Farm Hosts must allow connections from the third-party load balancer on the TCP port specified on the Farm Manager under Admin Console | Tools | Host Options | Security.

- **Farm Managers** must allow connections from Farm Hosts on the TCP port specified under Admin Console | Tools | Host Options | Security.

- To use a **cloud license,** the Application Publishing Service must be able to connect to portal.graphon.com and cloud.graphon.com on port 443.

- To use a **Backup License Manager**, the Application Publishing Service must be able to connect to the Backup License Manager on the TCP port specified under Admin Console | Tools | Host Options | Security, and the Backup License Manager must be configured to accept connections on the same port.

- To use an **on-premises license**, the Application Publishing Service must be able to connect to the GO-Global License Service (lmgrd.exe), and lmgrd.exe must be able to connect to the GO-Global license daemon (blm.exe). If there are firewall rules that restrict these connections, the GO-Global License Service should be configured to use port 27000 and blm.exe should be configured to use port 5678. In addition, if the Application Publishing Service has access to the internet, it must be able to connect to license.graphon.com on port 443.

- GO-Global's **Universal Printer Driver** uses port 9010. This port cannot be changed. If any other software on a GO-Global Host uses port 9010, users will be unable to print with the Universal Printer Driver.

- The **Admin Console** can optionally allow broadcast messages over UDP port 491, which will allow it to populate a list of other hosts. This port number cannot be changed.

Connections from Browsers to Third-Party Load Balancers

Third-party load balancers generally accept connections on either port 80 (HTTP) or port 443 (HTTPS). By default, the Web App and AppController connect to GO-Global's default port, 491. Therefore, when a third-party load balancer is used, you will generally need to configure the Web App and AppController to use the load balancer's port. You can do this by adding the **port** parameter to the URL or by specifying the port in the logon.html page.

For example, if the load balancer is configured to accept connections on port 443, configure the Web App and AppController to use port 443 by uncommenting the **controlArgs.set(["port", "491"]);** line in logon.html and changing 491 to 443.

Note that any firewalls or proxy servers between users' browsers and the load balancer must allow connections on the load balancer's port. For example, if the load balancer "front end" is set to use port 443 and there is a firewall between the internet and the third-party load balancer, the firewall must allow incoming connections on port 443.

In many cases, users' browsers will have to traverse a firewall, proxy server, or other edge device to connect to the internet. These devices may only allow outbound connections over port 443. GO-Global administrators do not always have control over these devices. Therefore, when users access GO-Global via the internet, the load balancer should generally be configured to use port 443 and not GO-Global's default port 491. In this scenario, GraphOn recommends that port 491 be configured via the Host Option's **Security** tab for GO-Global's internal communications only.

Connections from Third-Party Load Balancers to Farm Hosts

After a load balancer accepts a connection, it must forward the connection to a Farm Host. This is usually specified in the load balancer's backend settings. Farm Hosts accept connections on the port specified in the **Security** tab of the Admin Console's Host Options dialog. Therefore, third-party load balancers must be configured to forward connections to this port. In addition, if there is a firewall between the load balancer and the Farm Hosts, the firewall must be configured to allow connections on this port.

For example, if Farm Hosts are configured to use the default port 491, the load balancer must forward connections to port 491, and a firewall between the load balancer and the Farm Hosts must allow connections on port 491.

GO-Global Protocol Requirements

GO-Global relies on various network protocols and transport mechanisms to enable secure communication between its different components, as detailed in the table below. Administrators can use this information to implement appropriate network rules for their GO-Global environment.

Data Transmissions Between...	Transport Layer Protocol	Higher-Level Protocols
AppController and Application Publishing Service (APS)	TCP	RXP, RXPS, WS, WSS
Browser and APS	TCP	HTTP, HTTPS
Web App and APS	TCP	WS, WSS
APS and APS (e.g., Farm Host to Farm Manager)	TCP	RXP, RXPS
Session Processes and APS	Localhost Named Pipes or TCP	RXP, RXPS
APS and Admin Console	TCP for selected host; UDP to populate list of hosts	RXP, RXPS

CHAPTER II

GO-Global Licensing

2

Overview

Historically, GO-Global has supported only one licensing mechanism: Flexera-based, on-premises licenses. GraphOn will continue to use on-premises licenses as the sole licensing mechanism for all perpetual licenses. On-premises licenses, however, are not as well suited to manage modern, subscription-based pricing models. To reduce the burden of managing licenses and to support modern pricing models, GO-Global has added support for cloud licenses.

Unlike on-premises licenses, cloud licenses do not require a license file. As a result, customers activating GO-Global with cloud licenses do not need to know a license's Product Code (a long, random number) or the Host ID (MAC address) of the computer on which the license will be used. Customers using cloud licenses will never have the delivery of a license delayed because they entered the wrong Product Code, and they will never receive a license file that does not work because the Host ID they entered was incorrect. In addition, customers using cloud licenses never need to request a new license file or make any licensing changes on a computer—not when the MAC Address of the computer changes, not when GO-Global is upgraded, not when the number of seats changes, and not when the license is renewed.

With cloud licenses, administrators simply run the Activation Wizard on a host, sign in to their GraphOn account, and select the license they want the host to use. Thereafter, no changes are required on the computer. Changes to a license's version, seat count, and expiration date are made in GraphOn's Cloud Licensing Service and are immediately and automatically enforced by the GO-Global Hosts using the license. If the computer's MAC Address changes (e.g., in a cloud environment), the cloud license continues to work without issue. And if a customer wishes to use a cloud license on a different computer (or multiple computers simultaneously), the administrator simply runs the Activation Wizard on the new computer and selects the cloud license. There is no need to submit a request to rehost a license and wait to receive a new license file.

GraphOn expects that cloud licenses will be the primary licensing mechanism used by GO-Global customers for subscription-based models. On-premises licenses will also be supported for subscription-based models for customers who prefer or require on-premises licenses.

An Application Host or Application Host Manager must use one license type at a time – either on-premises or cloud. If an Application Host or Application Host Manager is already using one type of license, it is not possible to add seats from a different type of license to the Application Host or Application Host Manager. For example, if a Relay Load Balancer is using an on-premises license, it is not possible to add seats from a cloud license to the Relay Load Balancer.

License Consumption

GO-Global's cloud and on-premises licenses are based on concurrent usage. One license seat is consumed for each user who is actively using GO-Global from a given device. If a user runs multiple sessions from the same device under the same user account, only one license seat is consumed. In addition, license seats are released when users disconnect from sessions. No license seats are consumed by sessions that have no clients connected to them.

Due to browser security limitations, license seats cannot be shared when the GO-Global Web App is used. Each instance of the GO-Global Web consumes a license seat. For example, if the GO-Global Web App is running in two browser tabs on the same computer, two license seats are consumed.

On-Premises Licenses

On-premises licenses are enforced using license files that are tied to the MAC address (Host ID) of a computer's network adapter. A license file is only usable when it is installed on a computer that has a network adapter with a MAC address that matches the Host ID specified in the license file. License files are stored in the \Program Files\GraphOn\GO-Global\Licensing directory on GO-Global license servers.

A GO-Global *license server* is a computer on which the GO-Global License Manager service is installed and running. By default, the GO-Global Host installer, gg-host.exe, installs the GO-Global License Manager service together with the Host component. This configuration is ideal for small deployments where one computer operates as both an *application server* and a *license server*. In larger deployments, license files are generally installed on a *central license server*, with several GO-Global application servers configured to check out licenses from the designated central license server. And when high-availability is needed, redundant license servers can be configured.

License Creation

When a customer places an order for a new license, GraphOn processes the order and creates a new license in its license database. Each license is assigned a unique License Master ID and a unique Product Code. The License Master ID is a human-friendly identifier of the license in the form of "LIC-xxxxx." The Product Code is a longer, alphanumeric identifier that is required for more secure functions, such as activating a new license, renewing maintenance orders, and License Change Requests (LCRs).

Activating GO-Global

To activate GO-Global with an on-premises license, customers first activate the license to obtain a license file, and then install the license file on the designated license server. After creating the license record in its license database, GraphOn emails the license's License Master ID and Product Code to the contacts identified on the order. An administrator can then activate the license via the Customer Portal.

If the license server fails at some point in the future, you will need the license's Product Code to obtain an emergency license. The Product Code is contained within the license file. Therefore, save a copy of the license file in a safe place where you can quickly find it if there is a failure on the license server.

To activate a license

1. Sign in to the Customer Portal.
2. Click **License Management | Activate License**.
3. Enter the license's Product Code, your email address, and the Host Name and Host ID of the computer on which the license file will be installed.
4. Click **Activate License**.

The Customer Portal then validates the information entered and creates a license (.lic) file. The portal sets the name of the license file to the **License ID**, an alphanumerical identifier that uniquely identifies the license file. (For example, **8d73e4k.lic** where 8d73e4k is the License ID.) In addition, it stores the License ID in the license file, along with the license's License Master ID and Product Code. Finally, the portal emails the license file to the administrator.

To complete the GO-Global activation, the administrator installs the activated license file on the designated license server, following the instructions contained within the license file, and being sure to follow the final step and restart the **GO-Global License Manager Service**.

Adding Seats — On-Premises Perpetual

When customers need to add perpetual seats to an on-premises license server, they place an order for a new add-on license. With each order for an add-on license, GraphOn creates a new license master for the add-on seats, and emails the license's License Master ID and Product Code to the contacts listed on the order. The customer's administrator then activates the add-on license using the same procedure that was used to activate the license server's original license. When installing add-on perpetual licenses on license servers, leave any existing license files in place.

To install an add-on on-premises perpetual license

1. Copy the license file to the license server, following the instructions within the license file. Leave any existing license files in place.
2. Restart the **GO-Global License Manager Service**. The add-on license will not be recognized until the service is restarted. Restarting the service does not interrupt users who are already logged in.

When multiple license files are installed on a license server, the name of each license file must be unique on the server. GraphOn delivers license files with the file names set to the License ID, which is always unique. This allows administrators to install multiple license files on the same license server without making any changes to the files.

GraphOn recommends installing license files as delivered (with the 'LicenseID.lic' naming convention). However, administrators can rename license files, for system management reasons, for example. When administrators do this, they must ensure the names of license files are unique on the license server, and that the file extension is .lic. (For example, License1.lic, License2.lic, License3.lic.) If the file extension is not '.lic', the GO-Global License Manager service will not recognize the license file.

Adding Seats — On-Premises Subscription

To add subscription seats to an on-premises license server, customers place an order for the add-on seats. With each order for add-on seats, GraphOn creates a new license file which will *replace* the existing license file installed on the license server. The License Master ID and Product Code do *not* change. After the new subscription license file is installed on the license server, the previous subscription license file must be ***removed***.

To install an add-on on-premises subscription license

1. Copy the new license file to the license server, following the instructions within the license file.
2. Remove the previous subscription license file.
3. Restart the **GO-Global License Manager Service**. The new subscription license will not be recognized until the service is restarted. Restarting the service does not interrupt users who are already logged in.

License Upgrades and Rehosts

The version of an on-premises license must be greater than or equal to the version of GO-Global that is used with the license. Therefore, new license files are needed when GO-Global is upgraded to a new version. In addition, a new license is required when a license is rehosted (i.e., when a license is moved to a new computer with a different MAC address.)

To obtain a new license file, an administrator submits a **License Change Request** (LCR) via the Customer Portal. Change requests are typically processed within 1-2 days, but may take up to 5 business days to process. Once processed, a new license file, with a new License ID, is emailed to the administrator. (The License Master ID and Product Code do not change.) The administrator then installs the new license file and removes the old license file, following the instructions contained within the file. The old license file must be removed, because it has been voided/revoked by GraphOn, and GO-Global Hosts do not allow users to sign in when a voided license is present on the host's license server.

New license files are not required when GO-Global is downgraded. On-premises licenses are backwards compatible and are valid for any release of GO-Global with a version number that is less than or equal to the version of the license.

License Database

Customers can view the details and status of their licenses in the Customer Portal. In addition, customers can use the Admin Console to view the status and details of the license(s) that a GO-Global Host is using. Both the Customer Portal and the Admin Console display license status, version, and maintenance expiration date.

Multiple Host Environments

By default, the GO-Global License Manager service is installed together with the GO-Global Host, and the GO-Global Host is configured to use the GO-Global License Manager that is on the same computer. Alternatively, one or more GO-Global Hosts can be configured to use a central GO-Global License Manager that is running on a different computer.

To configure a host to use a license server running on a different computer

1. If there is a firewall between GO-Global Hosts and the license server, configure the license server to use port 27000, configure the license manager (BLM) to use port 5678, and open these two ports in the firewall:

    a. The license server uses ports 27000-27009 by default. Configure the license server to use port 27000 by adding 27000 to the end of the SERVER line in the license file(s) as follows:

    SERVER LicenseServer1 00d0b74f4023 27000

    b. The license manager (BLM) uses an ephemeral port by default. Configure it to use port 5678 by adding “port=5678” to the end of the DAEMON line in the license file(s) as follows:

    DAEMON BLM port=5678

    c. Configure your external firewall and any software firewall on the license server to allow TCP ports 27000 and 5678.

2. On each GO-Global Host, disable the GO-Global License Manager service:
    a. Click Control Panel | Administrative Tools | Services.
    b. Right-click GO-Global License Manager from the list of services and click **Properties**.
    c. Under Startup type, select **Disabled**.
    d. Click the **Stop** button.
    e. Click **OK**.

3. Configure each GO-Global Host to use the central license server by one of the following methods:

    a. Set the LM_LICENSE_FILE environment variable to port@host (e.g., 27000@LicenseServer1) instead of the path to the license file.

    —or—

    b. Copy the license file from the central license server to the Licensing directory on the GO-Global Host and add a USE_SERVER line directly after the SERVER line in the license file as follows:

        SERVER LicenseServer1 00d0b74f4023 27000
        USE_SERVER

High Availability

GO-Global supports high-availability for on-premises licenses via redundant license servers. If you wish to use redundant license servers, select stable systems as server machines. Do not pick systems that are frequently rebooted or shut down. Redundant license server machines can be any supported GO-Global Host machines. These servers must have excellent communications on a reliable network and need to be located in the same subnet. Avoid configuring redundant servers with slow communications or dial-up links.

GO-Global supports two methods of license server redundancy for on-premises licenses:

- Three-Server Redundancy
- License-File List Redundancy

The License Manager service should be disabled on secondary servers of Central License Servers and Three-Server Redundant License Servers.

Three-Server Redundancy

With three-server redundancy, if any two of the three license servers are up and running, a “quorum” of servers is established, and the system is functional and serves its total complement of licenses. Three-server redundancy is designed to provide hardware failover protection only and does not provide load-balancing. This is because with three-server redundancy, only one of the three servers is **"master"** and capable of issuing licenses.

The following is an example of a three-server redundant license file that GraphOn supplies after registering online. You must provide the hostnames of the three GO-Global Hosts as well as the hostids (Ethernet addresses, in most cases) for each. The port of the license server (e.g., 27000) must also be appended to each server line, if it is not already listed.

SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
DAEMON BLM port=5678
INCREMENT session blm 6.0 31-dec-2025 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 6.0 31-dec-2025 uncounted D1D222D031C4 \
HOSTID=ANY

The three-server license file needs to be copied to each of the three license servers. Lastly, you must point the GO-Global Host to the license server. This can be done in two different ways, either by copying the license to each GO-Global Host and editing it to use USE_SERVER (see example below), or by adding each server to the environment variable.

SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
USE_SERVER

With the second option, add each server to the environment variable, using commas to separate the servers. For example, LM_LICENSE_FILE = 27000@wilson,27000@piper,27000@caspian. Restart the **GO-Global Application Publishing Service** and the **GO-Global License Manager** on the "master" server first (wilson, in the example above), then on the secondary and tertiary servers.

We recommend running Flexera's **lmtools** application to check the status of the redundant license servers once all three servers are up and running. Launch lmtools.exe and select the **Server Status** tab. Click on **Perform Status Enquiry** and verify that your servers are "UP."

You can obtain lmtools from the Licensing directory (\GO-Global\Licensing) or from the Start menu. The lmtools application is included for diagnostic purposes. Any questions on its functionality should be directed to Flexera.

License-File List Redundancy

As an alternative to three-server redundancy, license-file list redundancy is available when there is limited system administration available to monitor license servers, when load-balancing is required for applications located far apart (e.g., Chicago and Tokyo), or when two or more license servers are required. With license-file redundancy, each one of a group of license servers serves a subset of the total licenses. As such, this method does not provide true redundancy in the way three-server redundancy does. Set the **LM_LICENSE_FILE** environment variable to a list of license files, where each license file points to one of the license servers. GO-Global attempts a license checkout from each server in the list, in order, until it succeeds or gets to the end of the list. The following example illustrates how license-file list redundancy works. If ten licenses are desired, you will need to request two Product Codes with a count of five for each.

The actual licenses will be generated from the Product Codes. Unlike with three-server redundancy, the server machines can be physically distant. The license servers on both servers need to be running.

The sample license files will look like:

License 1 for chicago:

```
SERVER chicago 00508BFE7FFE 27000
DAEMON blm port=5678
INCREMENT session blm 6.0 permanent 5 DF9C8F5ADF34 HOSTID=ANY \
        user_info="Joe User joeu@mycompany.com" ISSUER="GraphOn \
        Corporation" ISSUED=17-feb-2025 NOTICE="Copyright (C) \
        1996-2025 GraphOn Corporation. All Rights Reserved" ck=142 \
        SN=12865-AA
INCREMENT any_app blm 6.0 permanent 5 1DF84A360E8F HOSTID=ANY \
        user_info=" Joe User joeu@mycompany.com " ISSUER="GraphOn \
        Corporation" ISSUED=17-feb-2025 NOTICE="Copyright (C) \
        1996-2025 GraphOn Corporation. All Rights Reserved" ck=84 \
        SN=12865-AA
```

License 2 for tokyo:

```
SERVER tokyo 00508BF77F7E 27000
DAEMON blm port=5678
INCREMENT session blm 6.0 permanent 5 16BE40E1D98D HOSTID=ANY \
        user_info="Joe User joeu@mycompany.com" ISSUER="GraphOn \
        Corporation" ISSUED=17-feb-2025 NOTICE="Copyright (C) \
        1996-2025 GraphOn Corporation. All Rights Reserved" ck=142 \
        SN=12865-AA
INCREMENT any_app blm 6.0 permanent 5 6DB6F3E402DF HOSTID=ANY \
        user_info=" Joe User joeu@mycompany.com " ISSUER="GraphOn \
        Corporation" ISSUED=17-feb-2025 NOTICE="Copyright (C) \
        1996-2025 GraphOn Corporation. All Rights Reserved" ck=84 \
        SN=12865-AA
```

The administrator of the chicago server should set **LM_LICENSE_FILE** to: 27000@chicago;27000@tokyo where 27000 represents the port that the license servers in Chicago and Tokyo are running. This will direct the license engine to first attempt license checkouts from **chicago**. If unsuccessful, it will attempt to checkout from **tokyo**.

The administrator of the tokyo server should set **LM_LICENSE_FILE** to: 27000@tokyo;27000@chicago. This will direct the license engine to first attempt license checkouts from **tokyo**. If unsuccessful, it will attempt to checkout from **chicago**.

To change or set the LM_LICENSE_FILE variable

1. To view or change the current Environment Variables, right-click **My Computer** and select **Properties**.
2. Select the **Advanced** tab and click **Environment Variables** below.
3. Under **System variables**, select LM_LICENSE_FILE and click **Edit**.
4. Change the **Variable value** from **C:\Program Files\GraphOn\GO-Global\Licensing** to reflect the new redundant servers. Separate the license server names with a semicolon (;). GO-Global will attempt the first server in the list. If that fails for any reason, the second server is tried.
5. Restart the **GO-Global Application Publishing Service**.

As with three-server redundancy, we recommend running **lmtools** to verify the status of the redundant license servers once all servers are up and running.

Using On-Premises Licenses in Cloud Environments

GO-Global license files are bound to the MAC address of the computer on which the GO-Global License Manager service is running. In cloud environments, such as Amazon Web Services (AWS), the MAC address of a virtual computer can change. If the MAC address of a computer running the GO-Global License Manager service changes, the service will no longer be able to check out licenses and GO-Global sessions will fail to start. To prevent this, virtual computers running the GO-Global License Manager service must be configured to have a fixed MAC address. In AWS environments, this may be done by creating an **Elastic Network Interface** (ENI) with a fixed **Elastic IP address** (EIP) and a fixed MAC address, and attaching the ENI to the virtual computer (the EC2 Instance) that is running the GO-Global License Manager service.

To create an EIP and ENI in AWS and attach it to an EC2 Instance

1. Create an Elastic IP (EIP)

   From the EC2 console's navigation pane, go to NETWORK & SECURITY | Elastic IPs, and select **Allocate new address**.

   For more information, consult the AWS EIP documentation: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

2. Create an Elastic Network Interface (ENI)
   - 2.1 From the EC2 console's navigation pane, select **Network Interfaces**.
   - 2.2 Click **Create Network Interface**.
   - 2.3 Enter a **Description**, and choose a subnet from the appropriate Availability Zone.
   - 2.4 Leave the Private IP as auto assign.
   - 2.5 Choose the Security Groups that include your firewall rules.

3. Assign the Elastic IP (EIP) to the Elastic Network Interface (ENI)
   - 3.1 After creating the EIP and ENI, go to Network Interface | Actions | Manage IP Addresses.
   - 3.2 Assign the EIP you created in Step 1 to the ENI.

For more information, consult the AWS ENI documentation: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

In order to assign an ENI to an Instance, the subnet of the ENI must be in the same Availability Zone as the AWS Instance running the GO-Global License Manager service. You can use the subnet in the Availability Zone or create a custom subnet in the Availability Zone via Amazon Virtual Private Cloud (VPC).

4. Attach the ENI to the Instance running the GO-Global License Manager service
   4.1 From the EC Instances, select the Instance that is running the GO-Global License Manager service and go to Actions | Networking | Attach Network Interface.
   4.2 Choose the ENI created in Step 2. If it is not available, it may be attached to another AWS instance or it may have been created in a different Availability Zone than the Instance.

Emergency On-Premises Licenses

If a customer has a problem with a license server (e.g., if the hardware on which the license server is running fails), the customer can request an emergency, on-premises license in the Customer Portal.

To obtain an emergency, on-premises license file

1. Sign in to the Customer Portal.
2. Click **License Management**.
3. Click **Emergency License Request**.
4. Fill out the form. The Product Code can be obtained from the host's license file.
5. Click **Request Emergency License**.

Upon completion of these steps, the Customer Portal will validate the information entered and send a temporary, on-premises license file to the email address specified in the form.

To install an emergency, on-premises license

1. When you receive the emergency, on-premises license file, copy the file to the \Program Files\GraphOn\GO-Global\Licensing directory on the host.
2. Restart the **GO-Global License Manager Service**.
3. Restart the **GO-Global Application Publishing Service**.

Cloud Licenses

For subscription-based models, cloud licenses provide a simple, high-availability alternative to GO-Global's on-premises licenses. Cloud licenses are easier to manage than on-premises licenses because there are no license files. With cloud licenses, there is no need for Product Codes or Host IDs, no need to rehost licenses when GO-Global is installed on a different computer, and no need to obtain new license files when GO-Global is upgraded.

To activate GO-Global with a cloud license, the GO-Global Application Host or Application Host Manager must be able to connect directly to the GraphOn Cloud License Service, cloud.graphon.com (IP address: 13.52.136.225) on port 443. Similarly, the GO-Global Activation Wizard must be able to connect directly to the GraphOn Portal, portal.graphon.com (IP address: 52.8.15.135) on port 443.

If these conditions are not met, the Activation Wizard will notify you that GO-Global is unable to communicate with GraphOn's cloud license service. If you see this message, you must modify your firewall or proxy server to allow access to the above addresses and ports.

License Creation

There are two ways to create a cloud license:

- By starting a new 30-day trial in the Activation Wizard, which GraphOn will then convert to a cloud license when an order is placed
- By placing an order for a cloud license, without running the 30-day trial

Most cloud licenses are created by starting a new trial in the Activation Wizard and are then converted to production cloud licenses when a customer places an order. The trial provides 30-day support for the full functionality of GO-Global. The process of converting a cloud trial license to a production cloud license does not require the customer to make any changes on the hosts using the license. This enables customers to configure licensing during the trial period and continue to use the configuration, without modification, after the order is completed.

When a customer places an order for a new cloud license after starting a trial, the customer provides GraphOn with the License Master ID ("LIC-xxxxx" identifier) of the cloud trial license and identifies the license's Site Administrators. GraphOn verifies that the user who started the trial is one of the license's Site Administrators and then processes the order. Upon completion of the order, GraphOn converts the license from a cloud trial license to a cloud production license. The expiration dates and seat limits of the license are updated, and the hosts using the license see the changes immediately, without any changes on the hosts. GraphOn then notifies the contacts on the order that the order has been completed.

Alternatively, if a customer places an order for a cloud license without having started a trial, GraphOn creates a new license in its license database and emails the new license's License Master ID and Product Code to the contacts listed on the order.

The only time the Product Code of a cloud license is needed, is when a customer needs to request an emergency, on-premises license to work around an issue.

Activating GO-Global

To activate GO-Global with a cloud license, one of the Site Administrators listed on a license must run the Activation Wizard on a host, sign in to their GraphOn account, and select the license they want the host to use.

To switch from one or more on-premises licenses to a cloud license

Use the following instructions if the on-premises licenses are in use on a single Application Host or Application Host Manager (e.g., Relay Load Balancer or Farm Manager).

1. Remove all on-premises license files from the \Program Files\GraphOn\GO-Global\Licensing directory on the host.
2. Stop the **GO-Global License Manager Service**.
3. Restart the **Application Publishing Service**.
4. Run the **Activation Wizard** and select the new cloud subscription license.

If the on-premises licenses are in use on a central license server that is used by more than one GO-Global Host, use the following instructions to switch from one or more on-premises licenses to a cloud license.

1. If the GO-Global Hosts are not currently using an Application Host Manager (Relay Load Balancer or Farm Manager), create a Farm Manager that will act as the central license server for the hosts and connect the Applications Hosts to the new Farm Manager.
2. Ensure that the **ManageLicensesFrom** property in HostProperties.xml is set to **Relay** on all Application Hosts and the Application Host Manager.
3. Remove any on-premises license files in the \Program Files\GraphOn\GO-Global\Licensing directory of the Application Host Manager.
4. Stop the **GO-Global License Manager Service** on the Application Host Manager.
5. Restart the **Application Publishing Service** on the Application Host Manager.
6. Run the Activation Wizard on the Application Host Manager and select the new cloud subscription license.
7. If high availability is required (e.g., if three redundant license servers are currently in use), configure a Backup License Manager. Run the Activation Wizard on the Backup License Manager and select the new cloud subscription license.

8. If any Application Host or Application Host Manager is not running GO-Global version 6.2.1 or later, upgrade it to GO-Global 6.2.1 or later.

To switch from a cloud license to an on-premises license

1. Copy one or more on-premises license files to the \Program Files\GraphOn\GO-Global\Licensing directory on the host.
2. Start the **GO-Global License Manager Service**.
3. Restart the **Application Publishing Service**.

Thereafter, if you would like to switch back to using the host's original cloud license, simply remove the on-premises license file(s) from the Licensing directory and restart the Application Publishing Service.

Adding and Removing Seats

Customers can add seats at any time during the term by placing an order for additional seats. GraphOn will prorate based on the subscription expiration date. Customers can reduce seats during the subscription term, up to ten days before the term expires. Increases and decreases to a cloud license's number of seats are immediately enforced on all hosts using the license as soon as the seat number is modified in GraphOn's license database. No changes are required on the GO-Global Hosts that are using the license.

License Upgrades and Rehosts

Cloud subscription licenses support GO-Global v6.1 and later. Cloud licenses are not tied to specific computers or a computer's MAC address. As such, they do not need to be upgraded or rehosted. In addition, they continue to function without issue if the MAC address of a GO-Global Host changes.

License Management

Customers can manage their cloud licenses on the Cloud License Administration page of the Customer Portal. The Cloud License Administration page allows users to perform the following operations on licenses on which they are Site Administrators:

- View detailed information about each license, including the hosts using the license
- Edit a license's description
- Deactivate GO-Global on any of the license's hosts

To manage cloud licenses

1. Sign in to the Customer Portal.
2. Click **License Management**.
3. Click **Cloud License Administration**.

Cloud License Activation via PowerShell

GO-Global can be activated using PowerShell and an active cloud license.

Identify the cloud license you wish to use (e.g., from the portal's Cloud License Administration page.) Run the **Invoke-GGActivate** script on the computer that will manage GO-Global licenses. For example, in a load-balanced environment, run the command on the Application Host Manager (e.g., Farm Manager or Relay Load Balancer). Alternatively, if the computer is an Independent Host, run the command on the Independent Host.

Open an elevated PowerShell prompt on the GO-Global Host or Farm Manager and run the following command:

```
PS> Import-Module "C:\Program Files\GraphOn\GO-
Global\PowershellModules\GraphOn.GO-Global.SessionManager.PowerShell"
```

If the Import-Module command fails due to an issue with the PowerShell execution policy, you may need to adjust the execution policy to allow the module to be imported. Run the command **Set-ExecutionPolicy RemoteSigned** to configure PowerShell to permit the execution of scripts that are either created locally or downloaded from the internet but signed by a trusted publisher.

The following command will display version information:

```
PS> Get-GGModuleInfo
```

After loading the module, run one of the following commands for more information:

```
PS> Get-Help Invoke-GGActivate
PS> Get-Help Invoke-GGActivate -Detailed
PS> Get-Help Invoke-GGActivate -Full
```

To run the activation script

From the PowerShell Console, run the following command with these required parameters:

```
PS> Invoke-GGActivate -username "my-GGPortal-email@example.com"
-password "mypassword" -licenseMaster "LIC-000000" -macAddress
"001122334455"
-accountID "0123456"
```

If a parameter is missing or an additional parameter is required, the activation script will provide a prompt.

The following parameters are supported:

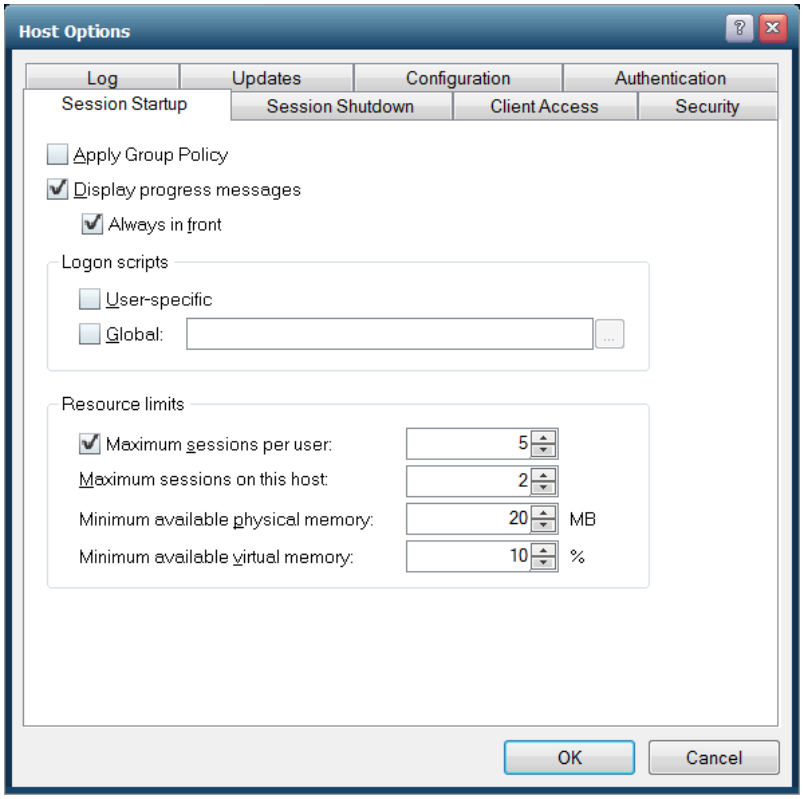
Parameter	Description
-username	The username of a Site Administrator on the license which will be used to activate GO-Global
-password	The portal account password
-licenseMaster	The license master. (For example, LIC-123456)
-computerName	The name of the computer (e.g., the **displayname** in the \ProgramData\GraphOn\GO-Global\config.xml file)
-macAddress	The computer's MAC address. (This is stored in the **hardwareid** in\ProgramData\GraphOn\GO-Global\config.xml file.) For example, 00005E005300
-computerUUID	The Universally Unique Identifier is found in config.xml. (For example, 4f017fcd65de4f959d704fd672e36b5db61dbc5dcb33d9c1d3342c8fb3336210)
-operatingSystem	The operating system found in config.xml. (For example, Windows 10 Pro N)
-hostVersion	The version of the host. (For example, 6.3)
-productFamily	The product that is to be activated. (For example, GO-Global – Windows)
-accountID	The account ID in the portal. (Users can have multiple accounts.) (For example, 1234567) Contact GraphOn Support to determine the ID of your account.
-configPath	The path to config.xml if it cannot be found in the default location. (For example, C:\ProgramData\GraphOn\GO-Global\config.xml)
-Verbose	Optional parameter for displaying more information.

Multiple Host Environments

GO-Global can be activated on multiple hosts using the same cloud license, but this is not recommended. When more than one host uses a license, GO-Global attempts to distribute the license's seats proportionally across the hosts based on values set for the **Maximum sessions on this host** option on each host. For example, if all the hosts using a license have the same value for the **Maximum sessions on this host** option, GO-Global will attempt to distribute seat reservations equally across the hosts. Then, if one host needs more seats than it has reserved, the **Cloud License Service** will attempt to reclaim seat reservations for other hosts to provide more seats for the requesting host. This is a time-consuming process that can delay users' sessions from starting. Also, if a host that has seats reserved is not running, GO-Global cannot reclaim the seats. And if the host that needs the seats is temporarily unable to communicate with the Cloud License Service, it will not be able to increase its seat reservation. For these and other reasons, administrators should avoid activating GO-Global on multiple hosts using the same license.

In environments with multiple hosts, GraphOn recommends that customers configure the hosts to use an Application Host Manager (i.e., a Relay Load Balancer or Farm Manager) and run the Activation Wizard on the Application Host Manager, not the Application Hosts. This ensures that all the seats of a cloud license will be available for use by all hosts, even when the Application Host Manager is unable to communicate with the **Cloud License Service**. It also prevents unnecessary delays from occurring while the Cloud License Service moves seat reservations back and forth between the hosts using the license. For more information about load balancing, see Chapter VII.

In some cases, administrators may wish to activate GO-Global on a test host using the same license that is used on a production host or farm. In these cases, administrators must take care to ensure that the test host does not reserve an excessive number of the license's seats. This can be managed by adjusting the **Maximum sessions on this host** option on the **Session Startup** tab of the **Host Options** dialog. For example, a host with the **Maximum sessions on this host** set to 2 would reserve, at most, 2 seats.



Releasing Reserved Seats

When the Application Publishing Service shuts down, it releases the license seats that the host has reserved. If, however, the Application Publishing Service or the computer on which it is running crashes, the host's seats will not be released. In these cases, the host's seats will become available as soon as the Application Publishing Service is restarted. If, however, the Application Publishing Service cannot be restarted (e.g., if the host computer will no longer start due to a hardware failure or the virtual machine on which GO-Global is running has been reset to a snapshot) administrators can release the seats that are reserved for the host by detaching the host from the license via the Customer Portal.

To detach a host from a license and release its reserved seats

1. Sign in to the **GraphOn Customer Portal**.
2. Click **License Management.**
3. Click **Cloud License Administration**.
4. Click the license the host is using.
5. Under **Hosts Using This License**, select the host(s) you want to detach from the license.

Each time the Activation Wizard is run on a GO-Global Host, a record for the host is created in the Cloud License Service's database. These records are displayed under **Hosts Using This License**. A given host computer may be listed multiple times. Look for host records that have the correct hostname, that have a state of OFFLINE, and that have seats reserved. Select these host records.

6. Click **Deactivate Host(s).** The following message will be displayed:
If you deactivate GO-Global, users will be unable to start sessions on this host until GO-Global is reactivated by running the GO-Global Activation Wizard on the host. Are you sure you want to deactivate GO-Global on this host?

In certain cases, this message can be misleading. If, for example, you have run the Activation Wizard on the host computer and configured GO-Global to use a different license, clicking **Deactivate Host(s**) will not deactivate GO-Global and prevent it from using the new license. It will simply detach the selected host records from the old license and release any seats reserved for those host records. Similarly, if you reactivate GO-Global on a host using the same license, there will be multiple host records for the host in the list of **Hosts Using This License**. In this case, be sure that the Application Publishing Service is running on the host and then only select host records have a state of OFFLINE.

7. Click **Yes** to detach the selected host record(s) from the license and release any seats reserved for them.

High Availability

GraphOn's cloud licensing system is designed from the ground up to provide high availability. The reliability of cloud licenses begins with the **GraphOn Cloud License Service**. GraphOn Cloud License Service is a web service that is hosted on the internet in a high availability environment. It has multiple redundancies and no single point of failure.

Of course, having multiple redundancies in the Cloud License Service provides little benefit if there is a network outage that prevents hosts from communicating with the service. For this reason, hosts can continue to use cloud licenses for up to 72 hours when they are unable to communicate with the Cloud License Service.

To provide this level of reliability, hosts do not check out and check in license seats from the Cloud License Service when users, respectively, start and stop sessions. Doing so would be unreliable and would place heavy loads on the Cloud License Service. Instead, hosts reserve seats from the Cloud License Service and then limit seat usage to the number of seats they have reserved.

When Hosts are Connected to the Cloud License Service

When the Application Publishing Service starts up, it connects to the Cloud License Service and negotiates a seat reservation with the service. If there is only one host configured to use the cloud license, the Cloud License Service sets the host's seat reservation to the cloud license's seat limit. Alternatively, if multiple hosts are configured to use a license, the Cloud License Service distributes the license's seats among the hosts, increasing and decreasing the seat reservations of the hosts as the load shifts between the hosts.

When a user signs in to a host, the host compares the number of seats in use on the host to the number of seats it has reserved. If the number of seats in use is less than the number of seats reserved, the host increments its count of the seats that are in use and allows the user's session to start. In this case, no communication with the Cloud License Service is necessary. Alternatively, if the number of seats already in use on the host is equal to the number of seats the host has reserved, the host sends a request to the Cloud License Service to increase the host's seat reservation.

When the Cloud License Service receives a request to increase a seat reservation, it checks to see if the sum of all seats reserved by the hosts using the license is less than the cloud license's seat limit. If it is, the Cloud License Service increases the host's seat reservation and notifies the host of the increase. Alternatively, if all of a cloud license's seats are already reserved, and if there are other hosts using the cloud license that are connected to the Cloud License Service, the Cloud License Service attempts to renegotiate the seat reservations with the other hosts that are using the license to free up seats for the host that needs them.

During a seat reservation renegotiation, if there are seats available on the other hosts using the license, the hosts release some number of them, up to all that are not in use, back to the Cloud License Service. The Cloud License Service then increases the requesting host's seat reservation and notifies the host of the increase. Alternatively, if there are no seats available on any of the hosts using the cloud license (if all of the cloud license's seats are in use), the Cloud License Service notifies the host that there are no seats available. In this case, the host notifies the user that the maximum number of seats allowed by the license has been reached and prevents the user's session from starting.

When hosts are connected to the Cloud License Service, they periodically send license audit data to the Cloud License Service. This audit data includes records of all license-related events that occur on the host (e.g., all seat check-outs and check-ins, and all seat reservation changes). The Cloud License Service stores this data in its database and uses it to determine the maximum concurrent seat usage during each billing period of a monthly subscription.

When Hosts are Disconnected from the Cloud License Service

When hosts are disconnected from the Cloud License Service, they are limited to the number of seats they had reserved when the connection to the Cloud License Service was lost. As long as the number seats in use on a host remains below the number of seats it has reserved, the host functions the same way it does when it is connected to the Cloud License Service. When a user signs in to a host, the host increments its count of the seats in use and allows the user's session to start.

When the host is disconnected from the Cloud License Service however, and a user signs in to a host when all the seats the host has reserved are in use, the host is unable to request an increase to its seat reservation. Therefore, it notifies the user that the maximum number of seats allowed by the license has been reached and prevents the user's session from starting.

When a host is disconnected from the Cloud License Service, a warning is displayed to administrators whenever they start the Admin Console or sign in to the host. The warning states that the host is unable to communicate with the Cloud License Service and that it will stop functioning if connectivity is not restored within **x** hours, where **x** is 72 hours minus the number of hours the host has been disconnected from the Cloud License Service.

When a host remains disconnected from the Cloud License Service for over 72 hours, it disconnects all users who are connected to the host. What then happens to the users' sessions depends on what **Disconnected sessions terminate** is set to on the host. If it is set to **Immediately**, the host terminates user sessions immediately. If it is set to **Never**, user sessions remain running, but users are unable to reconnect to them until the host reconnects to the Cloud License Service. If it is set to **After** x **minutes**, users' sessions remain running on the host for up to x minutes, but if the host fails to reconnect to the Cloud License Service within the specified number of minutes, the host terminates the users' sessions.

Seat Reservation Backup Storage Locations

Hosts store their seat reservations in the following locations:

- In the memory of the Application Publishing Service
- In the System Extensions Driver
- In Backup License Managers (if configured)

When the Application Publishing Service starts and is unable to connect to the Cloud License Service, it attempts to determine what the host's seat reservation is, first, from the System Extensions Driver and, second, from its Backup License Managers (if there are any). If the host is unable to determine its seat reservation from any of these sources (e.g., if the host computer has been restarted and there are no Backup License Managers available), the host sets the seat reservation to zero. In this case, users will not be able to start sessions on the host until the host connects to the Cloud License Service.

Similarly, hosts store their license audit data in the following locations:

- In the memory of the Application Publishing Service
- In the System Extensions Driver
- In Backup License Managers (if configured)
- On the hard drive of the host

When a host is disconnected from the Cloud License Service, it continues to record license audit data in these locations. Then, when the host reconnects to the Cloud License Service, it checks each of the above sources for the license audit data (in the order listed) and sends the accumulated audit data to the Cloud License Service from the first source that has it.

Backup License Managers

It is expected that GO-Global Application Hosts and Application Host Managers will, at times, be unable to communicate with GraphOn's Cloud License Service. This can occur, for example, if a network problem prevents a host from connecting to the internet. Since connectivity to the Cloud License Service cannot be guaranteed, GO-Global is designed to continue working and allowing users to start sessions for up to 72 hours without being able to communicate with the Cloud License Service. It does this via Backup License Managers. Any Application Host or Application Host Manager that is using a cloud license should be configured to use a Backup License Manager.

In other words, you should not expect or require that Application Hosts and Application Host Managers using cloud licenses will always be able to connect to the Cloud License Service. Instead, you should ensure that Application Hosts and Application Host Managers using cloud licenses are configured to use a Backup License Manager.

Backup License Managers provide the following functions:

- They allow a host to continue using the seats it has reserved when the host is restarted while it is unable to communicate with the Cloud License Service.
- They release the seats reserved for a connected host when the host crashes, so the seats are immediately available to other hosts that are using the license.
- They provide a secure location for storing license audit data so the data is not lost or corrupted if a host is restarted.

Any GO-Global Host, regardless of its role, can be used as a Backup License Manager. To provide the second function listed above, however, GO-Global must be activated (via the Activation Wizard) on a Backup License Manager using the same cloud license as the hosts that it serves.

Hosts can be configured to use multiple Backup License Managers. At least one is required to provide high availability. Adding additional Backup License Managers increases the level of high availability.

To configure a Backup License Manager

1. On the computer that will serve as the Backup License Manager, run the Activation Wizard and select the cloud license that is used by the hosts that will connect to it.
2. On each GO-Global Host that will use the Backup License Manager, run the Admin Console, and click **Tools** | **Host Options**.
3. Click the **Configuration** tab.
4. In the **Backup License Manager(s)** field, type the address of the Backup License Manager computer. Optionally, to provide redundancy, enter the addresses of two or more Backup License Managers, with the addresses separated by semicolons. For example, server1_address;server2_address;server3_address.
5. If a Backup License Manger is configured on the Host Options dialog's **Security** tab to use a different port than the host, specify the port after the address, separated by a comma. For example, server1,443: server2,443;server3.
6. Click **OK**.
7. Restart the **GO-Global Application Publishing Service**.

GraphOn recommends that failover Application Host Managers (e.g., failover Relay Load Balancers) be configured as Backup License Managers for their primary Application Host Manager, and vice versa. This ensures, for example, that seats reserved by a primary Relay Load Balancer are immediately available to the failover Relay Load Balancer when the primary Relay Load Balancer crashes.

Backup License Managers can only be used when the host is configured using a cloud license. The control is disabled when the host is configured using an on-premises license.

When a Host without a Backup License Manager Fails

When a host is not configured to use a Backup License Manager and it is restarted when it is unable to communicate with the Cloud License Service, the host's reservation of license seats will be lost, and users will not be able to start sessions. Therefore, if GO-Global is not configured to use a Backup License Manager and a message is displayed indicating that GO-Global is unable to communicate with the Cloud License Service, *do not* restart the computer or the Application Publishing Service until connectivity to the Cloud License Service is restored. If this message is displayed, no action needs to be taken, regardless of whether a Backup License Manager is used.

Another issue can arise when no Backup License Manager is used and the same cloud license is used by multiple Applications Hosts or Application Host Managers. The issue is that seats reserved by a host are not released and are not available to other hosts if any of the following occur:

- The Application Publishing Service crashes or is terminated
- The host computer crashes or is powered off
- The virtual machine on which the GO-Global Host is running is powered off or reset to a snapshot

For example, if a Relay Load Balancer has no Backup License Manager, and the VM on which it is running is powered off or reset to a snapshot, any seats that were reserved by the Relay Load Balancer will not be available for use on other hosts. To release the seats, administrators must restart the computer and then either stop the Application Publishing Service via Windows Services or shut down the computer.

GO-Global releases the seats reserved for a host when the Application Publishing Service is stopped via Services or the computer is shut down normally (i.e., is not powered off). Therefore, administrators who wish to take a host offline should either stop the Application Publishing Service via Services or shut down the computer.

In cases where a GO-Global Host cannot be restarted (e.g., when a hardware failure has occurred or the virtual machine has been reset to a snapshot that does not have GO-Global installed), Site Administrators of the cloud license can release the seats by deactivating the GO-Global Host on the GraphOn Customer Portal. Deactivating a host detaches the host from the license and releases any seats that are reserved for the host.

To deactivate a host and release its seats

1. Sign in to the GraphOn Customer Portal using an account that is a Site Administrator of the host's license.
2. Click **License Management**.
3. Click **Cloud License Management**.
4. Click the license the host is using.
5. Click the checkbox next to the host that has the seats reserved.
6. Click **Deactivate Host(s)**.

When a GO-Global Host is deactivated, sessions will no longer start on the host. To re-activate the host, re-run the Activation Wizard on the host.

Emergency On-Premises Licenses

If a customer is unable to restore connectivity to the cloud license service within 72 hours or, for any other reason, is unable to resolve a problem with a host that is using a cloud license, the customer can request an emergency, on-premises license for the host in the Customer Portal. Customers *should not* request an emergency, on-premises license when connectivity to the cloud license service is lost, unless they anticipate that connectivity will not be restored within 72 hours.

To request an emergency, on-premises license, customers must provide the cloud license's Product Code. This is the only situation in which a customer using a cloud license will require the license's Product Code.

To obtain an emergency, on-premises license

1. Copy the Product Code of the host's cloud license to the clipboard:
   a. Run the Admin Console.
   b. Click **Licenses.**
   c. Click **Copy product code**.
2. Sign in to the Customer Portal.
3. Click **License Management**.
4. Click **Emergency License Request**.
5. Fill out the form, pasting the Product Code copied in step 1 into the **Product Code** field.
6. Click **Request Emergency License**.

Upon completion of these steps, the Customer Portal will validate the information entered and send a temporary, on-premises license file to the email address specified in the form.

To install an emergency, on-premises license

1. When you receive the emergency, on-premises license file, copy the file to the \Program Files\GraphOn\GO-Global\Licensing directory on the host.
2. Start the **GO-Global License Manager Service**.
3. Restart the **Application Publishing Service**.

The **Application Publishing Service** *must be* restarted for the emergency license to be activated.

Whenever there is an on-premises license file in the Licensing directory on the host, a host that is otherwise configured to use a cloud license will use the on-premises license instead of the cloud license. To revert back to using the cloud license, simply remove the on-premises license file from the Licensing directory and restart the Application Publishing Service.

CHAPTER III

Configuring the Host

3

Installing the GO-Global Host

GO-Global is delivered as a self-extracting executable and can be installed by double-clicking **gg-host.exe**. When running the host setup program, you must be logged in to an account that is a member of the computer's Administrator's group.

By default, the GO-Global Host setup installs all the core Host components, Web components (including all the files necessary to configure the host for browser logons) and Licensing components. You can customize the installation by clicking the **Customize** button and unchecking the components you do not wish to install. Otherwise, click the **Install** button.

During the installation, the installer displays a screen that explains how to activate GO-Global using an on-premises license. If you would like to use an on-premises license, install the on-premises license at this time. Alternatively, if you would like to activate GO-Global using a cloud license, run the Activation Wizard.

Activating GO-Global with an On-Premises License File

If you would like to use an on-premises license on the host, copy your on-premises license file(s) to the Licensing directory (e.g., C:\Program Files\GraphOn\GO-Global\Licensing). If you would like to use an on-premises license on a different host, see Multiple Host Environments.

If you opt to copy your license file(s) later, you must restart the GO-Global License Manager, then the GO-Global Application Publishing Service after copying the file(s).

To restart the GO-Global License Manager

1. Click Control Panel | Administrative Tools | Services.
2. Select **GO-Global License Manager** from the list of services.
3. Right-click and select **Restart**.

To restart the GO-Global Application Publishing Service

1. Click Control Panel | Administrative Tools | Services.
2. Select **GO-Global Application Publishing Service** from the list of services.
3. Right-click and select **Restart**.

Minimum permissions for the license file(s) (in C:\Program Files\GraphOn\GO-Global\Licensing*.lic) are:
Administrators: Full Control; **Users**: Read & Execute; **SYSTEM**: Full Control

If the following error message appears in a Log file, it is possible that the permissions are incorrect for the license file:

FlexLM code #-1; FlexLM text: Cannot find license file. The license files (or license server system network addresses) attempted are listed below. Use LM_LICENSE_FILE to use a different license file, or contact your software provider for a license file.)

When combining two GO-Global licenses or when using two separate licenses on the same GO-Global Host, the hostnames in the license files are case-sensitive and must be identical.

Activating GO-Global with a Cloud License

To activate GO-Global using a cloud license, run the Activation Wizard.

To run the Activation Wizard

1. From the Start menu, click GraphOn GO-Global | Activation Wizard.
2. When the Activation Wizard opens, follow the prompts. Sign in using your GraphOn account. Create an account if you do not have one. Then click the **Sign in** button.

GO-Global Application Hosts, Application Host Managers and the GO-Global Activation Wizard cannot traverse proxy servers. To activate GO-Global with a cloud license, the Application Host or Application Host Manager must be able to connect directly to the **GraphOn Cloud License Service**, cloud.graphon.com (IP address: 13.52.136.225) on port 443. Similarly, the GO-Global Activation Wizard must be able to connect directly to the GraphOn Portal, portal.graphon.com (IP address: 52.8.15.135) on port 443.

If these conditions are not met, the Activation Wizard will notify you that GO-Global is unable to communicate with the cloud license service. You must modify your firewall or proxy server to allow access to the above addresses and ports. Alternatively, you can request an on-premises license as described below.

3. If applicable, select a GraphOn customer account.
4. Select the license you would like the computer to use.
5. Click **Accept** to accept the GO-Global License Agreement.
6. Click **Activate** to activate GO-Global on the computer.

Completing the Installation

After activating GO-Global, **restart** the computer.

When the computer restarts, select a web browser to open GO-Global's ***Quick Start***. This guide provides basic instructions for publishing applications through the Admin Console, and sharing links to the applications. The ***Quick Start*** is also accessible via the Start menu.

If you would like to set startup preferences for the GO-Global Host, choose GO-Global Application Publishing Service from the list, and click the **Startup** button. Select the options you want to apply to the GO-Global Host.

Upgrading to GO-Global 6.3 from Earlier Versions

Customers upgrading to GO-Global 6.3 from earlier versions must obtain a version 6.3 license before they can upgrade. The version 6.3 host installer *will not upgrade* a computer that does not have a version 6.3 GO-Global license.

GO-Global cloud-based licenses will automatically be upgraded when a new version of GO-Global is released. If the host being upgraded is using an on-premises license, submit a License Change Request in the Customer Portal to obtain a new license file.

To obtain a version 6.3 on-premises license file

1. Sign in to the **Customer Portal**.
2. Click **License Management**.
3. Click **License Change Request**.
4. Complete the form.
5. Click **Submit Request**.

After submitting the License Change Request form, a GO-Global license file will be sent via email.

To install the new license file

1. If GO-Global 6.0 is currently installed, place the new license file in the \Program Files\GraphOn\GO-Global\Licensing directory. Alternatively, if GO-Global version 5.0 is currently installed, place the license file in the \Program Files\GraphOn\GO-Global\Programs directory.
2. Remove older version license files.
3. Restart the **GO-Global License Manager Service**.

Restarting the License Manager will not affect sessions running on the GO-Global Host.

Run the Host Installer

After upgrading the host's license, run the GO-Global Host installer (gg-host.exe) and reboot the computer when prompted.

The host installer will resume automatically after restarting. As part of the installation process, existing versions of GO-Global are removed, but Registry settings and files are saved. These files can be found in the %PROGRAMFILES%\GraphOn\GO-Global.backup folder and in the Registry at HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global.backup. The installer also moves the new license file(s) from the **Programs** directory to the **Licensing** directory.

When upgrading from version 5 to version 6.3, you will be prompted to restart the computer two times.

Customers must have an active Support contract to upgrade licenses. If your Support contract has expired, contact your GO-Global reseller or sales@graphon.com to renew it.

Activating GO-Global using an On-Premises Trial license

For computers without direct access to the internet, or if a cloud trial license cannot be established, GraphOn will generate an on-premises trial license, which will be sent via email.

To activate GO-Global using an on-premises license

1. Determine the computer's **Host Name** and **Host ID** (Physical Address).
    a. Open the Command Prompt window by clicking Start | (All) Programs | Accessories | Command Prompt.
    b. Type **ipconfig /all** and press the **Enter** key.
    c. Locate the computer's **Host Name** and **Physical Address**.
    d. Email sales@graphon.com with the computer's Host Name, Host ID (Physical Address), and number of seats.

2. When you receive the license file from GraphOn:
    a. Copy the .lic file into c:\Program Files\GraphOn\GO-Global\Licensing directory.
    b. Start the **GO-Global License Manager Service**.
    c. Restart the **GO-Global Application Publishing Service**.

Installing a Perpetual, On-Premises License

Administrators can install a perpetual, on-premises license on systems currently using a cloud or on-premises trial license. After the order for a perpetual, on-premises license is placed, GraphOn processes the order and creates a new license. License information is emailed to the contacts identified on the order request. The administrator must activate the license via the Customer Portal by supplying the Product Code, email address, Host Name, and Host ID. **The new license (.lic) file is emailed as an attachment**. The License ID is used to format the name of the license file. (For example: **8d73e4k.lic** where 8d73e4k is the License ID). The license file attachment must be installed on the designated license server.

To install a perpetual, on premises license

1. Remove any trial or voided license (.lic) files from the **Licensing** directory on the GO-Global license server (e.g., C:\Program Files\GraphOn\GO-Global\Licensing\)
2. Move the new .lic file to the **Licensing** directory on the GO-Global license server.
3. Optionally, if you have a conflicting license manager, add a port number after the hostid on the "SERVER" line. For example: SERVER 2016ITL1 000C2931282E 27009
   (This will direct the license manager to use port 27009.)
   Please note that any other modifications could corrupt and disable the license.

4. Open **Services** on the GO-Global license server and restart the **GO-Global License Manager**.
5. On all the GO-Global Hosts using the license server:
   a. Ensure there are no GO-Global sessions running on the host.
   b. Open **Services** and restart the **GO-Global Application Publishing Service**. (This will terminate all user sessions.)

Using GO-Global's Integrated Web Server

The Application Publishing Service includes an integrated web server that users can use to access GO-Global Hosts from a browser. This eliminates the need to install a separate web server on the GO-Global Host or on another computer. This simplifies browser-based access to hosts and greatly simplifies internet deployments.

To access a GO-Global Host using GO-Global's integrated web server, users simply browse to the address and port of the GO-Global Host. For example, if the GO-Global Host is configured to use its default port, 491, users will access the GO-Global Host by browsing to:
http://[host_address]:491/

Alternatively, if the GO-Global Host is configured on the Security tab of the Admin Console's Host Options dialog to use port 80 (the default HTTP port), the port need not be specified after the web server address but must be specified for the GO-Global Web App. In this case, users will access the GO-Global Host by browsing to:
http://[host_address]/?port=80

Similarly, if TLS security is enabled on the Security tab of the Host Options dialog and the Port is set to 443 (the default HTTPS port), the port need not be specified after the web server address but must be specified for the GO-Global Web App. In this case, users will access the host by browsing to:
https://[host_address]/?port=443

Installing the Web Files on a System other than the Host

You can install the GO-Global web files on a system other than the GO-Global Host.

To install the Web files on a system other than the GO-Global Host

1. Run the Host installer on the desired web server, selecting to install the web files.
2. Edit the logon.html page on the web server and add the following statements, inserting the address of the GO-Global Host in place of hostname.

```
if (host.length == 0)
{
        host="hostname";}
```

Hosting Web Files from a Directory other than the Default Directory using IIS

You can host the GO-Global web files from a directory other than the default goglobal directory, using Microsoft IIS Web Server.

To host web files from a directory other than the default directory

1. Create a directory in c:\inetpub\wwwroot\ on the web server and call it what you would like your users to see. For example, create a folder: C:\inetpub\wwwroot\Web.
2. Copy the contents of c:\Program files\GraphOn\GO-Global\Web directory from a GO-Global Host to the new directory.
3. Open IIS Manager and go to Sites | Default Web Site. Right-click **Default Web Sites** and click **Add Virtual Directory**.
4. Provide the same **Alias** as the directory created in Step 1, and point the **Physical Path** to the directory where you copied the files in Step 2. For example, c:\inetpub\wwwroot\Web.
5. Click the new virtual directory; then double-click on **MIME Types**.
6. Click **Add**. In the File name extension box, type .mem. In the MIME Type box, type application/octet-stream. Then click **OK**.
7. Add **logon.html** as the **Default Document** for this **Virtual Directory**. (For more information about configuring the default document in IIS, see https://support.microsoft.com/en-us/help/320051/how-to-configure-the-default-document-in-internet-information-services)
8. To verify that the IIS settings are correct, open a browser and type the URL to connect to your GO-Global host, for example: **http://hostname/web/logon.html** or **https://hostname/web/**. (*hostname* is name of your GO-Global Host. *web* is the name of the virtual directory you created in ISS.)

Running GO-Global through Apache HTTP Server

When the Apache HTTP Server 2.4 web service is installed on the GO-Global Host, users can connect from a client machine using a web browser.

If IIS is installed, the **World Wide Web Publishing** service must be stopped and disabled before downloading Apache. From **Services**, right-click **World Wide Web Publishing** service and select **Properties**. From the **Properties** dialog, select **Disabled** from the **Startup type** drop-down menu and click the **Stop** button. Click **OK**.

1. Go to http://www.apachelounge.com/download/ and download the latest version. The version tested by GraphOn was **httpd-2.4.29-Win64-VC15.zip**.
2. Download and install **C++ Redistributable Visual Studio 2017**. The version tested by GraphOn can be downloaded from the following link: https://aka.ms/vs/15/release/VC_redist.x64.exe
3. Extract **httpd-2.4.29-Win64-VC15.zip** onto the GO-Global Host in C:\Apache24 directory.
4. Add **logon.html** to the **DirectoryIndex** directive in the **httpd.conf** file. For example, open **C:\Apache24\conf\httpd.conf** in a text editor and edit the **DirectoryIndex** line. Save the file. The DirectoryIndex line should look like this:

   ```
   <IfModule dir_module>
   DirectoryIndex logon.html index.html
   </IfModule>
   ```

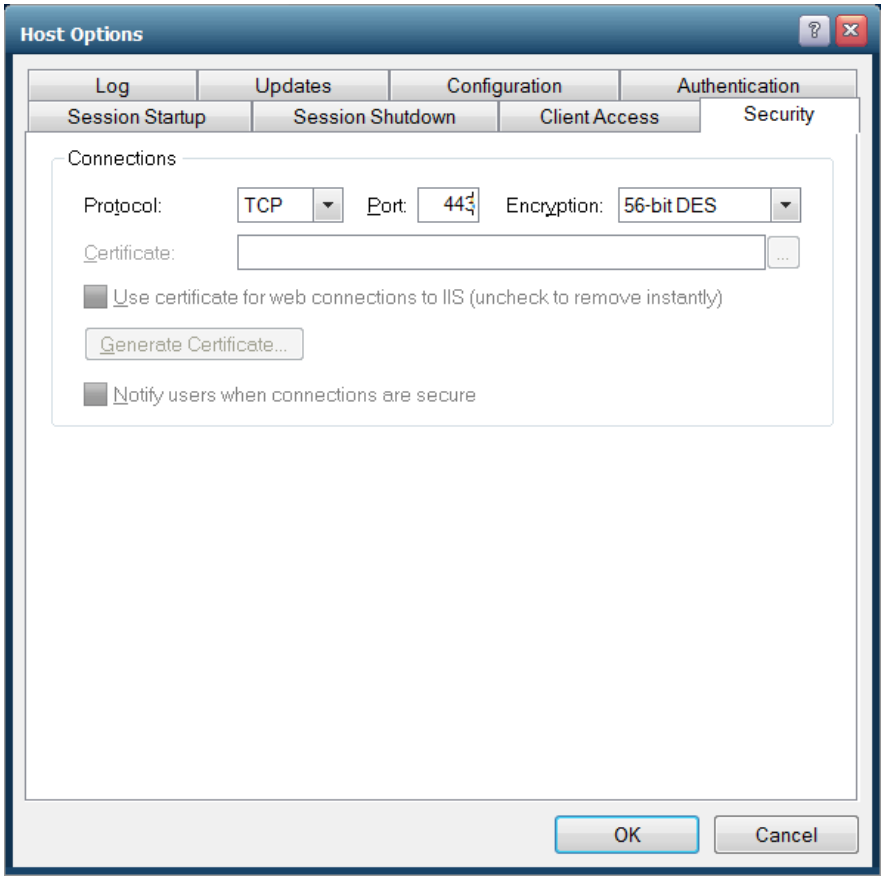
5. Click Start | All Programs | Accessories | Command Prompt. Right-click **Command Prompt** and **Run as administrator**.
6. In the **Command Prompt** window, type the following:

   ```
   cd C:\Apache24\bin

   httpd -k install

   httpd -k start
   ```

   You may need to open port 80 in the firewall if it is not already open. If TLS is running, verify that port 443 is open.
7. Open c:\Apache24\bin and run **ApacheMonitor.exe**. From the system tray, open the Apache Monitor and verify that the service has started.
8. Open c:\Apache24\htdocs and create a directory called **goglobal**.
9. Copy the contents of c:\Program files\GraphOn\GO-Global\Web into c:\Apache24\htdocs\goglobal directory.
10. Open a browser on the GO-Global Host and go to **http://localhost/goglobal/logon.html** or **http://localhost/goglobal/** to start a session.

Enabling Internal and External Users to Open Secure Connections to a Host

1. Install the Web component on a different computer than the Host. (The web server and the GO-Global Host cannot listen on the same port, on the same computer.)
2. Ensure that Microsoft IIS is either *not* running, or *not* accepting connections on the GO-Global Host.
3. From the Admin Console, change the value of the **Port** field on the **Security** tab of the **Host Options** dialog to 443. For more information about the Security tab, see Chapter IX.



4. After modifying the host port setting, append the **port** parameter followed by 443 to the web link that is used to connect to the host. For example, **http://hostname.graphon.com/goglobal/?host=hostname.graphon.com&port=443**
5. Obtain **TLS Certificates** for the host via the **Security** tab of the **Host Options** dialog. If you are using a separate web server, ensure that the domain name of the web server computer and the domain name of the GO-Global Host are the same. Otherwise, the browser will prevent the Web App, which is downloaded from the web server, from opening a WebSocket connection to the GO-Global Host.

6. Configure the external DNS to resolve the **Common Name** of the host certificate to the external IP address of the host computer. If you are using a separate web server, configure the external DNS to resolve the **Common Name** of the web server's certificate to the external IP address of the web server computer.
7. If users will access the host from the internal network, configure the internal DNS to resolve the **Common Name** of the host certificate to the internal IP address of the host computer and, if there is a separate web server, to resolve the **Common Name** of the web server's certificate to the internal IP address of the web server.

Server Roles and the Configuration Tab

Administrators can designate server roles in the Admin Console, through the **Configuration** tab of the **Host Options** dialog. For example, administrators can designate a GO-Global Host as an Application Host (i.e., Independent Host, Dependent Host, or Farm Host) or as an Application Host Manager (i.e., Relay Load Balancer or Farm Manager.)

Load balancing and server roles are described in Chapter VII. Through the Configuration tab, administrators can also configure a Backup License Manager, described in the previous chapter.

Application Host Managers and License Servers

When an Application Host Manager (e.g., Relay Load Balancer) is used, GO-Global manages licenses from the Application Host Manager by default. This provides the following benefits:

- It enables administrators to add and remove Application Hosts to a cluster without having to make licensing configuration changes.

- When a cloud license is used, it enables all hosts in the cluster to share reserved seats when the hosts are unable to communicate with the GraphOn Cloud License Service.

Prior to version 6.1, GO-Global managed licenses from Dependent Hosts by default. This required administrators to configure each Dependent Host to use a central license manager. Dependent Hosts that are upgraded to version 6.1 or later from older versions will continue to manage licenses from Dependent Hosts.

After upgrading, administrators can change this by editing the value of the **ManageLicensesFrom** property in the **HostProperties.xml** file from **Host** to **Relay** on all the Dependent Hosts and the Relay Load Balancer, as follows:

To checkout licenses from the Relay Load Balancer

1. Stop the **GO-Global Application Publishing Service**.
2. Locate the file **HostProperties.xml** in the C:\ProgramData\GraphOn\GO-Global directory.
3. Open **HostProperties.xml** in WordPad and locate the **ManageLicensesFrom** property.
4. Set the **ManageLicensesFrom** property to **Relay**.
5. Save the file.
6. Restart the **GO-Global Application Publishing Service**.

Downgrading GO-Global

GO-Global's migration utility (migrate.exe) can be used to install older versions of GO-Global on systems where a newer version is already installed. The migration utility backs up and restores settings, configuration files, licenses, and registry entries.

To run the migration utility

1. Open Command Prompt.
2. Type migrate.exe -d, followed by the complete path to the host installer you are downgrading to. If there is a space in the path, it will need to be enclosed in quotes.

   For example:
   migrate.exe -d "c:\users\username\Downloads\gg-host.exe"

The migration utility will run several times, each time creating a log file in the %temp% folder. During a downgrade, the installer's user interface is hidden. The machine will reboot twice; once after the existing version is uninstalled, then again after the gg-host.exe specified on the command line is installed. After the first reboot, click **Yes** when presented with the UAC prompt. If the UAC is canceled after the first reboot, a shortcut named **Complete GO-Global Downgrade** is created on the desktop.

When the Command Prompt is run using a non-admin account, the shortcut is placed on the desktop of the user running the command. When the Command Prompt is run using an admin account, the shortcut is placed on the admin's desktop.

The migration utility is included in Programs folder on the GO-Global Host (e.g., C:\Program Files\GraphOn\GO-Global\Programs.). It can be used to downgrade to any 6.x release and can be copied to another system along with a host installer (gg-host.exe).

Managing Applications

The Admin Console allows you to publish and share applications.

Installing Applications

When installing applications to be run through GO-Global, please consult the vendor's documentation for instructions on proper multi-user installation. You will likely need to install the application under an administrative account, but installation requirements will vary depending on the application. Installation should also adhere to Microsoft's guidelines for multi-user deployment.

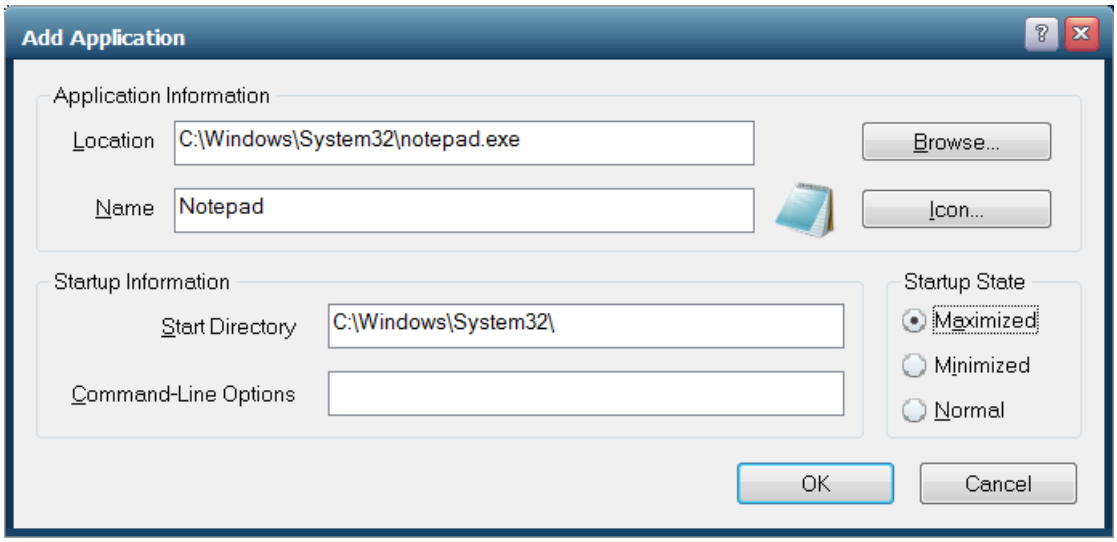
Deploying applications via GO-Global does not entitle your enterprise to unlimited access rights. You must still abide by the vendor's licensing agreement with regard to the number of applications that can be run concurrently.

Publishing Applications

Applications are published in the Admin Console. When you publish an application, you can specify the application's startup state, as well as startup parameters that control how the application opens. When running the ***Quick Start***, follow the prompts to publish an application.

To publish an application

1. Select the desired host from the list of **All Hosts**.
2. Click the **Applications** tab.
3. Click the **Add** button.
4. Click the **Browse** button next to the **Location** box to locate and select the application's executable file.
5. Click **OK.**



By default, the browse dialog opens to the **PROGRAMDATA\Microsoft\Windows\Start Menu\Programs** directory. After publishing the first application, the dialog then opens to the directory of the last published application.

Changing the Application Name

If you browsed for the application's .exe file, the file name will automatically be entered in the **Name** box. (This application name is displayed to users in the Program Window.) You can keep the default display name, or you can type a new one. The application name cannot consist entirely of spaces, and it cannot contain a backslash (\). This field cannot be left blank.

Changing the Application Icon

Click the **Icon** button if you would like to select an icon other than the application's default icon.

Changing the Startup State

In the Startup State section, select whether the application starts *Maximized*, *Minimized*, or in *Normal* mode. The default startup state is Normal.

Changing the Start Directory

If you browsed for the application's executable file, the pathname of the directory will automatically be displayed in the **Start Directory** box. Otherwise, type the full pathname of the directory in which you want the application to start.

Specifying Command-Line Options

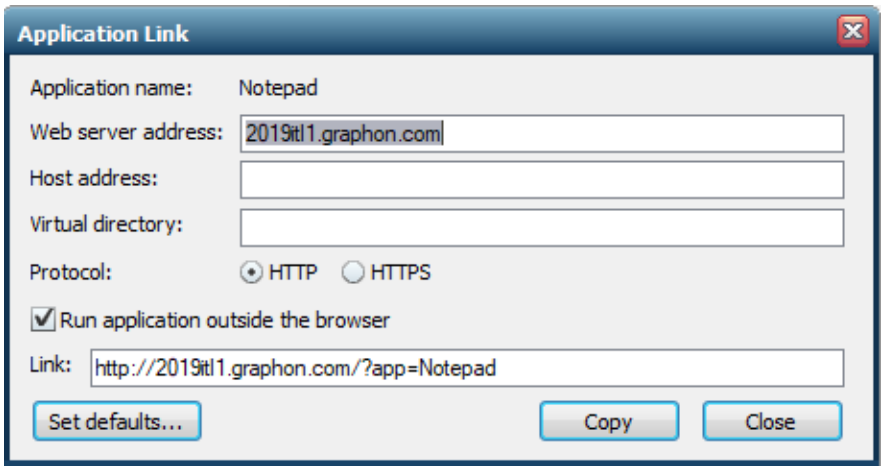
In the **Command-Line Options** box, you can specify launch parameters for the application. Because these parameters are specific to each application, please refer to the application's documentation for information about specific launch parameters.

Sharing a Link to a Published Application

The Admin Console's **Get Link** button allows you to copy a link to the selected application and share it with users for quick access to the application.

To share an application link

1. From the list of **Installed Applications**, select the application you would like to share.
2. Click the **Get Link** button to the right of the list of Installed Applications.
3. From the **Application Link** dialog, click the **Copy** button to copy the link to the clipboard.
4. Paste the link into an email or instant message and share with users.



If the Admin Console is running in tutorial mode, the following message is displayed when clicking the **Copy** button: *Click **Copy** to copy this link to the clipboard. You can then paste it into an email or instant message and share it with users*.

When a user clicks on a link to an application, the following actions occur:

1. The user's browser opens a connection to the web server at the address specified in the **Web server address** field.
2. The user's browser downloads and runs the GO-Global Web App.
3. The GO-Global Web App opens a WebSocket connection to the Application Publishing Service (APS) at the address specified in the **Host address** field and passes the link's arguments to the host.
4. The APS processes the link's arguments and determines if AppController should be used.
5. If AppController should not be used (if useApp=false), the APS starts the user's session and displays the session within the user's browser using the Web App.
6. Alternatively, if AppController should be used, the APS communicates with the Web App over the WebSocket connection and orchestrates the starting and, if necessary, installation of AppController:
   a. If installation of AppController is required, the browser opens another connection to the web server at the **Web server address** and downloads AppController.
   b. AppController starts and opens a connection to the Application Publishing Service at the **Host address**.
   c. The Application Publishing Service starts the user's session. By default, the user's session is displayed outside the browser window by AppController. Alternatively, if the "embed" URL parameter is set to true, the user's session is displayed within the browser by the Web App, and AppController provides access to client devices (e.g., drives, printers, etc.).

Editing the Web Server Address

The **Web server address** specifies the address that users must enter into their browsers' address bars to download the GO-Global Web App and AppController. This address appears in the URL after the protocol prefix (http:// or https://).

By default, GO-Global sets the **Web server address** to the local address of the GO-Global Host. If, however, a web server on another computer or a load balancer will be used, set the **Web server address** to the address of the web server or load balancer. Similarly, if users will connect to the host via the host's public address rather than the host's local address, set the **Web server address** to the host's public address.

By default, browsers connect to port 80 when the protocol is HTTP, and to port 443 when the protocol is HTTPS. If the web server that will accept the browser's connection is configured to use a different port, the port must be appended to the **Web server address**. For example, if GO-Global's integrated web server is used (the default), and the port specified on the Security tab of the Admin Console's Host Options dialog is set to the default 491, GO-Global appends **:491** to the **Web server address** as follows: **http://web_server_address:491**

By default, GO-Global sets the **Web server address** so that connections from browsers are directed to the host's Application Publishing Service, GO-Global's integrated web server. Therefore, if the GO-Global Host is configured to use its default port 491, or any port other than 80 or 443, GO-Global appends the port to the **Web server address**. If, however, the connections from users' browsers will be accepted from some other web server (e.g., Microsoft Internet Information Services), it will generally not be necessary to append the port to the **Web server address** because the port will be specified implicitly by the protocol (HTTP or HTTPS).

The port discussed in this section (which may be specified implicitly via the protocol or explicitly after the web server address) is the port that the browser uses to connect to the web server. It is not the port that the Web App uses to connect to the Application Publishing Service. By default, the Web App attempts to connect to the GO-Global Host on GO-Global's default port, 491.

If the **Port** specified on the **Security** tab of the Admin Console's **Host Options** dialog is something other than 491, the port must be specified in the URL by adding the **&port** parameter to the URL. For example, if the **Port** specified on the **Security** tab is 80, it must be added to the URL as follows: **http://web_server_address/?port=80.**

To edit the Web Server address

1. In the **Application Link** dialog, type the address of your web server in the **Web Server address** box. The application link will update automatically.
2. Click the **Copy** button to copy the URL and share with users.

If users will access the host from both internal and public networks, the host and web server must be accessible from both the internal and public networks via the addresses specified in the **Host address** and **Web server address** fields.

To accomplish this, internal DNS entries must map the **Host address** and **Web server address** to the internal IP addresses of the computers, and public DNS entries must map the **Host address** and **Web server address** to the public IP addresses of these computers.

Editing the Host Address

The **Host address** specifies the address that AppController or the Web App will use to connect to the Application Publishing Service on the host computer. By default, this is the local, fully qualified domain name of the computer on which the GO-Global Host is installed. In cases where clients connect to hosts via a load balancer (e.g., a GO-Global Relay Load Balancer or a third-party load balancer), set the **Host address** to the fully qualified domain name of the load balancer.

If the Host address is not specified (the default), AppController and the Web App use the Web server address to connect to the Application Publishing Service.

To edit the Host address

1. In the **Application Link** dialog, type the fully qualified domain name of the host in the **Host address** box. The application link will update automatically.
2. Click the **Copy** button to copy the URL and share with users.

Editing the Virtual Directory

If Microsoft Internet Information Services (IIS) is installed on the host computer, the GO-Global Host installer creates a virtual directory in IIS named *goglobal* for the GO-Global Web files. When hosting web files from a virtual directory other than the default, edit the name of the virtual directory in the **Application Link** dialog.

When using GO-Global's integrated web server, no virtual directory is required.

For backward compatibility, GO-Global's integrated web server will also work with URLs that include the goglobal virtual directory even when the **Virtual directory** field is blank.

To edit the Virtual Directory

1. In the **Application Link** dialog, type the name of the virtual directory in the **Virtual Directory** box. The application link will update automatically.
2. Click the **Copy** button to copy the URL and share with users.

Editing the Protocol

The protocol that browsers use to connect to the web server is specified at the beginning of the URL. Generally, when the protocol specified on the **Security** tab of the Admin Console's **Host Options** dialog is set to TCP, the protocol specified in the **Application Link** dialog must be HTTP. Similarly, when the protocol specified on the **Security** tab is TLS, the protocol specified in the **Application Link** dialog must generally be HTTPS. If there is a mismatch, the Web App will fail to connect to the host, and the host's log will contain a message explaining the issue.

The only time this is not true, is when the host is deployed behind a load balancer that terminates the TLS at the load balancer. In this case, the protocol in the **Application Link** dialog must be HTTPS, but the protocol on the **Security** tab will be TCP (unless the load balancer uses TLS for internal connections).

By default, GO-Global sets the protocol in the **Application Link** dialog to HTTP or HTTPS when the protocol specified on the **Security** tab is, respectively, TCP or TLS. In cases where TLS is terminated at the load balancer, administrators can change the protocol.

To edit the Protocol

1. In the **Application Link** dialog, click **HTTP** or **HTTPS**. The application link will update automatically.
2. Click the **Copy** button to copy the URL and share with users.

Running the Application Outside the Browser

When the user clicks the link to the published application and signs in to the GO-Global Host, the application opens and runs outside the web browser. To disable this default setting, uncheck **Run application outside the browser**. This will add the parameter **&embed=true** to the URL. When the user clicks the link with this parameter added, the application will run inside the user's web browser.

Enabling Access for Remote Users

If you have users who will access a GO-Global Host from the internet, you must ensure that these users are able to connect to the host computer. This is typically done via a VPN or by configuring a GO-Global Relay Load Balancer in a DMZ network. Alternatively, if you don't have a VPN or a DMZ network, you can forward ports from your internet router to the GO-Global Host using the following steps:

1. Open your router software and locate the port forwarding settings. Typically, this will be under **Advanced** and then **Port Forwarding**.
2. Create a new service called GO-Global, if needed.
3. Set the internal and external port range to 491 and set the protocol to UDP/TCP packets.
4. Enter the internal IP address of the GO-Global Host.
5. Click **Apply** or **Save** to store the changes.
6. In the **Application Link** dialog, type the public IP address of the GO-Global Host in the **Host address** box. The application link will update automatically. (The public IP address can be found by visiting whatismyip.com from a browser on the GO-Global Host.)
7. Click the **Copy** button to copy the URL and share with remote users.

Setting Default Link Properties

You can set the default application link properties to those specified in the **Application Link** dialog, to include the Host address, Web server address, and whether the application is run inside or outside the browser. These default link properties will be applied when new applications are published.

To set the default link properties

1. From the **Application Link** dialog, click the **Set defaults** button.
2. Click **Yes** to confirm.

Duplicating an Application

Duplicating an application makes an exact copy of the selected registered application. This is useful if you want to make the same application available to different users or groups but with variations. For instance, you may want to register one version of an application with command-line options to bypass the **Sign In** dialog, and another version without command-line options that requires clients to sign in. When duplicating an application, you are required to select a new display name.

To duplicate an application

1. From the list of **Installed Applications**, select the application you would like to duplicate.
2. Click Tools | Applications | Duplicate.
   –or–
   Click the **Duplicate** button to the right of the list of Installed Applications.

To rename an application's display name

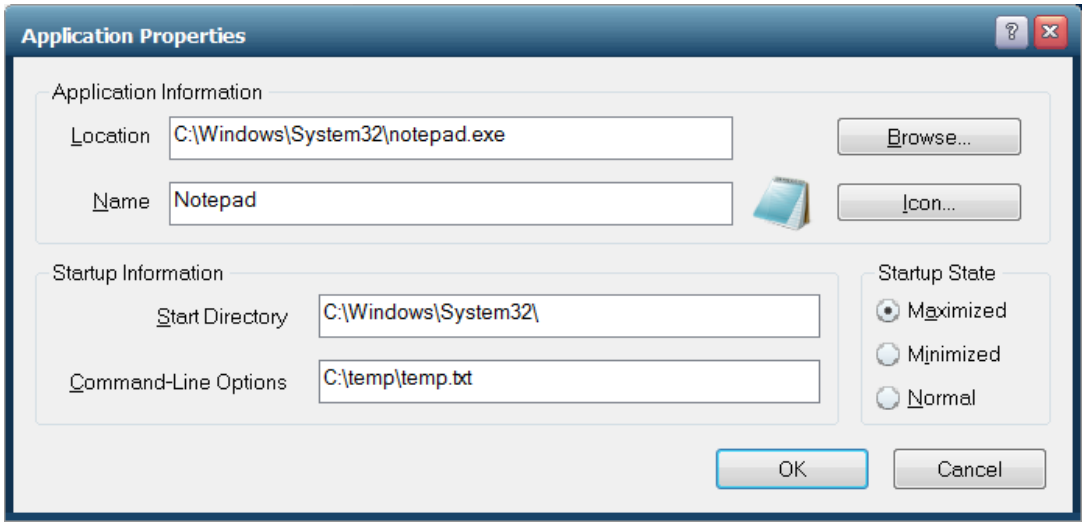
1. From the list of Installed Applications, select the application you would like to rename.
2. Click Tools | Applications | Rename.
   –or–
   Click the **Rename** button to the right of the list of Installed Applications.
3. Type a name in the **New** box in the **Rename Application** dialog.

Editing an Application's Properties

Once an application has been published, you can edit the application's properties at any time. For example, you can edit the application's startup state, the location of its executable file, or the folder from which you want the application to start.

To edit an application's properties

1. Click the **Applications** tab.
2. Select an application from the list of **Installed Applications**.
3. Click the **Properties** button.
4. Do any of the following:
   - In the **Location** box, type a new pathname.
   - In the **Start Directory** box, type the full pathname of the directory in which you want the application to start.
   - In the **Command-Line Options** box, type any startup parameters for the application.
   - In the **Display Name** box, type a new display name for the application.
   - In the **Startup State** section, select whether the application starts maximized, minimized, or in normal mode.
   - Click the **Icon** button to browse for a new application icon.



To remove an application

1. Click the **Applications** tab.
2. From the Installed Applications list, select the application(s) you want to remove.
3. Click the **Remove** button.

   –or–

   Click Tools | Applications | Remove.

If you remove an installed application from the Admin Console while a user is running the application, the user's session is not interrupted. When the user exits that application, however, the application will no longer be available, and the icon will not appear in the Program Window.

After registering an application with the Admin Console, the application's name and path will appear in the list of **Installed Applications**. You can sort items in the list in ascending or descending order by clicking the column's title. This holds true for all lists in the Admin Console.

If you want to set up applications that use ODBC data sources, you must set up the ODBC drivers as system DSNs (data source names), in order for GO-Global clients to be able to access the data sources. For more information about data sources, consult the Windows ODBC Data Source Administrator online Help.

Due to access restrictions, the Admin Console cannot verify the validity of paths specified in UNC format (e.g., \\Machine Name\Folder Name\...) or that reside on a mapped network drive. If the Location or Start Directory of a published item involves a mapped drive or is specified with a UNC path, the Admin Console will accept the specified path regardless of whether or not it is valid. If the path is invalid, or if the client user does not have rights to access the specified executable file or folder, the published item will not appear in the Program Window. Select the item and click the **Properties** button. Try updating the item's **Location** or its **Start Directory**.

If the item has been uninstalled or moved to a new location, it will not be displayed in the Admin Console when the Application Publishing Service has been restarted.

The Admin Console is unable to display group and user settings for any item's path specified in UNC format or that resides on a mapped drive. The following message is displayed in the Admin Console's Application Users/Groups window for any application or file where this applies: "User/Group settings not available."

If an item that resides on a mapped drive but is not licensed for use with GO-Global is published in the Admin Console, the item's icon will appear in the Program Window. However, the user will be unable to open the item and will receive an error message when attempting to launch it.

Click the right mouse button on an item in the list of Installed Applications or the list of Application Users/Groups to display shortcut menus of the most frequently used commands.

Assigning Application Launch Parameters to Users or Groups

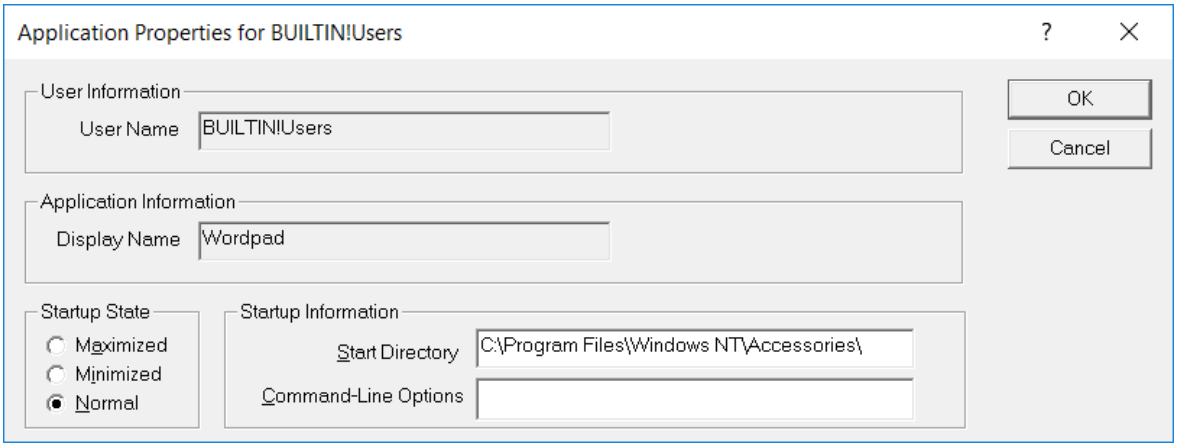
The Admin Console allows you to assign specific parameters for how an application will run for users or groups on the network or on local machines. The parameters set for a user or group will apply each time that user or group launches the application. Application launch parameters set for an individual take precedence over parameters set for a group or for an application. When a client launches an application through GO-Global, the Program Window will first check for launch parameters assigned to the individual user. If no parameters are assigned, it will check the list of Groups the user belongs to, in the order the Program Window obtains them from the system. Otherwise, the Program Window will look for generic launch parameters assigned to the application.

Check the user's ***About GraphOn GO-Global*** box to verify what Group or Groups the user is assigned to and in what order the Groups are listed in the system.

File permissions for users and groups are controlled by Windows NT file system (NTFS) security settings on the host. File permissions are *not* set through the Admin Console. When you select an application from the Installed Applications list, the Application Users/Groups list displays the user permissions that have been specified for that file and/or application with NTFS. You can then edit the application's properties for specific users or groups. File permissions can only be set on drives formatted with NTFS.

To assign application launch parameters for a user or group

1. Click the **Applications** tab.
2. Select an application from the list of **Installed Applications**.
3. Select a user or group from the **Application Users**/**Groups** list.
4. Click the **Properties** button.
5. Do any of the following:
   - In the **Start Directory** box, type the full pathname of the directory in which you want the application to start.
   - In the **Startup State** section, select whether the application starts maximized, minimized, or in normal mode.
   - In the **Command-Line Options** box, type the command-line arguments you want to use when launching the application.



CHAPTER IV

Running GO-Global

4

AppController

AppController combines the functionality of GO-Global's native clients and browser add-ons into a single application that can be started from a computer's desktop, a mobile device, or a web browser.

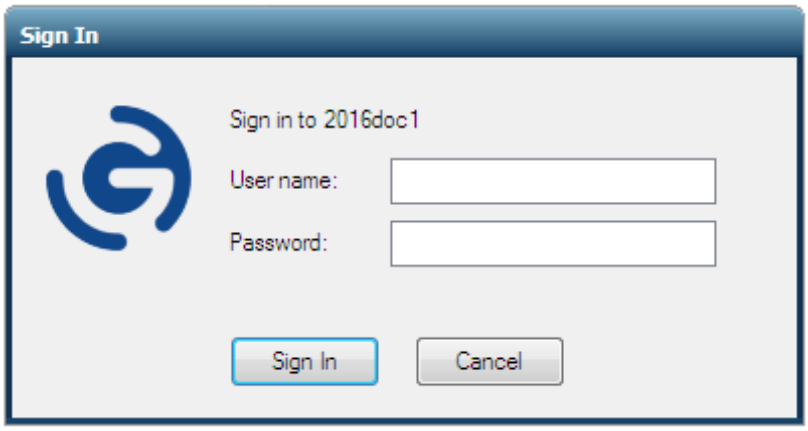
To install AppController

1. Start a Web browser.
2. In the Location box, type http:// followed by the host name and AppController installation page. For example, **http://hostname/goglobal/**
3. If AppController is not installed, you will be prompted to download it. Run the setup program from your computer's operating system (e.g., **GO-Global.AppController.exe, GO-Global.AppController.dmg, GO-Global.AppController.deb,** or **GO-Global.AppController.rpm.)**
4. On macOS, drag **AppController** to the Applications folder.

After installing AppController, you can run GO-Global from a browser, from the Start menu, or from a shortcut. By default, the installation file names are renamed from AppController to GO-Global.AppController when downloaded. If the Installer name has been changed via the Branding dialog of the Admin Console, that name will replace GO-Global in the installer name. (E.g., Acme.AppController.exe).

To run AppController from the computer's menu

1. Select the AppController menu option:
    a. On Windows, click the **Start** button on the Windows taskbar, and select Programs | AppController.
    b. On Linux, select the Network or Internet category from the Applications menu, then click **AppController**.
    c. On macOS, select Go | Applications from the menu, then double-click **AppController**.
2. Type the address of the host in the **Connection** dialog.
3. Click **Connect**. When the **Sign In** dialog appears, type the following information:
    - Network user name in the **User name** box.
    - Network password in the **Password** box.



User names

Unlike Windows, GO-Global does not prompt users for a domain. When a domain is not specified, Windows attempts to authenticate the user on the local computer, the computer's domain, and trusted domains. If users wish to authenticate to a specific domain, they can enter both the name of the domain and the user name in the **User name** field.

For example, to authenticate on a specific domain, users can enter **domain\username**. Similarly, to authenticate to the local computer, users can enter **computername\username**.

GO-Global allows **three** invalid logon attempts before shutting down the logon process. After the third failed attempt, the **Sign In** dialog closes and the user is disconnected. The user can then reconnect to the host and again attempt to sign in, up to the number of failed attempts allowed by Windows. When users do not include the domain in the **User name** field, however, their account may be locked out before they have reached the number of failed attempts allowed by Windows. This is because each attempt that Windows makes to authenticate the user on the local computer, the computer's domain, and trusted domains counts as a failed attempt. To avoid this, include the name of the domain along with the user name in the **User name** field of the **Sign In** dialog.

On Windows computers, the Connection dialog has an option to create a shortcut to a GO-Global host. You can use this option to bypass the Connection dialog when connecting to a host.

To create a shortcut to a GO-Global Host on a Windows computer

1. Start AppController via one of the above methods.
2. Type the address of the host in the **Connection** dialog.
3. Select the **Create desktop shortcut** to this host check box.
4. Click **Connect**. A shortcut to the host will be created on the desktop of the computer.

To create an AppController shortcut on Windows

1. Right-click on the desktop.
2. Click New | Shortcut.
3. In the **Create Shortcut** dialog box, browse to the AppController executable. For example, "C:\Program Files\GraphOn\AppController\AppController.exe"
4. Add parameters after the path to AppController.exe. For example:

   "C:\Program Files\GraphOn\AppController\AppController.exe" -h hostname -a WordPad *-r "C:\Users\Public\Public Documents\test.rtf"*
5. Type a name for the shortcut and click **Finish**.

GO-Global Web App

Developed with JavaScript and HTML5, the GO-Global Web App is a zero-install client that allows users to run Windows applications from popular web browsers on Windows, Mac, and Linux computers. In addition, no special host configuration is required to deploy the Web App. The Web App supports client-side password caching, printing to local printers via GO-Global's Preview PDF printer, and copying and pasting text between local and remote applications using CTRL keys.

Running the GO-Global Web App

GO-Global can be run from popular web browsers, including Microsoft Edge, Mozilla Firefox, Google Chrome, and Apple Safari.

To run GO-Global from a Web browser

1. Start a web browser.
2. In the **Location** box, type http:// or https:// followed by the host name, followed by ?useApp=false
   For example:
   http://hostname/goglobal/?useApp=false or
   https://hostname/goglobal/?useApp=false
3. When the **Sign In** dialog appears, type the following information:
   - Network user name in the User name box.
   - Network password in the Password box.

When **https://** is specified in the Location box, the **TLS protocol** must be enabled on the Security tab of the Admin Console's **Host Options** dialog, and the common name of the TLS Certificate specified on the tab must match the host name specified in the URL. These are new requirements in GO-Global v6. With earlier versions, GO-Global's browser plug-ins and add-ons (which used technologies most browsers no longer support) could connect to GO-Global Hosts using TCP even when they were run from web pages that were downloaded to the browser over HTTPS. GO-Global's Web App, however, is subject to browser security restrictions, which require web apps to use WebSocket Secure connections when they are loaded over an HTTPS connection. See Selecting TLS Protocol for more information.

By default, GO-Global attempts to automatically download and run AppController. Appending **?useApp=false** to the logon URL will prevent GO-Global from downloading AppController and will run the GO-Global Web App instead.

Running the GO-Global Web App with AppController

The GO-Global Web App allows users to run applications from a browser without installing anything on their computer. However, there are several limitations when only the Web App is run. For example, when running only the Web App, the following features are not supported or available: client file access, serial and parallel ports, smart cards, client sound, printing directly to client printers, and running GO-Global in loose windows mode. These limitations can be easily overcome by downloading and installing AppController. After installing AppController on a Windows, Linux, or Mac computer, users who run GO-Global from a web browser will have access to all these features.

GO-Global provides the **useApp** parameter to control installation and execution of AppController. When useApp=true, the Web App will try to launch AppController. When useApp=false, the Web App will *not* try to launch AppController. When useApp=force, the user will not be given the option to run applications via the Web App within the browser. The user will only be able to run applications via AppController. useApp=true by default.

If this parameter is not specified in the URL (e.g., if the URL is **http://hostname/goglobal**), the user will be prompted to download, install, and run AppController.

When AppController is installed and enabled, the “embed” URL parameter can be used to control whether applications run within the browser window or outside the browser window. If the embed parameter is not specified or is set to “false” (e.g., if the URL is **http://hostname/goglobal/?embed=false**), the user’s applications will run outside the browser’s windows via AppController.

Alternatively, if the embed parameter is set to “true” (e.g., if the URL is **http://hostname/goglobal/?embed=true**) applications will run inside the browser window via the Web App. In this case, GO-Global will also start AppController (if it is installed and enabled), but AppController will only be used to provide access to the computer’s devices (e.g., printers and drives); it will not display the session’s applications.

When AppController is run inside the browser window, the default background color is white. The background color is specified by the **DesktopColor** property in the **HostProperties.xml** file. The color is specified as an RGB value in decimal format. For example, the default color of white is 16777215 in decimal (0x00FFFFFF in hexadecimal). To change the background color to blue, for example, set the **DesktopColor** property to 10906937.

When AppController is not installed or useApp = false, the embed option is ignored. Otherwise, embed is set to false by default.

When the embed option is enabled, AppController is launched with the **-host** parameter set to the value in the **hostaddress** field of the host's config.xml file. The GO-Global installer initializes this value to the name of the computer. If users connect to the host with a different address (e.g., a public DNS address), the **hostaddress** field in the config.xml file must be set to this address.

To modify the hostaddress value

1. Stop the **Application Publishing Service**.
2. Locate the **config.xml** file in the C:\ProgramData\GraphOn\GO-Global directory.
3. Open **config.xml** in WordPad and locate the <hostaddress> field.
4. Update the **hostaddress** value.
5. Save the edited .xml file.
6. Start the **Application Publishing Service**.

When using the GO-Global Web App, copying and pasting to the clipboard through an application's menu or toolbar is not supported. Instead, on Windows, use the keyboard shortcuts **CTRL+C** to copy and **CTRL+V** to paste. On the Mac, use the keyboard shortcuts **Command-C** to copy and **Command-V** to paste.

Accessing the Host or Relay Load Balancer Directly from the Internet

If users will be connecting to a GO-Global Host or Relay Load Balancer from the internet, the web server and host addresses in the URL must resolve to public (internet) IP addresses.

If users will be accessing a host or Relay Load Balancer from both the internet *and* the internal network, the external and internal DNS should be configured so that the public and internal addresses of the web server are the same, and the public and internal addresses of the host are the same. Alternatively, administrators can provide external and internal users with different URLs, but this may be confusing to users.

When hosts are accessed via a third-party load balancer, the URL must include the address of the load-balancer. For example, **http://loadbalancer.com/goglobal/?host=hostname&app=Notepad**

macOS App

GO-Global's macOS App is a lightweight application that provides seamless integration with the native macOS environment. It has been completely re-written to use modern macOS APIs, and provides simplified installation, sound support, multi-monitor support, and macOS Gatekeeper support, which helps protect against malware and misbehaving apps downloaded from the internet.

To install the macOS App

1. Launch your web browser.
2. In the Location box, type or paste the URL to connect to the GO-Global Host. For example, **http://host/goglobal/**
3. Follow the instructions to download and install **AppController.dmg**.
4. Open **AppController.dmg** and drag **AppController.app** into Applications.

To run the macOS App

1. From the menu bar, click Go | Applications.
2. Double-click **AppController**.
3. Type the host address in the **Connection** dialog.
4. When the **Sign In** dialog appears, enter the following information:
   - Your network user name in the **User name** box.
   - Your network password in the **Password** box.

To uninstall the macOS App, drag **AppController.app** from Applications to the trash.

To use startup parameters with the macOS App

1. Open **Terminal**.
2. Change to the **/Applications/AppController.app/Contents/MacOS/** directory.
3. Type **./AppController** and append startup parameters.

For example, ./ AppController -h 196.125.101.222 -ac all -hp 443

To create a desktop shortcut on macOS

1. Run Automator from the **Applications** folder.
2. Choose **Application** for the type of document.
3. Select **Run Shell Script** for the **Action**.
4. Add the following command line to the **Run Shell Script** dialog:
   /Applications/AppController.app/Contents/MacOS/AppController
5. Optionally add GO-Global startup parameters to the command line.
   For example: /Applications/AppController.app/Contents/MacOS/AppController -h 196.125.101.222 -u VictorH -a WordPad &
6. Save the application with an appropriate name on the desktop. Running the application will run AppController with the given startup parameters.

GO-Global provides limited support for client-attached USB devices. Specifically, it supports client-attached USB printers, drives, and some smart card readers. It does not support general-purpose USB-redirection of other types of USB devices.

GO-Global Startup Parameters

GO-Global supports the following shortcuts and parameters:

Client Shortcut URL Parameter	Parameter Description
-u user=	The name of the user's account.
-p password=	The user's password. This plaintext password parameter should only be used in controlled environments, due to security implications.
-h host=	*The network name of the GO-Global Host.
-hp port=	The port on which the GO-Global Host accepts connections. (491 by default.)
-a app=	The application to run. This may be a command-line string or the application name, as registered with the Admin Console.
-r Args=	Application arguments.
-c or -nc compression=	-c enables compression. -nc disables compression. compression=true enables compression. compression=false disables compression. Compression is enabled by default.
-ac printerconfig	Determines how printers are initialized at startup. When printerconfig=all or -ac is followed by all, all printers are automatically configured. When printerconfig is set to none or -ac is followed by none, printers are not automatically configured. When printerconfig is set to "default" or -ac is followed by default, the default printer is configured automatically. This is the default setting.
-f clientframe=	When set respectively to 1 or "true", all applications running in the session will be displayed within a bounding window. When set respectively to 0 or "false", applications will be displayed within their own individual windows.
-autoreconnect autoreconnect=	Determines how many times the client will automatically attempt to reconnect after a broken connection. When autoreconnect=n in a URL or -autoreconnect is followed by n, the client will automatically attempt to reconnect *n* number of times. autoreconnect is set to 20 by default.

Client Shortcut URL Parameter	Parameter Description
-geometry Not available	The width and height of the client window. For example: -geometry 800x600
-mm multimonitor=	-mm 1 or multimonitor= true will span the session's desktop across all monitors. -mm 0 or multimonitor=false will confine the session's desktop to the primary monitor. Multi-monitor support is enabled by default. For more information, see **Multi-Monitor Support**.
Not available width=	The width of the frame or embedded window. (800 by default.)
Not available height=	The height of the frame or embedded window. (600 by default.)
Not available embed=	When set to "true" applications run within the browser window. When set to "false" applications run outside the browser window.
Not available noscale=	When noscale is set to "true" and the browser is resized, the resolution of the embedded GO-Global session will adjust accordingly, rather than scaling the displayed image on the client. noscale is set to "false" by default.
Not available useApp=	When useApp is set to "true", the GO-Global Web App will try to launch AppController. When useApp=false, the Web App will not try to launch AppController. useApp is set to "true" by default.
-clientscale clientscale=	clientscale, followed by the percent scale factor, causes AppController on Windows to scale the applications running in the session relative to applications running locally on the client computer. For example, adding -clientscale 200 to the command-line will cause applications running in the GO-Global session to appear twice as large as applications running locally on the client computer.
-clientdpi ClientDPIScalingEnabled=	-clientdpi 1 or ClientDPIScalingEnabled=true enables the GO-Global App's DPI scaling feature. -clientdpi 0 or ClientDPIScalingEnabled=false disables the feature. When these options are specified, they override the value of the ClientDPIScalingEnabled property in the HostProperties.xml file on the host.

Client Shortcut URL Parameter	Parameter Description
-cn computerName	When -cn 1 or computerName=1, the Windows client sends the CLIENTNAME environment variable to the host rather than the actual computer name.
-krm keyreportingmethod=	This option instructs the client to send either Unicode or keycode values to the host based on character type. This option can be used to resolve issues where an application fails to process certain keys correctly. Valid values for the option are as follows: 0: a-z A-Z are Unicode, 0-9 are Unicode, other characters are Unicode 1: a-z A-Z are keycode, 0-9 are Unicode, other characters are Unicode 2: a-z A-Z are Unicode, 0-9 are keycode, other characters are Unicode 3: a-z A-Z are keycode, 0-9 are keycode, other characters are Unicode 8: a-z A-Z are Unicode, 0-9 are Unicode, other characters are keycode 9: a-z A-Z are keycode, 0-9 are Unicode, other characters are keycode 10: a-z A-Z are Unicode, 0-9 are keycode, other characters are keycode 11: a-z A-Z are keycode, 0-9 are keycode, other characters are keycode Please see the **Advanced Topics** chapter for more information.
-connectretry connectretry=	To increase the period of time that a client can attempt to connect to a host, use -connectretry X or connectretry=X, where X is the number of times the client will try to connect to the host before displaying an error message. The client will wait 4 seconds between attempts. If -connectretry 5 is specified, for example, the client will try to connect 5 times at 4 second intervals, for a total of 20 seconds.
-showlogon showlogon=	To prevent the Sign In dialog from being displayed to users when **Cache password on the client** is enabled, add -showlogon 0 (AppController on Windows only) or showlogon=false.
-dfw dfw=	When dfw is set to 1, contents of the window will be shown when moving or resizing windows. When dfw is set to 0, only the bounding rectangle will be shown when the window is moved or resized. Please see the **Advanced Topics** chapter for more information about Dragging Full Windows.

Client Shortcut URL Parameter	Parameter Description
-tls tls=	Set to 1 or "true", respectively, when AppController or the GO-Global Web App will connect to a load balancer that is configured to terminate TLS at the load balancer. Otherwise, if neither the load balancer nor GO-Global is configured to use TLS, or TLS is terminated at the GO-Global Host, set to 0 or "false", respectively. This is the default setting.
-wsurl wsurl=	The WebSocket URL that the Web App and/or AppController use to connect to the host service (e.g., web application firewall (WAF), reverse proxy, GO-Global Host, etc.). The format is: [protocol]://[address]:[port]/[resource]. The parameters specify, respectively, the protocol, address, port, and resource of the host service. For more information, see **Connecting with WebSockets**.

***If no host is specified in the logon HTML page, GO-Global detects the machine from where the logon file was downloaded, and makes the connection to that host. The Connection dialog is not displayed and the user is presented with the Sign In dialog only. If host= "?" users will be prompted for the address of the host.

Modifying the Logon HTML Page

When GO-Global is run from a Web browser, startup parameters can be specified by editing the GO-Global logon.html page.

To modify logon.html

1. Open logon.html in an HTML editor.
2. Locate the parameter you wish to edit. The most common parameters are listed in the logon page as follows:

```
//
// controlArgs.set([ "user",          "testuser1"     ]);
// controlArgs.set([ "password",      "testpassword1" ]);
// controlArgs.set([ "embed",         "false"         ]);
// controlArgs.set([ "width",         "640"           ]);
// controlArgs.set([ "height",        "480"           ]);
// controlArgs.set([ "desktop",       "false"         ]);
// controlArgs.set([ "app",           "testapp1"      ]);
// controlArgs.set([ "port",          "491"           ]);
// controlArgs.set([ "autoclose",     "false"         ]);
// controlArgs.set([ "printerconfig", "default"       ]);
// controlArgs.set([ "bInBrowser",    "false"         ]);
// controlArgs.set([ "host",          "testhost1"     ]);
// controlArgs.set([ "compression",   "true"          ]);
// controlArgs.set([ "clientframe",   "false"         ]);
// controlArgs.set([ "multimonitor",  "true"          ]);
```

```
// controlArgs.set([ "noscale",        "false"          ]);
// controlArgs.set([ "authority",      "not_specified" ]);
// controlArgs.set([ "credentials",    "not_specified" ]);
// controlArgs.set([ "sessionid",      "1234"           ]);
// controlArgs.set([ "autoreconnect", "0"              ]);
// controlArgs.set([ "windowless",     "false"          ]);
// controlArgs.set([ "maxbpp",         "16"             ]);
// controlArgs.set([ "keyboard",       "ClientSideIME" ]);
// controlArgs.set([ "args",           "testargs1"      ]);
// controlArgs.set([ "useApp",         "true"           ]);
// controlArgs.set([ "installApp",     "addLink"      ]);
// controlArgs.set([ "showTitle",      "false"          ]);
// controlArgs.set([ "appLauncher",    "true"         ]);
// controlArgs.set([ "tls",            "true"           ]);
// controlArgs.set([ "wsurl",          "ws[s]://addr[:port][/resource]"]);
```

3. Uncomment the corresponding controlArgs.set line by removing the // from the beginning of the line. Then edit the value, as desired. For example:

```
controlArgs.set([ "user",           "johng"      ]);
controlArgs.set([ "embed",          "true"          ]);
```

4. To specify startup parameters not listed, add controlArgs.set() for each parameter. For example:

```
controlArgs.set([ "parameter",          "true"      ]);
```

5. Save the page.

Changing the Default Logon HTML Page

Administrators can change the default document that loads when users browse to http[s]://[address][:port]/ to something other than logon.html by specifying the name of the document in the **DefaultDocument** property in **HostProperties.xml**.

To change the default logon HTML page

1. Create a copy of logon.html in the C:\Program Files\GraphOn\GO-Global\Web directory and rename it. (E.g., logon2.html)
2. Edit the new HTML page and configure the parameters as needed.
3. Stop the **Application Publishing Service**.
4. From the C:\ProgramData\GraphOn\GO-Global directory, open **HostProperties.xml** in WordPad.

5. Locate the **DefaultDocument** property and change the value from *logon.html* to the new HTML filename. (E.g., logon2.html)
6. Save **HostProperties.xml**.
7. Start the **Application Publishing Service**.

Specifying URL Parameters

Startup parameters can also be specified by appending them to the URL.

To specify URL parameters

1. In the web browser's Location box, type http:// followed by the host name and the AppController directory.
   For example, **http://hostname/goglobal/**
2. Append a question mark (**?**) to the URL followed by the desired parameter.
   For example, **http://hostname/goglobal/?user=user1**
3. Append an ampersand (**&**) to the URL to specify additional parameters.
   For example,
   http://hostname/goglobal/?user=user1&password=password1& app=wordpad

Connecting with WebSockets

When users connect to GO-Global Hosts from a browser or via an internet gateway such as a reverse proxy, GO-Global must tunnel its RXP protocol over WebSocket connections. For example, when users connect to a GO-Global Host from a browser, the GO-Global Web App connects using a WebSocket. In the default configuration, connections from three different programs are required to start a session:

1. The browser opens an HTTP or HTTPS connection and downloads the Web App and its supporting HTML and JavaScript files.
2. The Web App opens a WebSocket (**ws**) or WebSocket Secure (**wss**) connection and orchestrates the installation (if necessary) and starting of AppController.
3. AppController opens an RXP or RXPS connection and displays the session's applications.

By default, the Web App and AppController derive their connection parameters (**protocol**, **address**, and **port**) from the browser's URL as follows:

1. The Web App and AppController connect to the address specified in the browser's URL.
2. If the browser's URL specifies secure HTTPS, the Web App and AppController connect using their secure protocols (**wss** and **rxps**).
3. Alternatively, if the browser's URL specifies unsecure HTTP, the Web App and AppController connect using their unsecure protocols (**ws** and **rxp**).
4. The Web App connects to the port specified by the browser's URL (port 443 for HTTPS and port 80 for HTTP, by default). AppController connects to its default port (491).

The following table shows some examples:

	Browser			Web App			AppController		
URL	**prtcl**	**address**	**port**	**prtcl**	**address**	**port**	**prtcl**	**address**	**port**
http://url.addr	http	url.addr	80	ws	url.addr	80	rxp	url.addr	80
http://url.addr:491	http	url.addr	491	ws	url.addr	491	rxp	url.addr	491
https://url.addr	https	url.addr	443	wss	url.addr	443	rxps	url.addr	443
https://url.addr:491	https	url.addr	491	wss	url.addr	491	rxps	url.addr	491
http://url.addr/?host=host_addr	http	url.addr	80	ws	host_addr	80	rxp	host_addr	80
http://url.addr/?port=491	http	url.addr	80	ws	url.addr	491	rxp	url.addr	491

In some environments, it is necessary to have the Web App and AppController use different connection parameters than those that are derived from the browser's URL. For example, when the target endpoint *only* accepts HTTP/HTTPS connections (e.g., when a reverse proxy is used), or when users connect via a browser and either the Web App or AppController need to connect to a different endpoint (address and/or port) than the browser.

In these situations, administrators can specify the connection parameters that the Web App and AppController use by specifying a WebSocket URL via the **wsurl** parameter. When this parameter is specified, both the Web App and AppController establish WebSocket connections to the specified endpoint.

WebSocket URLs have the following format: **[protocol]://[address]:[port]/[resource]**
These parameters specify, respectively, the protocol, address, port, and resource of the host service.

The following table shows some examples of how the **wsurl** parameter may be used:

	Browser			Web App			AppController		
URL	**prtcl**	**address**	**port**	**prtcl**	**address**	**port**	**prtcl**	**address**	**port**
***http://url.addr?host=host_addr&port=491 &wsurl=**ws://wsurl_addr/**	http	url.addr	80	ws	wsurl_addr	491	ws	wsurl_addr	491
***http://url.addr?host=host_addr&port=491 &wsurl=**ws://**	http	url.addr	80	ws	host_addr	491	ws	host_addr	491
***http://url.addr:491/?wsurl=**ws://wsurl_addr/**	http	url.addr	491	ws	wsurl_addr	491	ws	wsurl_addr	491
***https://url.addr/?wsurl=**wss://wsurl_addr/**	https	url.addr	443	wss	wsurl_addr	443	wss	wsurl_addr	443

***** These URLs cannot be entered in the browser as-is. When the **wsurl** parameter is included in a URL, its value must be URL-encoded to ensure that the data is properly interpreted and safely transmitted to the web server.

URL-encoding is not required when the **wsurl** is specified in the logon.html page. For this and other reasons, GraphOn recommends specifying the **wsurl** in the logon.html instead of in the URL. For more information, see Modifying the Logon HTML Page.

.

When the **wsurl** is included in the URL, an online tool can be used to perform the encoding. For example, if the value of the **wsurl** parameter is **wss://host2.example.com:491**, entering this text in an online URL encoder results in the following conversion: **wss%3A%2F%2Fhost2.example.com%3A491**.

This converted text can then be added to the URL. For example:
https://host1.example.com/?wsurl=**wss%3A%2F%2Fhost2.example.com%3A491**

WebSocket Considerations

- If the URL starts with https://, the WebSocket protocol must be **wss**. Otherwise, it must be **ws**.

- If the **-h/host** parameter is specified, the address specified by the **-h/host** parameter is used and the **address** specified in the WebSocket URL is ignored. In this case, the address may be omitted from the WebSocket URL.
  For example, **https://host1.domain.com/?useApp=true&wsurl=wss://**

- If the **-hp/port** parameter is specified, the port specified by the **-hp/port** parameter is used and the **port** specified (either implicitly, by the protocol, or explicitly, after a colon) by the WebSocket URL is ignored.

- The **resource** parameter specifies the name of the endpoint of the GO-Global host or farm when a WAF or reverse proxy is used to route incoming connections to multiple web applications.

- When a WAF or reverse proxy with TLS enabled is used, the **-tls/tls** parameter must be specified.

- When TLS is terminated before the GO-Global Host (e.g., at a WAF or reverse proxy), the **Protocol** and **Encryption** values must be set to **TCP** and **None**, respectively, on the **Security** tab of the Admin Console's Host Options dialog.

- WebSocket support is not available from Linux clients.

- For AppController on Windows and MacOS, the default port 491 will be used unless the port is appended to the **-wsurl** parameter or the **-hp** parameter is specified. If both the **-hp** parameter is specified, and a port is appended to the **-wsurl** parameter, the **-hp** parameter will be used.

URL Examples (URL-encoding is omitted for clarity)

http://host1.domain.com/?useApp=true&**wsurl=ws:**//host2.domain.com
(Unencrypted WebSocket)

https://host1.domain.com/?useApp=true&**tls=true&wsurl=wss:**//host2.domain.com
(Encrypted WebSocket)

http://loadbalancer1.domain.com/?useApp=true&**wsurl=ws:**//host2.domain.com
(Unencrypted WebSocket)

https://loadbalancer1.domain.com/?useApp=true&**tls=true&wsurl=wss:**//host2.domain.com
(Encrypted WebSocket, TLS terminated at the load balancer)

AppController Examples

Windows:

\AppController.exe" **-wsurl ws:**//hostname.domain.com
(Unencrypted WebSocket using default port 491)

\AppController.exe" **-wsurl wss:**//hostname.domain.com:443
(Encrypted WebSocket using port 443)

On MacOS:

./AppController **-wsurl ws:**//hostname.domain.com
(Unencrypted WebSocket using default port 491)

./AppController **-wsurl wss:**//hostname.domain.com:443
(Encrypted WebSocket using port 443)

Web Files

The GO-Global Host setup installs the GO-Global web files under C:\Program Files\GraphOn\GO-Global\Web. If Microsoft Internet Information Services (IIS) is detected during installation, a *goglobal* virtual directory is created in IIS that points to the GO-Global web files. If a different web server such as Apache will be used, administrators must manually host the GO-Global web folder contents on the specified web server.

Administrators can edit the HTML pages to modify default options. During installation, the initial web page is set to logon.html. When users browse to this page, GO-Global automatically detects the user's platform and browser and runs the appropriate client.

There are two versions of AppController for Windows: an **All Users** version, and a **Single User** version. The installer for **All Users** version (**AppController.AllUsers.exe**) installs AppController for all users who use the computer, but it can only be installed by users who have administrator rights on the computer. To install the All Users version, the parameter **?allusers=true** must be appended to the URL, as follows: **http://hostname/goglobal/?allusers=true**

The installer for the **Single User** version (**AppController.exe**) can be run by users who do not have administrator rights on the computer, but it is only installed for the user running the installer. If another user wishes to run AppController on the same computer, he or she will also have to run the installer for the Single User version of the app.

Installation of the Single User version of AppController may fail if normal users are prevented from installing software by local or group policy.

Creating a URL Alias

When an external web server such as IIS or Apache is used, administrators can personalize the logon URL (e.g., use **http://hostname/wilson** in place of **http://hostname/goglobal**) by creating an alias for the URL.

For more information, see the following articles:

IIS: https://support.microsoft.com/en-us/help/308150/how-to-create-a-virtual-directory-on-an-existing-web-site-to-a-folder

Apache: https://httpd.apache.org/docs/2.4/mod/mod_alias.html

Alternatively, when GO-Global's integrated web server is used, administrators can personalize the URL by simply specifying a different **Virtual directory** in the **Get Link** dialog and clicking **Set defaults**.

Resizing the Client Window

The command-line argument **-geometry** can be used to modify the size of the client window when the command-line argument **-f** is used. Without **-geometry** on the command-line, the client window will be maximized. When GO-Global is run in loose window mode, **-geometry** has no effect. To resize the client window, append **-geometry** to the executable, followed by the desired width and height.

For example, on Windows:
“C:\Program Files\GraphOn\AppController\AppController.exe”
-f -geometry 800x600

On Linux:
./AppController -h 196.125.010.222 -f -geometry 800x600

On macOS:
./AppController -h 196.125.010.222 -f -geometry 800x600

Modifying the Session Window of the Web App

Users can define the size of the Web App’s session window by adding the height and width parameters to the logon URL. Add **width=x&height=y** to the URL, where x is the window width and y is the window height, in pixels.

In the following example, the session width is set to 600 pixels and the session height is set to 400 pixels:
http://hostname/goglobal/?useApp=false&**height=400&width=600**

Users can also define the size of the Web App’s session window using percentages. Add width=xx%25&height=yy%25 to the URL, where xx sets the percentage session width of the window width and yy sets the percentage session height of the window height. (%25 is the URL encoded symbol for %.)

In the following example, the session width is set to 95% of the window width and the session height is set to 75% of the window height:
http://hostname/goglobal/?useApp=false&**width=95%25&height=75%25**

Uninstalling AppController

Instructions for uninstalling AppController depend on the platform and browser.

To uninstall AppController on Windows

1. Open Control Panel.
2. Double-click **Programs and Features**.
3. Select **AppController**.
4. Click **Uninstall.**
5. Click **Uninstall**.

If users experience slow scrolling with GO-Global, try disabling the smooth scrolling option on the host in Internet Options or the browser's settings.

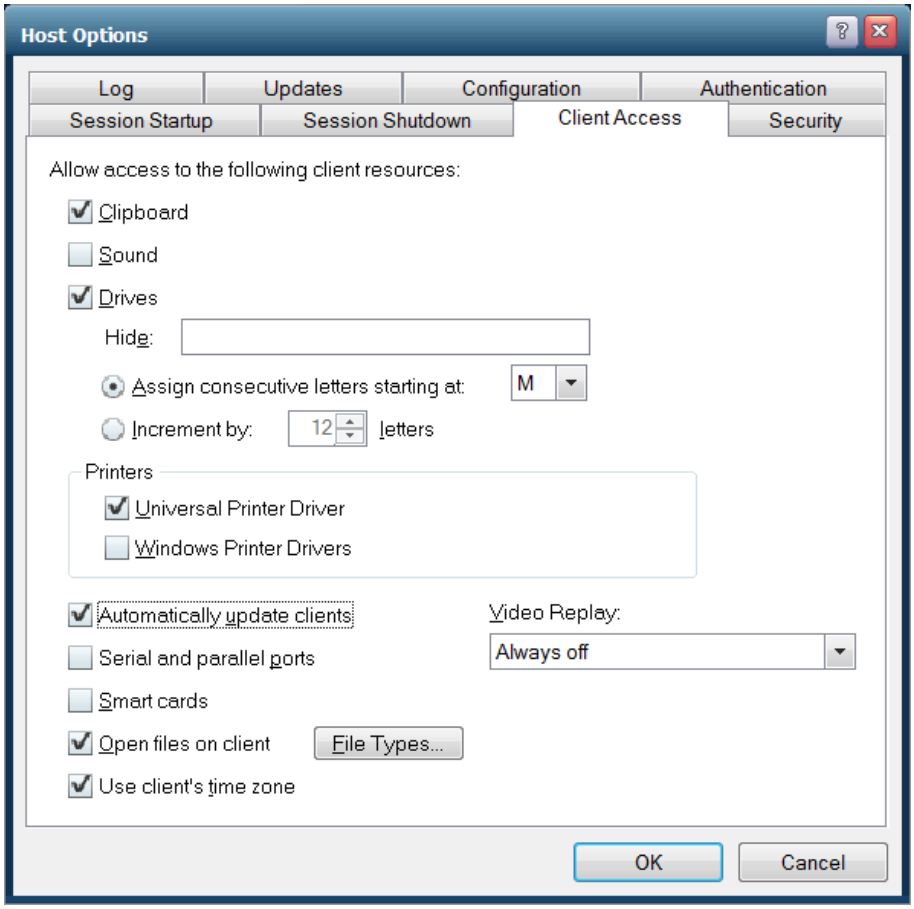
Automatic Client Updates

Administrators can configure GO-Global to automatically update the GO-Global Client when users connect to a GO-Global Host that is running a newer version.

To enable automatic client updates

1. Install AppController. (The Automatic client update feature is only available for Windows computers.)
2. From the Admin Console, click Tools | Host Options.
3. Click the **Client Access** tab.
4. Enable **Automatically update clients**.
5. Click **OK**.

The Automatic Client Update feature requires GO-Global's Web component to be installed on the computer together with GO-Global's Host component. If the Web component is not installed, re-run the GO-Global Host installer, click **Customize**, check **Web**, click **OK**, then **Install**.



Mac and Linux users can download the updated version of GO-Global by browsing to the host (e.g., **http://hostname/goglobal/**) and installing AppController.

The All Users and Single User versions of AppController upgrade the client differently. The **All Users** client installs and uses the AppController Update Service to perform the upgrade, whereas the **Single User** client performs the upgrade without the service. The Single User Automatic Client Update feature is only supported with version 6.1 and later; it is not supported when upgrading to version 6.1 or later from earlier versions of the product.

When **Automatically update clients** is selected in the Admin Console and a user signs in to the host from a Windows computer, GO-Global compares the version of AppController installed on the client computer to the version in the GO-Global\Web\Clients directory on the Host. If the client installer on the host is newer, GO-Global copies the installer to a temporary directory on the client computer. Then, when GO-Global closes, the new version is installed so it can be used in subsequent GO-Global sessions. Users will be updated on the screen when the new updates have finished installing.

In summary, a new version of GO-Global will be installed when the following conditions are met:

- **Automatically update clients** is enabled in the Admin Console
- A newer version of the client is available in the GO-Global\Web\Clients directory on the host
- The new client installer has been downloaded to the client computer
- The user has signed out of his or her GO-Global Client session

The default location for the Updates folder is C:\Program Files\GraphOn\AppController\Updates which is defined in the registry key: HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\AppController\Updates.

CHAPTER V

Administering User Accounts

5

Administering User Accounts

To access applications on a GO-Global Host, clients must sign in to the host machine. When users start a GO-Global client, they are prompted for their user name, password, and the name of the host they wish to access. This information is optionally encrypted and passed to the Application Publishing Service running on the GO-Global Host. The Application Publishing Service then performs the logon operation using standard multi-user features of Windows.

When a user signs in to a host and a domain is not specified, the GO-Global Host first attempts to authenticate the account on the local machine, followed by the machine's domain, and lastly the trusted domains. Users can override this default behavior and specify a domain by typing the domain name followed by a backslash (\) and their network user name in the **User name** box of the **Sign In** dialog. For example, NORTH\johng.

When a local user name on the GO-Global Host is the same user name as a domain account, each with a different password, GO-Global treats them as two separate accounts. Consider, for example, the following scenario:

- A local account on the GO-Global Host **johng** with a password of **local123**
- A domain account **johng** with a password of **domain123**

When typing user name, **johng** with the password **local123** in the Sign In dialog, the account will authenticate on the local GO-Global Host. When typing **johng** with the password **domain123** in the Sign In dialog, GO-Global does not attempt to authenticate on the domain, but fails with an invalid user name or password. You must specify the domain name in the **User name** field in the Sign In dialog. For example, NORTH\johng.

After a user signs in, GO-Global relies on the host's operating system to provide the security necessary to run applications safely in a multi-user environment. Applications run in the security context of the client user to ensure private sessions. Access to all machines and network resources is governed by the operating system and the rights that have been granted to individual user's sessions.

Users must be able to log on interactively (locally) on the GO-Global Host. Assign local logon rights to users in Local Security Policy, Domain Security Policy, and Domain Controller Security Policy.

This chapter contains basic information regarding the administration of user accounts on the GO-Global Host. For more detailed information, please consult Windows Help, accessible from the Start menu.

Setting Up User Profiles

Most Windows applications store user specific settings and files under the user's Windows profile. By default, Windows creates a local profile for each user that logs on to a system. A local profile is specific to a given computer and will not work well if you are running multiple GO-Global Hosts. If you are running a multi-host environment, you should set up roaming user profiles. A roaming profile is stored centrally and can be accessed from any networked computer for which that profile is valid. When a user with a roaming profile logs on to any networked computer, the desktop will appear exactly as the user left it the last time he or she logged off. For multi-host environments, working with roaming profiles is the only way to ensure that user specific settings are available to the user at all times.

A profile is only valid on the platform for which it was created. For example, a Windows Server 2016 profile can only be used on a Windows Server 2016 computer.

Setting File Permissions

As the system administrator, you may need to restrict user access to certain files and resources. Keep in mind that there are multiple users accessing the host. Particularly in a load-balanced server environment, we recommend write-protecting system and application folders so that users are unable to save files on a local GO-Global Host. Otherwise, the next time a user logs on to GO-Global and is routed to a different server, the files and folders will be inaccessible.

You must use Windows Explorer to set the permissions for files on the server. By setting file permissions, you can restrict user access to applications, printers, and folders.

While in Windows Explorer, choose the **Help** button or press **F1** for more information on setting file permissions.

Setting up a Network Printer

As the administrator, you can set up network printers for use by GO-Global clients. You must first create a port on the GO-Global Host that connects directly to the host and then install the printer locally. This provides direct access to the printer.

To add a port to the GO-Global Host

1. Click Start | Settings | Printers.
2. Double-click **Add Printer**.
3. Select local printer, then click **Next**.
4. Click Create a new port and select **Standard TCP/IP Port** as the type. Click **Next**.
5. Type the printer's IP address, as prompted by the printer wizard.
6. Select the printer manufacturer on the left and the printer model on the right, or click **Have Disk**.
7. Follow the directions provided by the wizard to install the proper printer.

CHAPTER VI

GO-Global Admin Console

6

GO-Global Admin Console

The Admin Console allows you to administer, monitor, and control client access to the GO-Global Host. The Admin Console displays a list of the users signed in to a GO-Global Host, along with the applications users are running. Through the Admin Console, you can perform a variety of administrative tasks, such as adding and removing applications, terminating user sessions, and ending processes running on the host.

To access the Admin Console

Double-click the **GO-Global Admin Console** icon on the desktop.

–or–

1. Click the **Start** button on the Windows taskbar.
2. Click GraphOn GO-Global | Admin Console.

The left panel of the Admin Console lists the hosts on the network running the Application Publishing Service. By default, the Admin Console displays information for the host running on your machine. To connect to other hosts and view information about them, click the host name from the list of GO-Global Hosts.

If the host's icon is colored red, the host is no longer running the Application Publishing Service or it has been turned off. In either case, the administrator is unable to access that host from the Admin Console.

Click the **All Hosts** icon in the left panel of the Admin Console to view a list of all active sessions on the network. This allows you to view active GO-Global sessions without connecting to individual hosts. This is also helpful for locating a particular session's host.

You must belong to the Administrators group on each GO-Global Host in order to access that host from the Admin Console. Without administrative rights on a host, you will be unable to add applications and terminate processes, etc.

Managing Sessions and Processes

Administrators can encrypt and shadow sessions and terminate processes and sessions through the Admin Console, as described below.

Terminating a Session

When terminating a user's session, all GO-Global-deployed applications that the user is running will be terminated, and the user will be logged off the GO-Global Host.

To terminate a session

1. Click the **Sessions** tab.
2. From the **Sessions Name** column, select the session(s) you would like to terminate.
3. Click Tools | Sessions | Terminate.

Ending a Process

A process is any action taking place on a GO-Global Host that is initiated by a client. A client running an application, for example, is a process. Each running application is assigned a unique name and process ID in the Windows Task Manager. These process names and IDs are duplicated in the Admin Console. Administrators can end any process from the Admin Console.

To end a process

1. Click the **Processes** tab.
2. Select the process or processes you would like to end.
3. Click Tools | Processes | Terminate.

Terminating a session or ending a process without giving users a chance to close their application can result in the loss of data.

Shadowing a Session

Session shadowing allows multiple users to view and control a single session and its applications. This allows technical support and system administrators to provide remote assistance to customers and users. Session shadowing may also be used for live collaboration.

Only administrators can connect to running GO-Global sessions, but only with permission from the session's user.

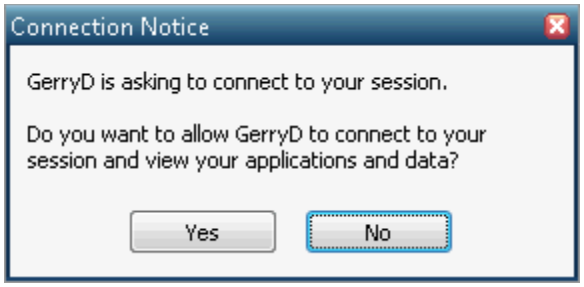
To shadow a session

1. Click the **Sessions** tab.
2. From the **Sessions Name** column, select the session(s) you would like to shadow.
3. Click Tools | Sessions | Connect.

   –or–

   From the **Sessions Name** column, right-click the session you would like to shadow.

After the session is selected, a message such as the following is displayed to the session's user, where GerryD is the administrator's user name:



If the user clicks **Yes** and permits access to his or her session, the connection is made immediately and the GO-Global client session opens in a new frame window.

If the user clicks **No** and denies access, the following message is displayed on the host:

Session shadowing will also be denied when the session is disconnected, when the session is about to be or is in the process of being shut down, or when the user fails to respond within one minute. Connection is also denied in the event of a GO-Global communication failure.

The **Sessions** tab of the Admin Console displays the number of clients connected to a session. 2 or higher in the **Connected Clients** column indicates that the session is being shadowed. Disconnected sessions have 0 connected clients. To disconnect from a session and end session shadowing, simply close the frame window where the session is displayed.

When a GO-Global session is being shadowed, the host's cursor remains on the client until that session is closed. It does not go away even when the session is no longer being shadowed.

Sending Messages to Users

The Administrator Messages feature allows administrators to send messages to connected users and alert them of system maintenance and other events. Administrators can display messages to select users, to all users running on a selected host, or to all users on all hosts.

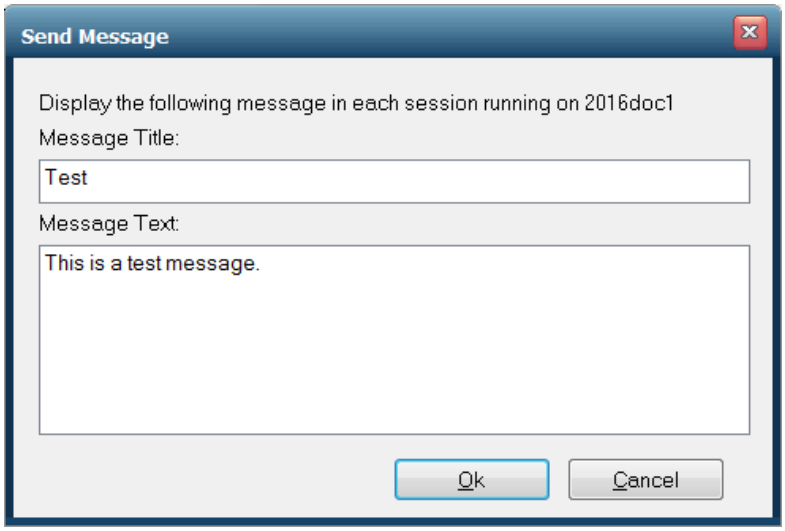
To send a message to select user(s)

1. In the Admin Console, click the **Sessions** tab.
2. Select one or more user sessions.
3. Right-click and select **Send Message** or click Tools | Send Message.
4. Type a title in the **Message Title** box.
5. Type a message in the **Message Text** box.
6. Click **OK**.

After clicking **OK**, the message is displayed immediately to the user.

To send a message to all users on a host

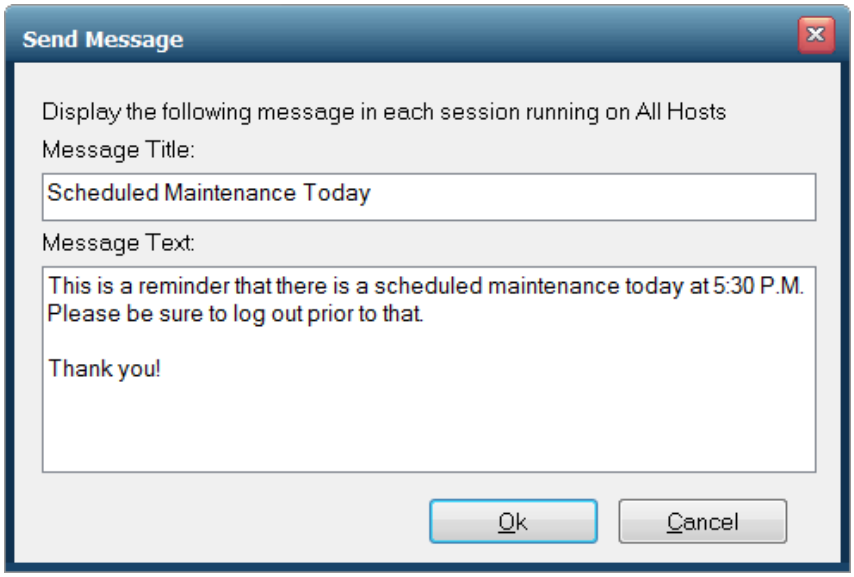
1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Right-click and select **Send Message** or click Tools | Send Message.
3. Type a title in the **Message Title** box.
4. Type a message in the **Message Text** box.
5. Click **OK**.



Users who are not connected to their sessions will see the message when they reconnect to their sessions.

To send a message to all users on all hosts

1. In the Admin Console, select the **All Hosts** icon.
2. Right-click and select **Send Message** or click Tools | Send Message.
3. Type a title in the **Message Title** box.
4. Type a message in the **Message Text** box.
5. Click **OK**.



Managing GO-Global Licenses

The Admin Console lists all the GO-Global licenses that are available to a host and displays each license's Product Code, number of seats, expiration date, status, etc. GO-Global warns administrators when expiration dates are approaching and when licenses and Support contracts have expired.

To view licenses

1. From the Admin Console, select the appropriate host from the list of GO-Global Hosts.
2. Click the **Licenses** tab.

For each license, the following information is displayed:

Column	Description
Status	A license status can be listed as *Active*, *Expired*, *Expires soon*, *Grace, Old version*, *Revoked,* and *Trial.*
License Master ID	GraphOn's unique, human-friendly identifier of the license (For example, LIC-122689)
Product Code:	28-digit alphanumeric code that appears in the license file, uniquely identifies the license, and is used for secure transactions (For example, 171205182219607CJs4ndny07Auu)
License ID	Unique, alphanumeric identifier of an on-premises license file (For example, GHPc7u with license file *GHPc7u.lic*). (Not used for cloud licenses.)
Seats	The maximum number of concurrent users the license allows.
Expiration Date	The date the license (e.g., a trial license or subscription) expires. When a license does not expire, the expiration date is listed as "perpetual."
Support Expiration Date	The date the Support contract expires.
Version	The license's GO-Global version number (e.g., 5.0 and 6.0)
License Server	The name of the license server that the host is using. If the host is using a cloud license, the License Server is cloud.graphon.com.

Depending on which column is selected, licenses are sorted alphanumerically in ascending order. Click the column header to sort in descending order.

At the bottom of the Licenses tab, GO-Global displays the number of **Total seats** for all the valid licenses listed for the selected computer. It also displays the number of **Seats in use**, which is the number of seats currently checked out from the licenses listed, and includes licenses that have been checked out from the selected computer and from any other GO-Global Host that is using the same license(s). If the host is configured to use a cloud license, **Reserved seats** is also listed. **Reserved seats** is the number of seats that will be available to the host if the host loses its connection to the Cloud License Service.

Customers with a valid GO-Global Support contract are able to receive technical support for issues that occur on the licensed host. When the Support contract has expired (as indicated in the **Support Expiration Date** column), only critical GO-Global Updates can be installed on the host. Non-critical GO-Global Updates cannot be installed, and customers are not eligible to request support. The frequency of expiration warnings varies depending on the type of license. You can opt to disable expiration warnings by checking **Don't display this message again**.

If a GO-Global Update was released after the Support contract on *any* of the licenses available to a GO-Global Host have expired, you must renew the Support contract in order to install the update on the host. If an update was released after the Support contract has expired on some, but *not all* licenses, you can either remove the license(s) with the expired Support contract, or you can renew the expired Support contract(s).

Contact your GO-Global reseller or sales@graphon.com to renew Support contracts.

If the expiration date of the Support contract for any license available to a GO-Global Host is earlier than the build date of the GO-Global Host, the **Application Publishing Service** will not run.

For on-premises trial licenses of GO-Global, the License Master ID, License ID, and the Support Expiration Date will be listed as *not applicable*. The **Expiration Date** column indicates the date that the trial will stop working. When a trial license status has *expired*, users are no longer able to run GO-Global on that computer. Extend the GO-Global trial license by contacting your GO-Global reseller or sales@graphon.com.

If a license is listed as *Revoked,* it is invalid, and must be removed from the system, and the Application Publishing Service must be restarted. Contact your GO-Global reseller or licenses@graphon.com for further assistance. If a license is listed as *Old version,* the version of the license is older than the license version required by the host. If it is the only license on the host, it will need to be upgraded. It does not need to be removed for other licenses to work.

To refresh the list of licenses, right-click and select **Refresh** or press the **F5** button on the keyboard.

In the event a cloud subscription license is not renewed before its expiration date, there is a grace period of usage following the expiration date. During the grace period, the license will continue to operate, allowing time for the customer to renew the license. At the end of the grace period, if the license has not been renewed, the status will change from *Grace* to *Expired*, and the license will stop working.

Session Reconnect

Session reconnect allows sessions to be maintained on a GO-Global Host without a client connection. If the client's connection to the host is lost, intentionally or unintentionally, the user's session and applications remain running on the GO-Global Host for the length of the session timeout specified in the Admin Console. Session reconnect allows users to return to their GO-Global session in the exact state they left it. Through the Program Window users can select to disconnect, rather than exit from GO-Global, and can return to their session as they left it — without having to shut down their open applications and running processes.

If the network connection is lost or if users unintentionally disconnect from GO-Global, their session state is preserved for the length of time specified in the Admin Console. After a user is authenticated through normal logon procedures, GO-Global determines if the user has an active session. If so, that session resumes and appears exactly as it did prior to disconnection. If not, a new session is started. Users are also able to disconnect from one client and reconnect to the session from another client.

When attempting to reconnect to a disconnected session, users are required to specify their logon credentials. After the host validates them, the host reconnects them to the disconnected session. If the session is hosted on a server that is part of a load-balanced configuration, the user is routed to his or her session without any indication that the session is on a load-balanced server. If Integrated Windows authentication is available, users are automatically re-authenticated and re-connected to their session.

Setting the Session Termination Option

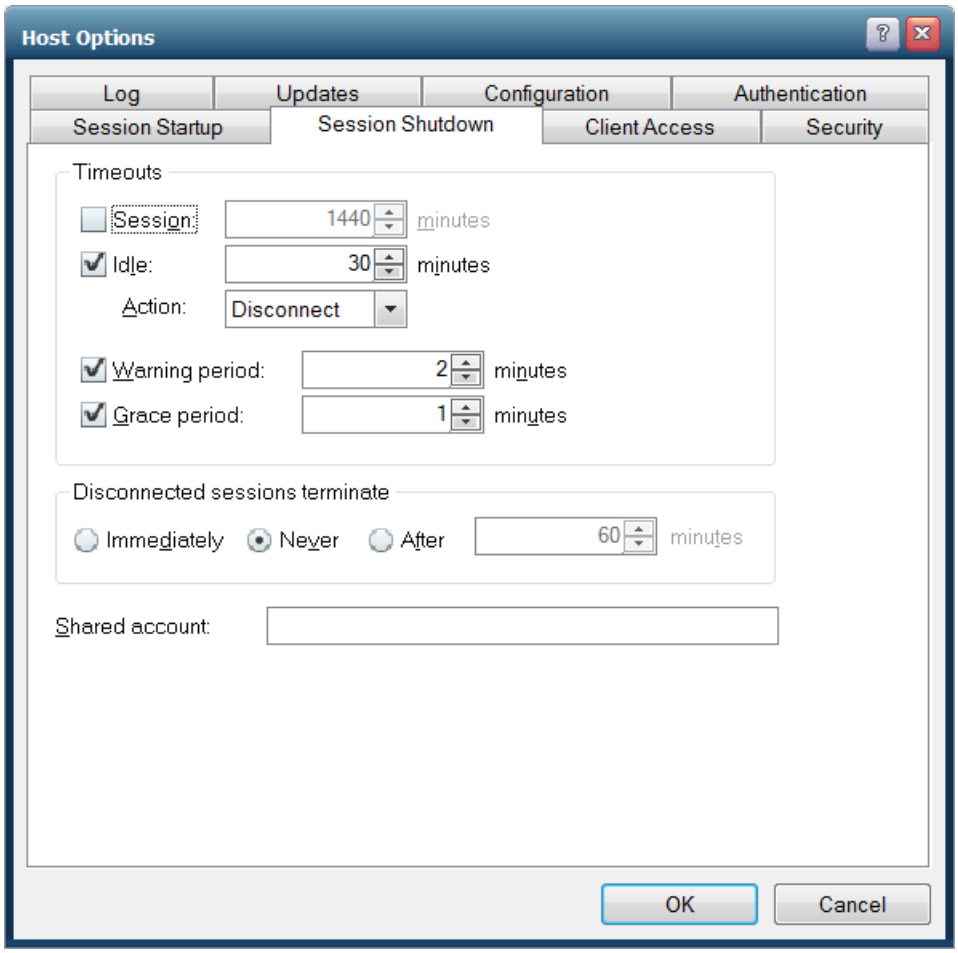
Administrators control how long client sessions and applications remain running on the GO-Global Host through the Admin Console's **Host Options** dialog.

- Select **Immediately** if you want client sessions to terminate as soon as the client disconnects.
- Select **Never** if you want sessions to terminate only when a user manually closes all applications running within a session or when an administrator manually terminates a session using the Admin Console. This is the default setting.
- Select **After __ minutes** to specify the number of minutes that a session will remain running after a client has disconnected from the session. Type the number of minutes in the edit field that a session should remain running after the client disconnects.

The **Sessions** tab of the Admin Console displays the number of clients connected to a session. Disconnected sessions have 0 connected clients.

To set the session termination option

1. From the Admin Console, click Tools | Host Options.
2. Click the Session Shutdown tab.
3. Select one of the following session termination options:
   Immediately
   Never
   After ___ minutes. In the edit box, type the number of minutes sessions should remain running after their clients disconnect.
4. Click **OK**.



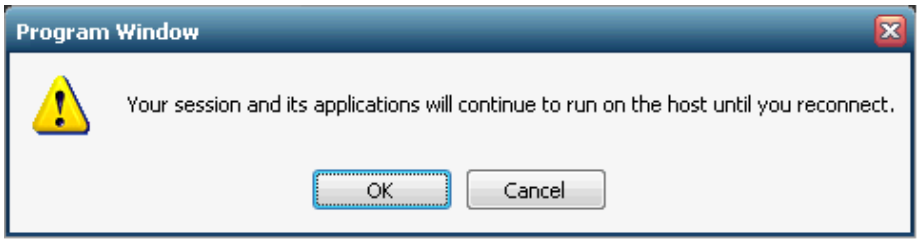
Disconnecting a Session

If sessions are set to never terminate or to terminate after a specified number of minutes, the Program Window's File menu includes a **Disconnect** option. If sessions are set to terminate immediately, the Disconnect option does not appear in the Program Window's File menu.

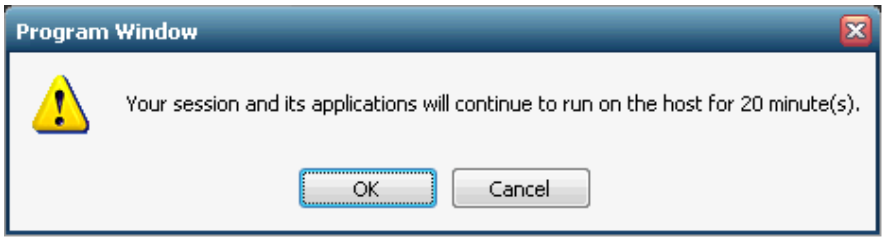
To disconnect a session

From the Program Window, click File | Disconnect.

With session termination set to **Never**, the following message is presented to the user upon disconnecting from GO-Global:



When sessions are set to terminate after a specified number of minutes (20 minutes, for example) a message such as the following is presented to the user upon disconnecting from GO-Global:



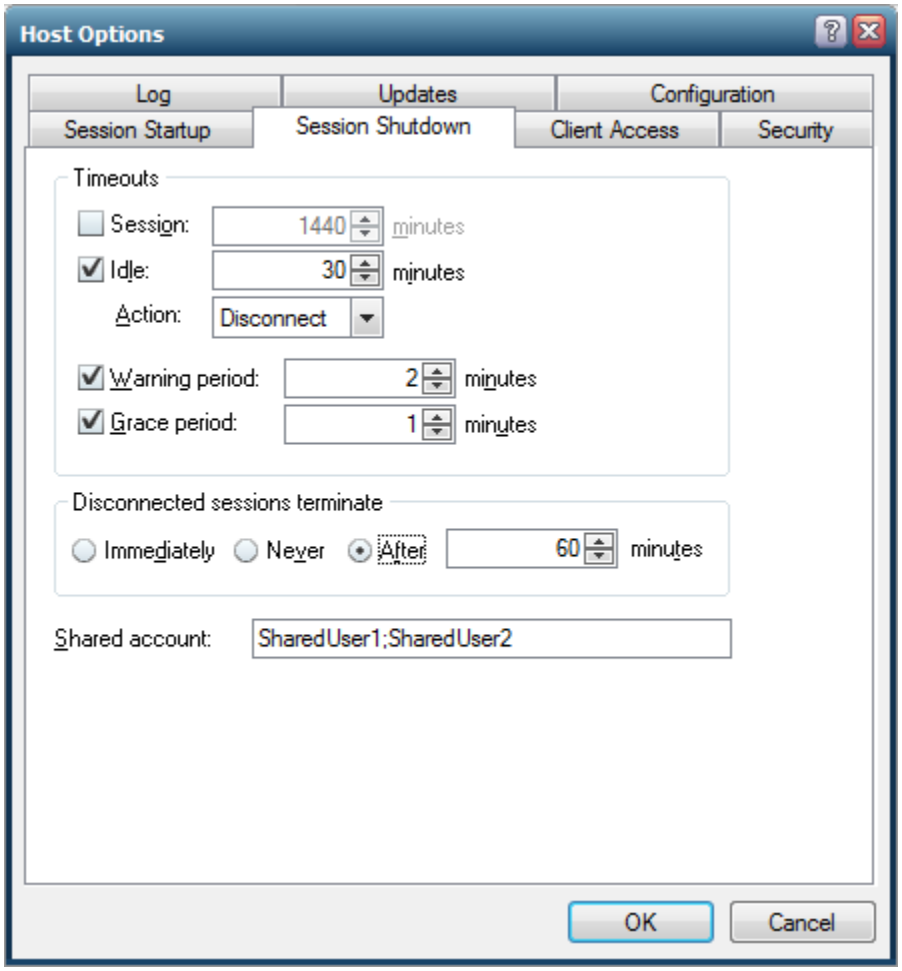
If a user attempts to disconnect from a session and already has a disconnected session, the following message appears:
You already have a session (session_name) that is disconnected. If you disconnect the current session, that previous session will be terminated.
Do you want to continue?

If the user clicks **Yes**, the disconnected session is terminated. If **No**, the user is returned to the running session.

When a user reconnects to a session, the -a and -r command-line arguments are ignored. In addition, when the user reconnects to a session from the same client computer, the -ac command-line argument is ignored.

Shared Account

A shared account should be specified when multiple users are using the same account for starting a GO-Global session. Users who sign in to GO-Global with a shared account cannot disconnect and then reconnect to GO-Global. This prevents a user from reconnecting to another user's session.



When logging on to a GO-Global Host with a shared account, the **Disconnected sessions terminate** option in the Admin Console is ignored, and the behavior is determined by the **SessionTimeoutBrokenConnection** property in the **HostProperties.xml** file. (HostProperties.xml is located in C:\ProgramData\GraphOn\GO-Global).

If the value of this property is set to 0, the session will terminate immediately. If the value is greater than zero, the session will be suspended and will remain running on the server for the number of minutes specified. In the latter case, only the user who started the session will be able to reconnect to the suspended session. By default, **SessionTimeoutBrokenConnection** is set to 0 minutes.

To specify a shared account

1. Click Tools | Host Options.
2. Click the **Session Shutdown** tab.
3. Type the user name of the shared account in the **Shared account** edit box. If multiple shared accounts are required, separate the user names of the accounts with semicolons.
4. Click **OK**.

Client Time Zone

By default, all GO-Global sessions are run in the time zone of the GO-Global Host machine. Administrators can opt to run GO-Global sessions in the time zone of the client computer by enabling the **Use client's time zone** option from the Admin Console.

To enable client time zone

1. Click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable **Use client's time zone**.
4. Click **OK**.

Client Clipboard

GO-Global allows client and host-based applications to exchange information using the clipboard. Users can cut and copy information from applications running on the client and paste it into applications running on a GO-Global Host, and vice versa. Clipboard support is disabled by default.

To enable client clipboard

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Clipboard** check box.
5. Click **OK**.

Client Sound

The GO-Global Host supports a virtual audio device that creates a private mixer for every GO-Global session. These components mix the audio played by applications running in the GO-Global session and encode it in Ogg Vorbis format. The host streams the Ogg Vorbis data to the client, and the client plays the audio.

To enable client sound

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Sound** check box.
5. Click **OK**.

The host computer does not need to have a sound card or speakers, but the Windows Audio service must be enabled on the host. AppController for Windows and macOS supports Client Sound. The client machine requires a sound card and speakers. Audio support is disabled by default.

Client Serial and Parallel Ports

GO-Global allows applications running on the host to access client machines' serial and parallel ports. Serial and parallel ports are disabled by default. Client serial and parallel port access is supported on Windows only.

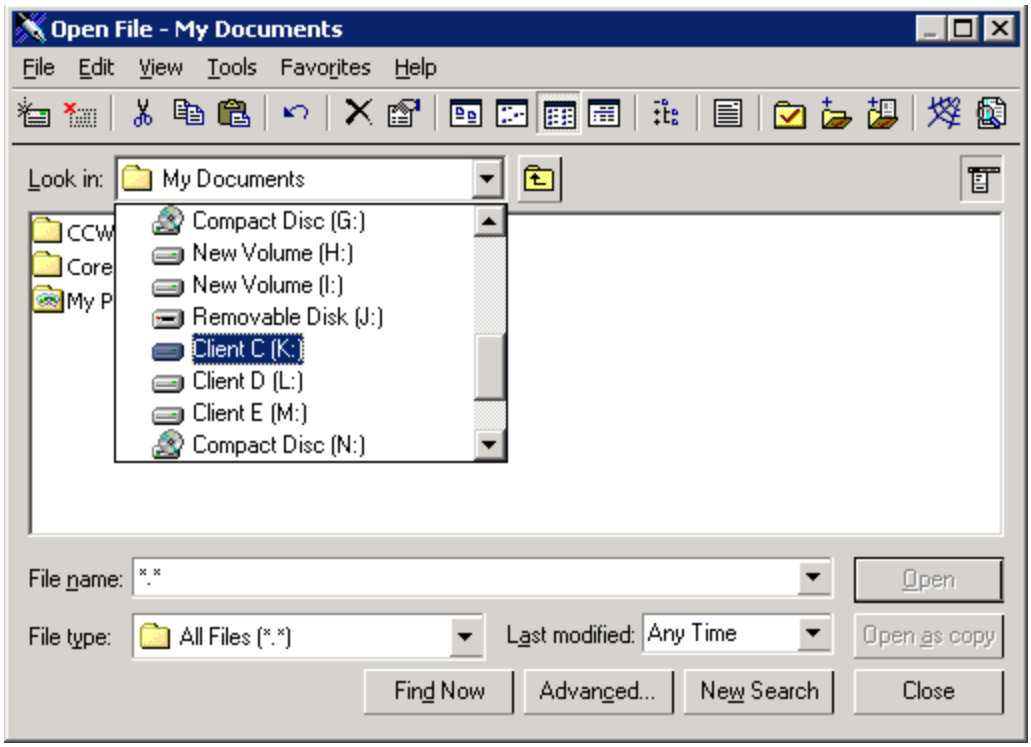
To enable serial and parallel ports

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Serial and Parallel Ports** check box.
5. Click **OK**.

Access to serial and parallel ports requires the loading of GO-Global libraries into session processes. This can affect the startup of a process, make some processes incompatible with GO-Global, or have fatal consequences during suspend/resume operations. For information on advanced configurations options, please consult the **Advanced Session Process Configuration** section in this guide.

Client File Access

GO-Global allows users to access files stored on the client computer and to save files locally. Client drives will be listed in the application's **Open** and **Save as** dialog boxes, and are designated with a Client prefix. For example, Client C (K:), Client D (L:).



The dialog boxes list both client and host drives. Support for client drives is disabled by default.

To enable support for client drives

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Drives** check box.
5. Click **OK**.

GO-Global allows users to access USB drives. Removable media such as floppy disks, CD ROMs, and DVD-ROMs are not supported as client drives.

Remapping Client Drives

When applications are run in GO-Global sessions with the Client Drives feature enabled, GO-Global must ensure there is a one-to-one mapping between drive letters and the drives of the client and host computers. If a drive on the client and a drive on the host are assigned the same drive letter, GO-Global must assign a new drive letter to one of the drives. Client drives can be remapped by either listing them sequentially starting at a given drive letter *or* incrementing their drive letters by a specified value.

To list client drives sequentially starting at a given drive letter

1. From the Admin Console, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. Click **Assign consecutive letters starting at: ___**.
5. In the edit field, type the drive letter that should start the sequence.
6. Click **OK**.

For example, if a client computer has C, D, G, and H drives, and the starting point is set to drive letter M, the client's drives will be remapped respectively to M, N, O, and P. If a drive letter is already assigned to a drive, the next available letter is used. In the example above, if the starting client drive letter is a letter at the end of the alphabet (Y, for example), it will map Y for C and Z for D. GO-Global will then go back through the alphabet and use X for G and W for H.

This feature is disabled by default. Once enabled, the default start drive letter is M.

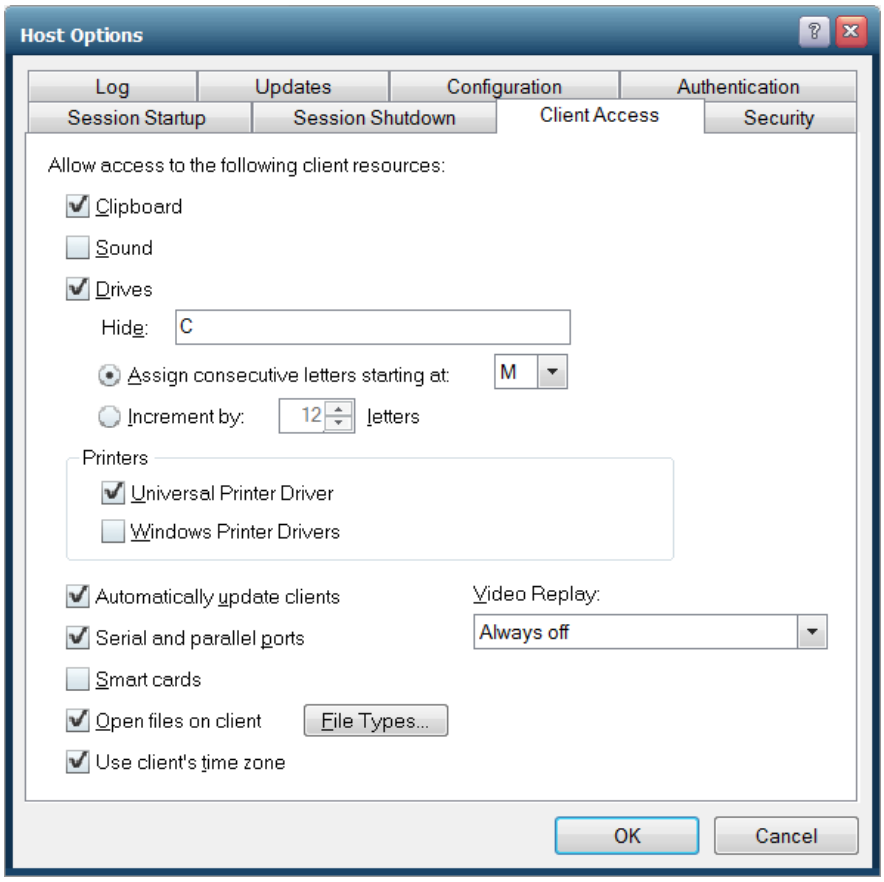
To increment client drive letters by a fixed value

1. From the Admin Console, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. Click **Increment by: ___ letters**.
5. In the edit field, type a number between 0 and 25 that will yield the desired offset.
6. Click **OK**.

For example, if the client computer has the same drives as above (C, D, G, and H), and the offset is 12, each of the client's drives will be incremented by 12 letters. The drives will be remapped respectively to M, O, P, and T. In the example above, when incrementing with a large number (22, for example), GO-Global will use Y and Z, then go back down the alphabet. Client drives C, D, G, and H would be remapped to Y, Z, V, and U respectively.

The default value for this setting is 12.

GO-Global does not map client drives A or B.



Hiding Client Drives

Through the Admin Console, administrators can hide client drives such as the client's operating system drive and CD ROM drive, making them inaccessible to the user through GO-Global.

To hide one or more client drives

1. From the Admin Console, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. In the **Hide** box, type the client drive letters you want to hide.
5. Click **OK**.

All client drives are mapped by default. Drives listed in the **Hide** box can be listed in any order. When hiding client drives on the Linux Client and the macOS App, the user's home directory is mapped, in addition to the Root. For example,
Client Home (N:)
Client Root (O:)

Hiding Host Drives

Microsoft's Group Policy Objects lets you hide specific host drives. For instructions, see http://support.microsoft.com/kb/231289. To hide host drives, the **Apply Group Policy** option must be enabled in the Admin Console's **Host Options** dialog. Click the **Session Startup** tab and click **Apply Group Policy**.

Video Replay

When Video Replay is enabled, GO-Global encodes videos and animations playing in GO-Global sessions in H.264 video format instead of GO-Global's RapidX Protocol, and sends the video data to the GO-Global client where it is decoded and displayed. This greatly improves the performance of video and animations playing in GO-Global sessions.

Encoding video in H.264 format is a CPU intensive operation, so GO-Global minimizes the area of the screen that is encoded in H.264 format. The GO-Global Display Driver monitors the display for areas where images are being frequently drawn to the same area of the screen and encodes only the bounding rectangle in H.264 format. The remaining area of the screen is encoded using RapidX Protocol.

Video Replay is disabled by default. Video Replay is only supported when AppController is run on Windows.

To enable Video Replay

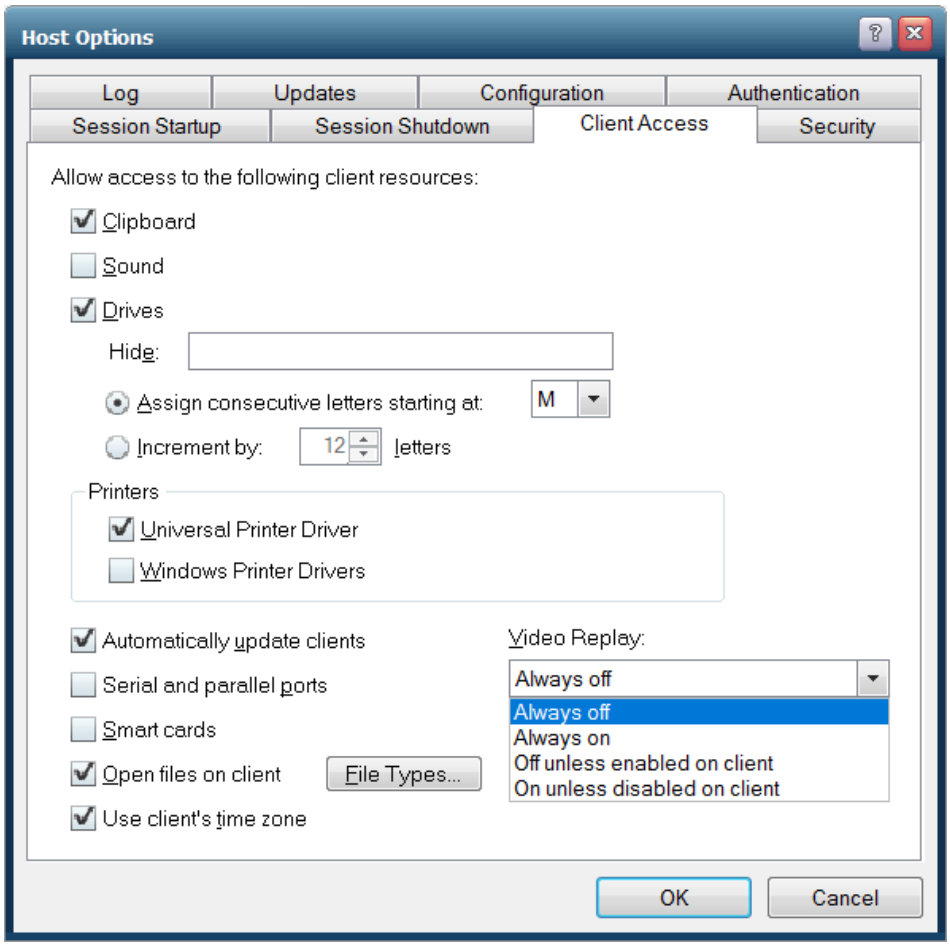
1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. From the **Video Replay** dropdown menu, click **Always on**.
5. Click **OK**.

By selecting **Off unless enabled on client**, administrators can disable Video Replay unless the command-line argument **–video** is appended to the shortcut or **video=1** is appended to the hyperlinks that open the logon HTML page. For example, http://hostname/goglobal/?**video=1**

Conversely, by selecting **On unless disabled on client**, administrators can enable Video Replay unless **–novideo** is appended to the shortcut or **video=0** is appended to the hyperlink. For example, http://hostname/goglobal/?**video=0**

By selecting **Off unless enabled on client**, administrators can disable Video Replay unless the command-line argument **–video** is appended to the shortcut or **video=1** is appended to the hyperlinks that open the logon HTML page. For example, http://hostname/goglobal/?**video=1**

Conversely, by selecting **On unless disabled on client**, administrators can enable Video Replay unless **–novideo** is appended to the shortcut or **video=0** is appended to the hyperlink. For example, http://hostname/goglobal/?**video=0**



File Open Redirection

File Open Redirection complements the Client Drives feature, which enables users to open files on the client in applications running on the host. File Open Redirection enables users to open files that are on the host or client in applications running on the client.

GO-Global supports redirecting file *open* operations to the client computer, but does not support redirection of file *creation* operations to the client. For example, if an application running in a GO-Global session uses Excel to generate a spreadsheet, Excel must be installed on the host computer.

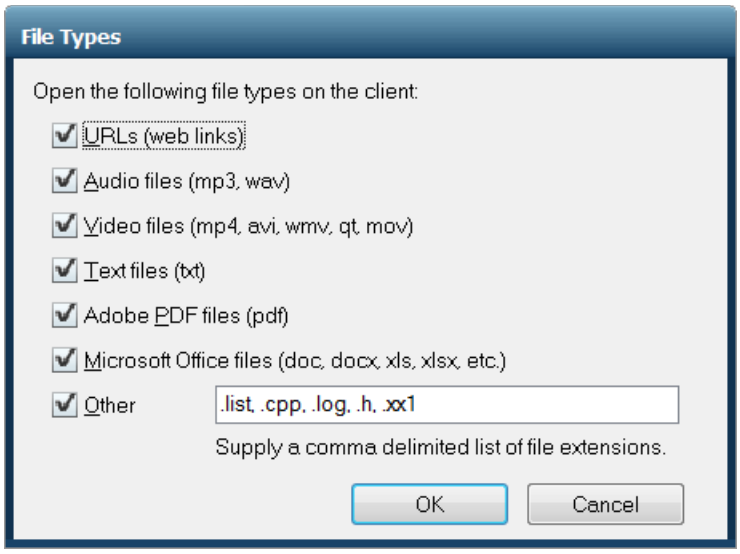
Opening Files on the Client

The **Open files on client** option allows users to open files that are on the host or client in applications running on the client. For example, if a user is running an application through GO-Global and opens a file format not supported by the application, GO-Global will automatically download the file to the user's computer and open the file using an application on the user's computer that supports the file format.

The **Open files on client** option is enabled by default for audio files, video files, text files, PDFs, and Microsoft Office files. The feature is supported when AppController is run on Windows and macOS.

To disable Open files on client

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Disable **Open files on client**.
5. Click **OK**.



URL Redirection

URL redirection allows GO-Global users to click web links that open in the default browser on the user's client rather than the default browser on the host. This enables users to efficiently access web content and videos running in GO-Global sessions. URL redirection is enabled by default.

To disable URL Redirection

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **File Types** button.
5. Disable **URLs (web links**).
6. Click **OK**.

Smart Card Document Signing

GO-Global provides support for smart card document signing on Windows only. Smart card document signing is enabled by granting applications access to client-attached smart cards via the **Smart cards** option on the **Client Access** tab of the Admin Console's **Host Options** dialog.

To enable smart card document signing

1. Start the Admin Console.
2. Click Tools | Host Options | Client Access.
3. Click **Smart cards.**
4. Click **OK**.

GO-Global supports the following smart card readers: Aladdin, SafeSign, and SafeNet. For support of smart card document signing, one of these readers must be installed on the client.

To configure Aladdin Smart Card

1. Enable **Smart cards**, as described above.

2. Install Aladdin software on the client and the host. (SafeNetAuthenticationClient-x32-x64-8.1-SP2.exe.)

3. Add the following registry settings on the GO-Global Host:

HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\AppServer]
"**SmartCardOptimization**"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\ScCertProp]
"**Enabled**"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\CertStore]
"**PropagateUserCertificates**"=dword:00000000
"**PropagateCACertificates**"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\System\Run\LocalMachine]
"**SafeNetCertMngr**"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\System\Processes]
"**SACMonitor.exe**"=dword:00000000

4. Reboot the GO-Global Host.

To configure SafeSign smart card

1. Enable **Smart cards**, as described above.

2. Install **SafeSign** software on the client and the host:
   On 32-bit operating systems: gemccid_en-us_32.msi
   On 64-bit operating systems: gemccid_en-us_64.msi
   -or-
   On 32-bit operating systems: SafeSign-Identity-Client-3.0.45-admin-eval.exe
   On 64-bit operating systems: SafeSign-Identity-Client-x64-3.0.45-admin-eval.exe
   (Be sure to install the admin eval package, and not the user eval package.)

3. Reboot the GO-Global Host.

To configure SafeNet smart card

1. Enable **Smart cards**, as described above.

2. Install **SafeNet** software on the client and the host:
   On 32-bit operating systems: SafeNet High Assurance Client (x32) 2.7.005.exe
   On 64-bit operating systems: SafeNet High Assurance Client (x64) 2.7.005.exe

3. Add these registry settings on the GO-Global Host:

[HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\AppServer]
"**SmartCardOptimization**"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\ScCertProp]
"**Enabled**"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SHAC\CertStore]
"**PropagateUserCertificates**"=dword:00000000
"**PropagateCACertificates**"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\System\Run\LocalMachine]
"**SHACMonitor**"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\System\Processes]
"**SHACMonitor.exe**"=dword:00000000

4. Reboot the host.

Monitoring Host Activity

The Admin Console displays information about host activity and processes taking place on the host. Administrators can use this information to determine which applications are no longer being used and whether additional hosts are required, for example.

Viewing Session Information

The Admin Console displays the following session information:

Column	Displays the...
Session Name	Unique identifier assigned to a session.
User	Network user name of the user accessing applications on the host.
Connected Clients	Number of clients connected to a session. 0 indicates that no one is connected to the session (the client has disconnected). 1 indicates that the client is connected and the session is active. 2 or higher indicates that the session is being shadowed.
IP Address	IP address of the client computer from which the user is accessing the host. (Each computer on a network has a unique IP address.)
Startup Time	Date and time the user started the application.
Applications	Number of applications the user is accessing.

To view session information

Click the **Sessions** tab.

Click the **All Hosts** icon from the left panel of the Admin Console to view a list of all active sessions on the network. This allows you to view active GO-Global sessions without connecting to individual hosts.

Viewing Process Information

A process refers to the specific application that a user is running from the host. The Admin Console displays the following process information:

Column	Displays the...
Name	Name of the application running on the host.
User	Network user name of the user accessing the application.
Startup Time	Date and time the user started the application.
Process ID	Process identification number assigned by the host's operating system. (The number for each running application matches the process identification number displayed in the Windows Task Manager.)

To view process information

Click the **Processes** tab.

Searching Sessions and Processes

The Admin Console's Search feature allows administrators to quickly locate the session and processes of a specific user. This is particularly helpful with large deployments, as it eliminates the need for the Admin Console to simultaneously display all sessions and processes that are running on a farm of GO-Global Hosts.

To search process and session information, enter a query in the search bar at the bottom of the Admin Console's right pane, then click the **Search** button or press the **F5** key.

When the **Sessions** tab is selected, the following session information can be searched:

- User
- Session ID
- IP address

When the **Processes** tab is selected, the following process information can be searched:

- Name
- User
- Process ID
- Session ID

Refreshing the Admin Console

You can manually update the sessions, processes, and applications information displayed in the Admin Console or you can set it to update automatically. If the Admin Console is set to update automatically, you can still update it manually at any time.

To refresh the Admin Console

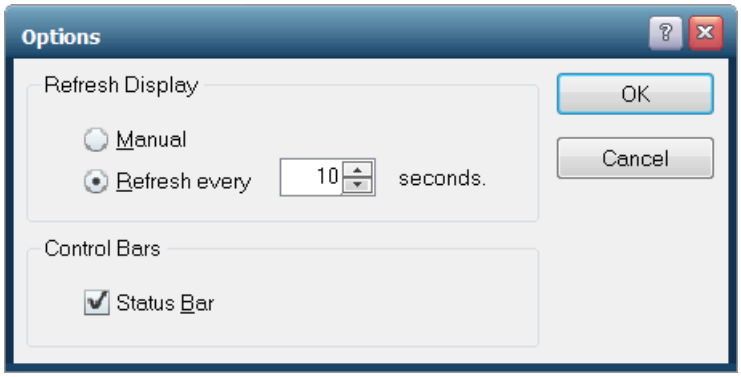
Click View | Refresh.

Setting the Refresh Rate

You can set the sessions, processes, and applications tabs of the Admin Console to manually refresh or to automatically refresh at a specified frequency.

To set the refresh rate to allow only manual refresh

1. Click View | Options.
2. Click **Manual**.



To set the refresh rate to refresh automatically

1. Click View | Options.
2. Click the **Refresh every *x* seconds** option.
3. Type a value in the **seconds** box.

The Status Bar

The Status Bar is displayed at the bottom of the Admin Console window. The Status Bar provides brief descriptions of menu commands when the mouse pointer is placed over that item in the menu. The Status Bar indicates the name of the GO-Global Host currently being accessed, as well as the Mem usage and CPU utilization for that host, as calculated by the Windows Task Manager.

The last two items on the Status Bar, **Sessions** and **Procs** indicate the number of sessions and the number of processes running on the active GO-Global Host. If **All Hosts** is selected, the **Sessions** number will reflect all the sessions running on the network, and the **Procs** number will reflect all the processes on the network.

To turn the Status Bar on or off

1. Click View | Options.
2. Select or clear the **Status Bar** check box.

Setting the Broadcast Interval

You can modify how often host information is sent to the Admin Console by modifying the Broadcast Interval value. This value represents how many milliseconds elapse between broadcasts, affecting how often a host's CPU, MEM, Sessions, and Processes status bars are updated, and how long it will take a host to appear in the list of **All Hosts**. The broadcast is sent via UDP and has a packet size of approximately 25-37 bytes.

To set the broadcast interval

1. Stop the **Application Publishing Service**.
2. Locate the **HostProperties.xml** file in the C:\ProgramData\GraphOn directory.
3. Open **HostProperties.xml** in WordPad and locate the following section:
   </property>
   <property id="BroadcastInterval" group="Miscellaneous" type="UINT32">
   <value>300</value>
   </property>
4. Type the desired number of milliseconds for the value. (This value must be an integer greater than or equal to 1. Setting the value to 0 will prevent other GO-Global Hosts from being listed in the Admin Console. The default value for Broadcast Interval is 300.)
5. Start the **Application Publishing Service**.

Setting the Sign In Time Limit

The Sign In dialog and its associated session remain running indefinitely if the user does not sign in. Administrators can limit the amount of time the Sign In dialog remains open by changing the default value of the **SignInTimeLimit** property from -1 (no limit) to the desired number of minutes. (For example, if SignInTimeLimit is set to 10, the Sign In dialog will remain open for 10 minutes.) When the limit is exceeded, the session will close after briefly displaying a message that informs the user why the session is closing.

To set the Sign In Time Limit

1. Stop the **Application Publishing Service**.
2. Locate the **HostProperties.xml** file in the C:\ProgramData\GraphOn\GO-Global directory.
3. Open **HostProperties.xml** in WordPad and locate the following section:
   </property>
   <property id=" **SignInTimeLimit**" group="Miscellaneous" type="UINT32">
   <value>-1</value>
   </property>
4. Type the desired number of minutes for the value. (The valid settings for **SignInTimeLimit** are -1 (no time limit) or a positive integer indicating the number of minutes for the time limit.)
5. Start the **Application Publishing Service**.

Session Startup Options

Through the **Session Startup** tab of the Admin Console's **Host Options** dialog, administrators can enable startup options such as h, Progress Messages, and Logon Scripts. Administrators can also set various resource limits.

Applying Group Policy

GO-Global supports Microsoft's Group Policy. Using Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options. Group Policy is enabled by default.

To apply Group Policy on a GO-Global Host

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **Apply Group Policy**.
4. Click **OK**.

It may take users longer to sign in to GO-Global when Group Policy is enabled.

Displaying Progress Messages

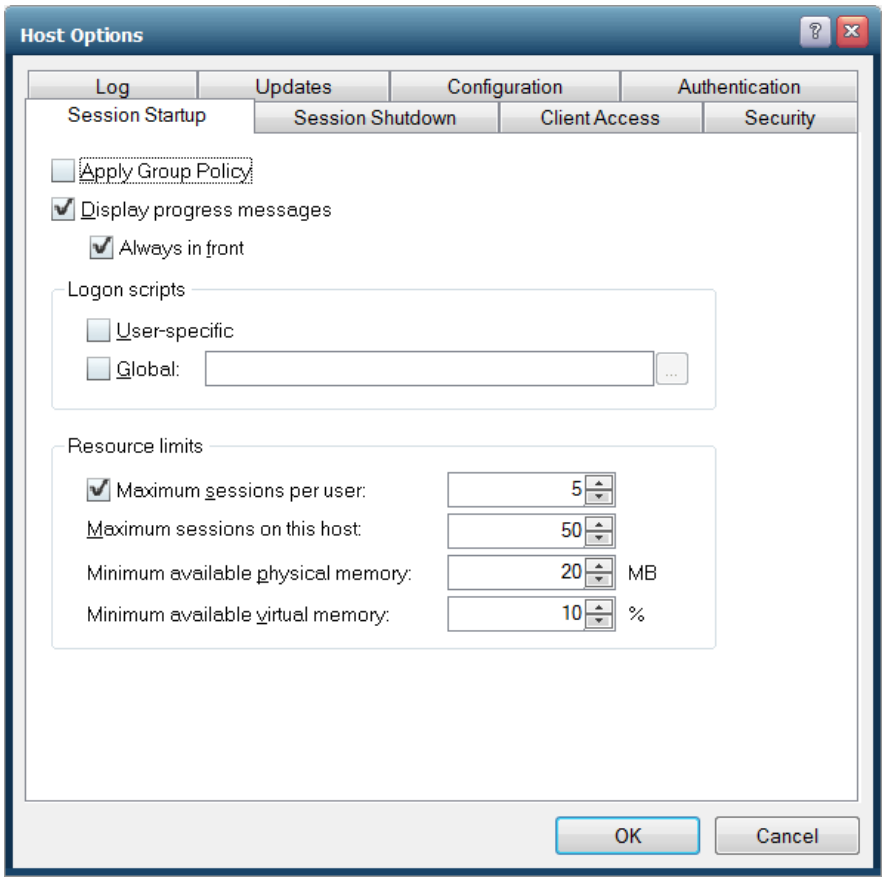
After a user is authenticated, a dialog that reports session startup progress can be displayed to users. When enabled, these messages inform users of the following:

- When their personal settings are being loaded
- When Group Policy is being applied
- When network drives are being connected
- When logon scripts are being run

To display session startup progress messages to users

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **Display progress messages**.
4. To ensure that messages are displayed in front of all other windows, select **Always in front**.
5. Click **OK**.

If a logon script has the ability to display user interface to the user, the **Always in front** option should not be enabled. Otherwise, the logon script's user interface may be partially obscured by the progress message.



Logon Scripts

Logon scripts allow administrators to configure the operating environment for GO-Global users. Scripts may perform an arbitrary set of tasks such as defining user-specific environment variables and drive letter mappings.

GO-Global supports two types of logon scripts: **global scripts** that execute for all users that sign in to the host, and **user-specific scripts** that execute for individual users. Before loading the user's profile and launching the Program Window, GO-Global's Logon Manager checks to see if a script of either (or both) type has been specified. If so, the Logon Manager runs the script(s) within the user's security context each time the user is authenticated.

User-specific logon scripts are specified using the functionality provided by the operating system. For example, the logon script for local users on a Windows Server 2016 is specified as follows:

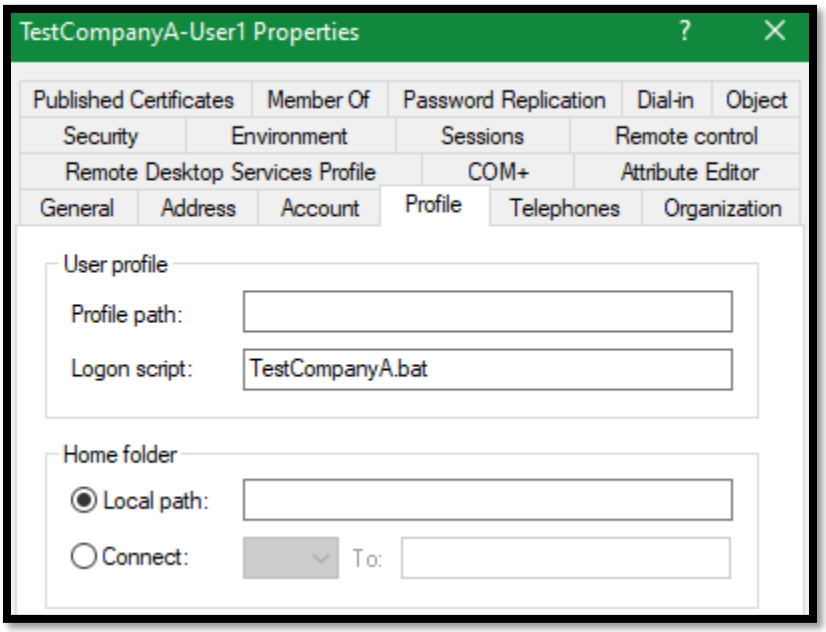
1. From the Control Panel, navigate to Administrative Tools | Computer Management | Local Users and Groups | Users.
2. Select a user and click **Properties**.
3. Click **Profiles**.
4. In the **Logon script** box, type the file name of the user's logon script.

If the value entered in the **Logon Script** box specifies a file name and extension only, GO-Global searches for the file in the following directories, in the following order:

1. If the user's account is a domain account:
a. \\DC\NETLOGON where DC is the hostname of one of your domain controllers.
b. \\DC\SYSVOL\FQDN where DC is the hostname of one of your domain controllers and FQDN is your domain's fully qualified domain name.

2. If the user's account is a local account:
a. *systemroot*\System32\Repl\Import\Scripts
b. *systemroot*\sysvol\sysvol*domainname*

If the logon script is stored in a subdirectory of one of the above directories, precede the file name with the relative path of that subdirectory.
For example, Companies\TestCompanyA.bat.



Administrators specify global and user-specific logon scripts through the Admin Console's **Session Startup** dialog.

To run user-specific logon scripts

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **User-specific**.
4. Click **OK**.

To run a global logon script

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **Global** and specify the path of the global script file.
4. Click **OK**.

Authenticated users must have read and execute access to the logon script files.

If a logon script fails to execute, an error message is displayed. Check the location of the logon script, as described above.

Additional tools such as DebugView, available from https://technet.microsoft.com/en-us/sysinternals/bb896647.aspx can help track the cause of the problem when these errors occur. Open the DebugView executable on the host and check for any errors that point to the incorrect location of the script.

Microsoft's VBScripts are not supported as logon scripts unless they are run in a batch file.

Best practices for domain accounts

- Store scripts on your domain controllers at \\FQDN\NETLOGON\ where FQDN is your domain's fully qualified domain name.
  For example: \\company.lan\NETLOGON\

- If you have had 2000/2003 domain controllers in your Active Directory domain, make sure the domain has been migrated from File Replication Service (FRS) to Distributed File System Replication (DFSR), and that replication is functioning correctly.

- Do not use UNC, DFS-Namespace, or absolute paths for Logon scripts. Instead use the script's file name only (or a relative path).

Setting Resource Limits

GO-Global allows administrators to prevent users from starting new sessions when certain resource limits are exceeded on a GO-Global Host. These limits help administrators prevent hosts from becoming loaded to the point where users experience performance problems and random resource allocation failures.

To limit the number of sessions per user

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **Maximum sessions per user** and enter the maximum number of sessions per user in the edit box.
4. Click **OK**.

Specifying the Maximum Number of Sessions

The maximum number of sessions that can be supported from a given host is set to 50 by default. Administrators should adjust this value to one that is appropriate for the capacity of the host.

To edit the maximum number of sessions per host

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Session Startup** tab.
4. Edit the number in the **Maximum sessions on this host** box. This will set the limit for the number of sessions the host can support. For example, if the maximum number of sessions is 11, the user who initiates the twelfth session will be prevented from logging on.
5. Click **OK**.

In a Relay Load Balancer setting, GO-Global checks the maximum sessions setting on the Relay Load Balancer and its Dependent Hosts. The **Maximum sessions on this host** value designated on the Relay Load Balancer is the maximum number of sessions that can be run concurrently on all Dependent Hosts assigned to that Relay Load Balancer.

This setting can be used to limit the maximum number of cloud licenses a given host will reserve.

Administrators can prevent new users from connecting to a GO-Global Host by setting the **Maximum sessions on this host** to 0. This allows administrators to gracefully remove a Dependent Host from a Relay Load Balancer environment.

Specifying the Minimum Physical and Virtual Memory

To prevent users from logging on when the available physical memory on a host falls below a given value, enter the value in the **Minimum available physical memory** edit box.

To prevent users from logging on when the available virtual memory on a host falls below a given value, enter the value in the **Minimum available virtual memory** edit box.

Session Shutdown Options

Through the Admin Console, administrators can specify time limits for the number of minutes of client idle time and the number of minutes that sessions are allowed to run on a host. Administrators can also specify whether the user is either disconnected or logged off when the idle limit is reached, and when to display warning messages to users about to be disconnected or logged off. Administrators can also designate a grace period during the log off period to allow users to save files and close applications, etc.

Specifying the Session Limit

The session limit is the number of minutes that a session is allowed to run on a GO-Global Host.

To specify the session limit

1. From the Admin Console, click Tools | Host Options.
2. Click the **Session Shutdown** tab.
3. Enable **Session**.
4. In the edit box, type the number of minutes that a session is allowed to run on a host before its user is logged off.
5. Click **OK**.

The minimum amount of session time is 1 minute and the maximum is 44640 minutes (31 days). This feature is disabled by default.

Specifying the Idle Limit

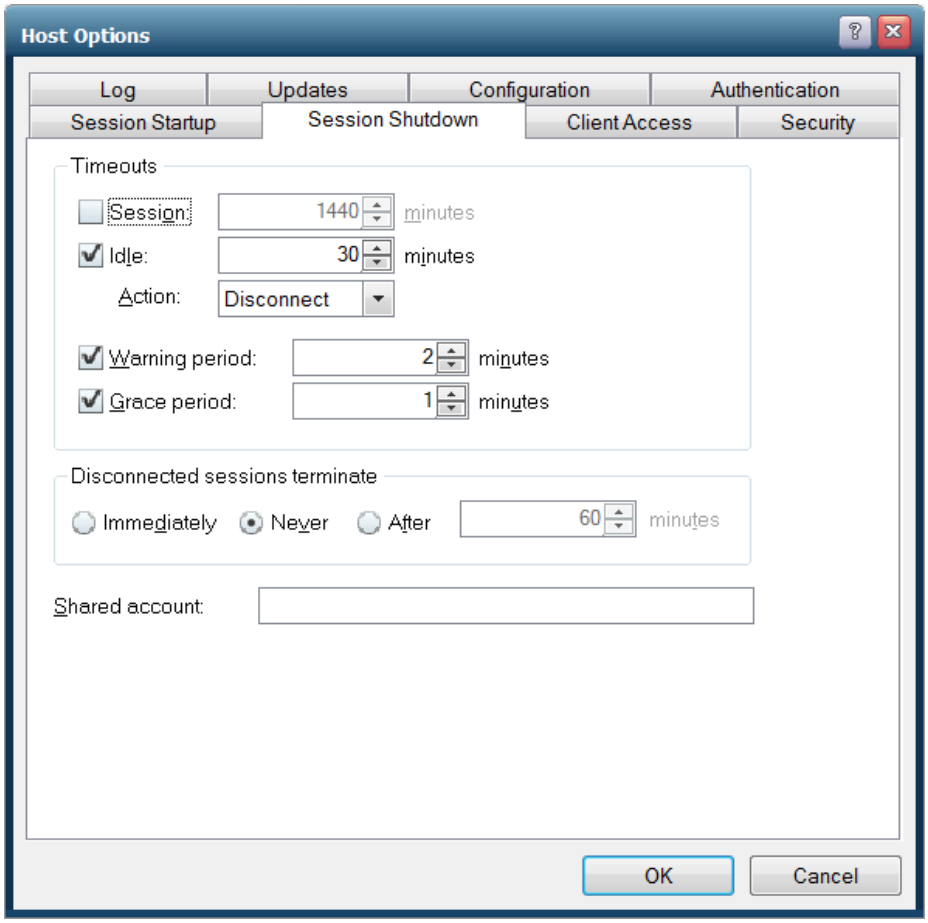
Idle time refers to the number of minutes since the last mouse or keyboard input event was received in a session. The idle limit is the number of minutes of idle time that a GO-Global Host allows.

To specify the idle limit

1. From the Admin Console, click Tools | Host Options.
2. Click the **Session Shutdown** tab.
3. Enable **Idle**.
4. In the edit box, type the number of minutes of idle time allowed by the host.
5. From the **Action** list, click **Disconnect** to disconnect users when the idle limit has been reached or click **Log off** to log users off when the idle limit has been reached.

6. Click **OK**.

The minimum amount of idle time is 1 minute and the maximum is 44640 minutes (31 days). The idle time is set to 30 minutes by default.



Specifying the Warning Period

The warning period refers to the number of minutes before a session limit or idle limit is reached when users are warned they are about to be disconnected or logged off. For example, if the warning period is set to 2, users will be warned 2 minutes before the session limit or the idle limit is reached. This feature is disabled by default.

To specify the warning period

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Shutdown**.
3. Enable **Warning period**.
4. In the edit box, type the number of minutes before a session or idle limit is reached when users are warned that they are about to be disconnected or logged off.
5. Click **OK**.

The warning period must be less than the session limit and idle limit settings.

Specifying the Grace Period

The grace period refers to the number of minutes after a logoff begins during which users may save files, close applications, etc. Grace period is enabled and set to one minute by default. The minimum grace period value is one minute and the maximum value is 15.

To specify the grace period

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Shutdown**.
3. Enable **Grace** period.
4. In the edit box, specify the number of minutes after a logoff begins that users are able to save files and close applications, etc.
5. Click **OK**.

Windows Compatibility Assurance

To provide multi-user remote access on all versions of Windows, GO-Global must access internal functions and data structures in Windows. When a computer running the GO-Global Host starts, GO-Global analyzes some of the operating system's binary files and automatically identifies the addresses of the operating system functions and variables that GO-Global requires.

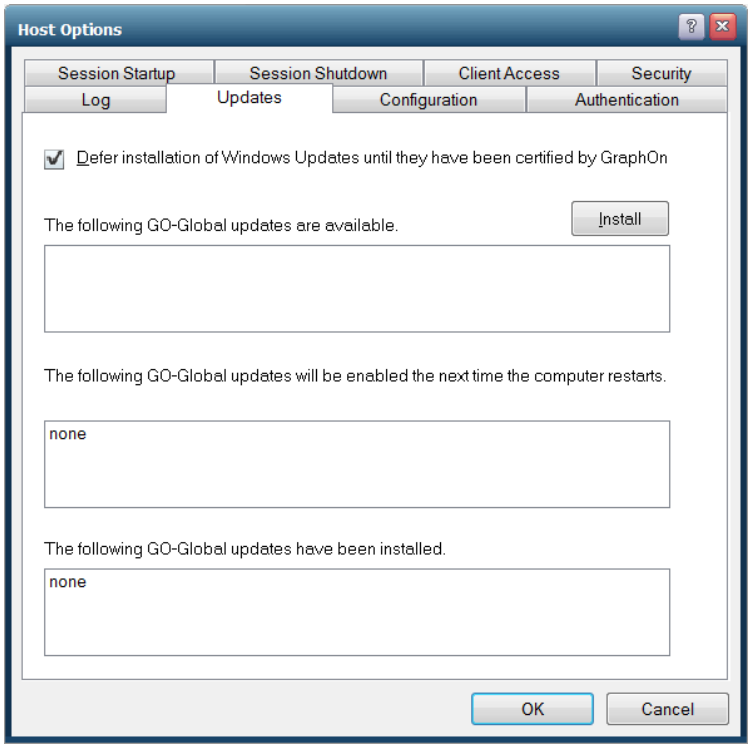
In most cases, GO-Global is able to identify the required operating system addresses regardless of the version of Windows and the Windows Updates that are installed on the computer. In rare cases, however, Windows Updates include changes to the operating system that either prevent GO-Global from locating a required address or are incompatible with GO-Global's interface to the operating system. When this happens, GO-Global is unable to start sessions on a computer. To prevent this from occurring, GO-Global provides **Windows Compatibility Assurance**.

The **Windows Compatibility Assurance** feature gives administrators the option to automatically defer installation of Windows Updates until GraphOn has verified that the updates are compatible with GO-Global. To do this, GraphOn continuously monitors Microsoft's Windows Update service for new updates. When Microsoft releases one or more Windows Updates, GO-Global suspends installation of all Windows Updates on affected GO-Global hosts until GraphOn has verified that the newly released Windows Updates are compatible.

To ensure GO-Global Hosts do not download newly released Windows Updates during the short window of time between when Microsoft releases a new update and GraphOn detects that the update has been released, GO-Global controls when Windows Updates can be installed on GO-Global Hosts. GO-Global delays Windows Updates by the number of days specified by the value of the **DelayWindowsUpdates** property in the HostProperties.xml file. (This is set to 1 day, by default).

If an incompatibility is identified, GO-Global prevents installation of all Windows Updates on affected hosts until it has automatically downloaded and installed an update that is compatible with all Windows Update releases. GO-Global notifies the administrator when a compatibility update is downloaded and installed. After the compatibility update is successfully installed and the computer is restarted, GO-Global will resume Windows Updates.

When enabled, Windows Compatibility Assurance minimizes the risk of incompatibilities. Windows Compatibility Assurance is enabled by default, but can be disabled through the **Host Options** dialog. However, if a Windows Update is incompatible with GO-Global, and it is installed on the host, GO-Global and/or the host machine will stop working. GraphOn recommends that this option is not disabled. However, if GO-Global is running on a closed network, and is unable to communicate with GraphOn's Update server, this feature can be disabled to prevent warning messages from being displayed.



To disable Windows Compatibility Assurance

1. From the Admin Console, click Tools | Host Options.
2. Click the **Updates** tab.
3. Click the checkbox next to **Defer Windows Updates until they have been certified by GraphOn**.

GO-Global displays messages describing an update's certification status when the Admin Console first opens and when selecting a host from the **All Hosts** list. Certification status messages display as follows:

	Message displayed:
If Windows Updates have been *certified* by GraphOn...	GO-Global is compatible with the latest Windows Updates, which were released on [date of release].
If certification by GraphOn is *pending...*	GraphOn is testing Windows Updates released on [date of release]. GO-Global is delaying installation of Windows Updates until GraphOn certifies that these Windows updates are compatible with GO-Global.
If certification by GraphOn is *pending*, but the Windows Compatibility Assurance option is disabled...	GraphOn is testing Windows Updates released on [date of release] to see if they are compatible with GO-Global.
If GraphOn determines that Windows Updates are incompatible...	GO-Global is incompatible with Windows Updates released on [date of release]. GO-Global is delaying installation of Windows Updates until a GO-Global Compatibility Update is available.
If Windows Updates are incompatible but the Windows Compatibility Assurance option is disabled...	GO-Global is incompatible with Windows Updates released on [date of release]. If these Windows Updates are installed on this computer, GO-Global and/or this computer will stop working.

GO-Global verifies that all the licenses the computer is using support the selected GO-Global update. If any of the licenses do *not* support the update, the GO-Global update will not be installed. For example, if the host is using a version 5 license and the selected GO-Global update is version 6, the GO-Global license(s) that this computer is using must be upgraded before the update can be installed. Contact your GO-Global reseller or sales@graphon.com to upgrade licenses.

Runtime Incompatibility Detection

In addition to ensuring compatibility with Windows, GO-Global detects incompatibilities at runtime and will disable itself if it detects that it is incompatible with the version of Windows or any other software installed on the computer.

Additionally, as a failsafe, when a computer starts up, GO-Global records its progress in the **\Windows\System32\Drivers\dbcm.bin** file. If a computer fails to start (e.g., crashes on startup), the next time it tries to start, GO-Global checks the contents of the **dbcm.bin** file to see if the computer fully started on the previous boot. If it did not, GO-Global assumes there is a compatibility issue between GO-Global and another application installed on the computer. To prevent the computer from crashing again, GO-Global does not load its drivers. This enables the computer to boot, but disables GO-Global.

When GO-Global has disabled itself in this manner and an administrator runs the Admin Console, a message is displayed that notifies the administrator that GO-Global has disabled itself *and* gives the administrator the option to re-enable GO-Global and restart the computer. If, however, the administrator chooses to re-enable GO-Global and the source of the incompatibility has not been resolved, the computer will again fail to start, and GO-Global will again disable itself.

GO-Global Updates

There are three types of GO-Global Updates:

- Critical
- Recommended
- Optional

Critical updates are changes that are required for GO-Global to run on the latest releases of Microsoft Windows. Critical updates do not include functionality changes. They generally only replace a few binary files on the host.

Recommended updates are changes that fix GO-Global defects and usability issues. They generally do not include user interface changes unless a user interface change is necessary to fix an important defect. Recommended updates generally replace all of GO-Global's binary files.

Optional updates are changes that add new features and functionality to GO-Global. Optional updates include major upgrades and minor upgrades. Optional updates generally replace all of GO-Global's binary files.

GO-Global will only automatically download and install *critical* GO-Global Updates if the Windows Compatibility Assurance option is enabled. By default, GO-Global defers installation of Windows Updates until they have been certified by GraphOn.

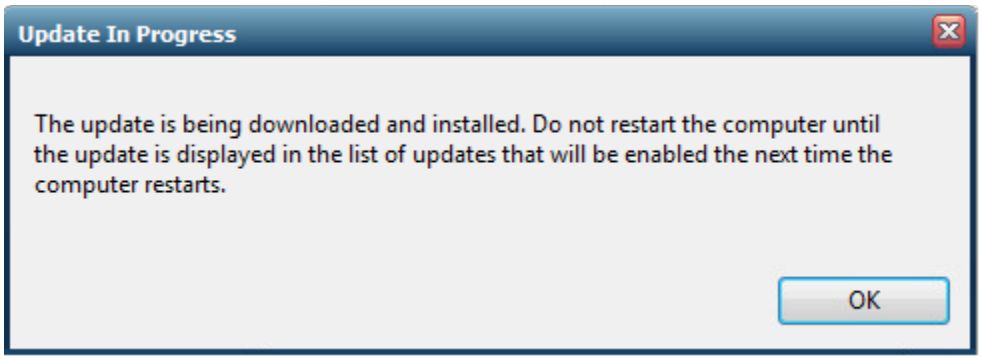
Installing a GO-Global Update

GO-Global displays the available GO-Global updates in the **Updates** tab of the **Host Options** dialog, and allows administrators to select an update and install it.

To install an update

1. From the Admin Console, click Tools | Host Options.
2. Click the **Updates** tab.
3. Select one or more updates from the list of available GO-Global updates.
4. Click the **Install** button.
5. Click **Yes** to confirm.

After confirming the download, the following message is displayed:



When the update has been installed, a message confirming installation will be displayed. The installed update will be enabled the next time the computer is restarted. GraphOn recommends restarting the computer at the first opportunity, when users will not be affected. After the computer has been restarted, and the update is enabled, a message will confirm that a new version of GO-Global has been installed and enabled.

Reviewing Pending and Installed Updates

When performing update checks, the Application Publishing Service looks for updates that support:

a. the version of GO-Global that is installed on the computer,
b. the version of the computer's operating system, and
c. the type of updates that are approved to be downloaded and installed on the host.

When the Application Publishing Service finds a match, it downloads the update's installer and runs it. After the update's installer has been run, the update is pending but not yet fully installed. Pending updates are installed and activated the next time the computer is restarted. Administrators can view the pending and installed updates on the **Updates** tab of the Admin Console's **Host Options** dialog.

To review pending and installed updates

1. From the Admin Console, click Tools | Host Options.
2. Click **Updates**.
3. **The following GO-Global updates will be enabled the next time the computer restarts** group box lists the updates that have been downloaded but are not yet fully installed.
4. **The following GO-Global updates have been installed** group box lists the updates that are installed and active on the host.
5. Click **OK**.

GO-Global's version number includes the software's *major version*, *minor version*, *service pack version*, and *build number*. For example, in version **6.1.2.37894**, **6** is the major version, **1** is the minor version, **2** is the service pack version, and **37897** is the build number.

The *build number* is increased in all GO-Global releases. A release in which only the build number is increased is a **Patch**. Patch releases generally include targeted fixes for urgent issues and product defects.

The *service pack* number is increased in **Service Pack** releases. Service Pack releases contain bug fixes, and include any fixes released in preceding Patch releases. In addition, Service Pack releases may include support for new platforms *and minor enhancements.*

The *minor version* number is increased in **Feature Upgrades**. Feature Upgrades include significant feature additions or alterations. Feature Upgrades also include bug fixes and security improvements, including any changes released in preceding Service Pack and Patch releases. Feature Upgrades generally include changes to administration user interfaces but do not make significant changes to the way end users interact with the product.

The *major version* number is increased in **Major Upgrades**. Major Upgrades include significant changes to GO-Global's underlying architecture or its user interface. They also include significant feature additions and bug fixes, including all the features and fixes released in preceding Feature Upgrades, Service Packs, and Patches.

Managing GO-Global Hosts from Client Machines

Administrators can connect to the Admin Console from any client machine. This allows the administrator to end processes, terminate sessions, and administer applications from any machine running a GO-Global client.

To access the Admin Console from a client machine

1. Set the permissions for the Admin Console so that only Administrators can access the application.
2. In Windows Explorer, locate **AdminConsole.exe** from the GO-Global\Programs folder.
3. Right-click **AdminConsole.exe** and select **Properties**.
4. In the **Properties** dialog box, select **Security**.
5. In the **Security** dialog box, select **Permissions**.
6. In the **File Permission** dialog box, set the permissions so that only Administrators can execute the application. (For help with setting permissions in Windows Explorer, choose the Help button from the File Permission box, or press F1 while running Explorer.)
7. Add the Admin Console (AdminConsole.exe) as a registered application with the Admin Console.
8. From the client machine, log on to a GO-Global Host as an Administrator, or as a user with administrative rights on the host. This will launch the Program Window.
9. From the Program Window, launch the Admin Console by clicking the Admin Console icon. (This icon will only appear in the Program Window if the user has administrative rights on the host.) You can administer applications and user access as if running the Admin Console from the GO-Global Host.

Keyboard Shortcuts for the Admin Console

Action	Result
Applications Tab	
Double-click the application	Displays **Application Properties** dialog
DELETE*	Removes selected application
CTRL+A*	Displays **Application Properties** dialog
CTRL+S	Displays **Application Properties for Users/Groups** dialog
Sessions Tab	
DELETE	Terminates selected session
Processes Tab	
DELETE	Terminates the selected process
General	
CTRL+TAB	Cycles through tabs
CTRL+SHIFT+TAB	Reverse cycles through tabs
CTRL+P	Displays **Options** dialog
CTRL+B	Turns **Status Bar** on or off
ALT+F4	Exits the Admin Console
F1	Displays Help for the Admin Console
F5	Refreshes the Sessions, Processes, and Applications tabs
INSERT	Displays **Add Application** dialog box

*An application from the list of Installed Applications must be selected in order for these shortcuts to work.

CHAPTER VII

Load Balancing

7

Load Balancing

Load balancing allows GO-Global sessions to be distributed across multiple hosts. Load balancing is required when the host resource requirements for a deployment exceed the capacity of a single host computer. GO-Global can also be used with any third-party TCP/IP based load-balancing service.

GO-Global supports three load balancing configurations:

1. **A third-party load balancer routing connections to a collection of Farm Hosts that are managed by a Farm Manager.** This configuration is recommended for large deployments (e.g., more than 500 concurrent users) when centralized management or session reconnect is required. In a load-balanced farm environment, administrators use the Admin Console on the Farm Manager to configure the published applications and settings on all the Farm Hosts. Administrators can manage and shadow sessions running on any host in the farm. Users can start sessions on one device (e.g., a computer in an office), disconnect, and then reconnect to their sessions from a different device (e.g., a home computer). This configuration provides optimal scalability, reliability, and stability for large deployments.

2. **A GO-Global Relay Load Balancer routing connections to a collection of Dependent Hosts.** This configuration is ideal for smaller deployments (e.g., less than 500 concurrent users) where a third-party load balancer is not available. GO-Global load-balances client connections and ensures that sessions start successfully. If a session fails to start on the selected host, the Relay Load Balancer selects another host and tries again until it finds one that can support the session.

3. **A third-party load balancer balancing connections to a collection of Independent Hosts.** This configuration is recommended for large deployments when session reconnect or centralized management is *not* required. Independent Hosts do not interact with other GO-Global Hosts running on the network and can have different configuration options and different published applications.

Load Balancing Requirements

- A GO-Global Host must be installed on each of the hosts in the cluster.
- For web deployments, if the load balancer is routing the connections from users' browsers (to download AppController and the GO-Global Web App) to the GO-Global Hosts, each of the GO-Global Hosts in the cluster must have the GO-Global Web files installed. If the load balancer is only routing connections from AppController and the GO-Global Web App to the GO-Global Hosts, the web files do not need to be located on each GO-Global Host. In that case, the Web files should be installed on the machine running the web server.
- If an application saves any user specific settings in the registry (e.g., Microsoft Word), it is strongly recommended that users operate with roaming profiles rather than local profiles. Since there is no way of predicting which server the user will actually be logged onto in a balanced server farm, working with roaming profiles is the only way to ensure that user specific settings are available to the user at all times.

When using on-premises licenses in a load-balanced configuration, GraphOn recommends using a license server. For more information, see the following sections: Multiple Host Environments, Three-Server Redundancy, and License-File List Redundancy.

When using cloud licenses, GraphOn recommends activating GO-Global on the Relay Server or Farm Manager. GraphOn does not recommend using cloud licenses when a third-party load balancer is used with Independent Hosts.

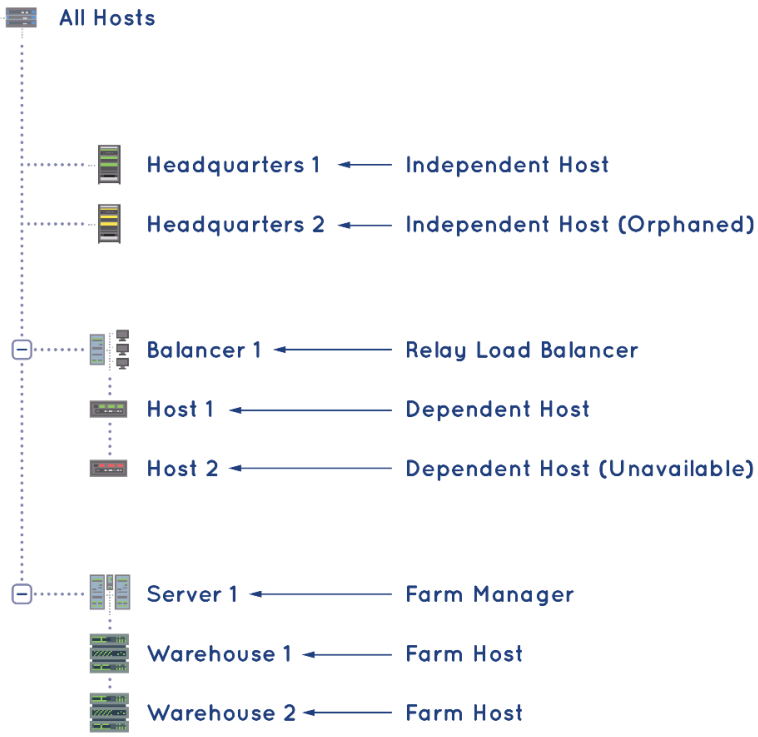
Independent Hosts

Independent Hosts are GO-Global Hosts that do not interact with other GO-Global Hosts running on the network. Independent Hosts appear in the Admin Console on the first level of the GO-Global Hosts tree view as an independent node. The GO-Global setup program configures hosts to operate as Independent Hosts. GO-Global clients can connect to Independent Hosts directly by specifying the name or IP address of the server in the **Connection** dialog or the location box of a web browser.

Clients can also connect to Independent Hosts through a third-party network load balancer that distributes client connections among several servers. However, this configuration only provides limited support for session reconnect. Specifically, it supports reconnecting users to their sessions if a network disruption breaks the connection, but it does not allow users to disconnect from their sessions and reconnect to them at a later time.

When using Independent Hosts together with a third-party load balancer, administrators must select the option to terminate disconnected sessions **Immediately** on the **Session Shutdown** tab of the Admin Console's **Host Options** dialog. Otherwise, users will have an option in the Program Window to disconnect from their sessions, but if they select this option, they will generally be unable to reconnect to their sessions.
In addition, administrators must set the value of the **SessionTimeoutBrokenConnection** property in each host's **HostProperties.xml** file to the number of minutes sessions should remain running on the host after a broken connection.

If the Application Publishing Service is not running on a host, the host's icon will be red. If the administrator does not have rights to access the host, the host's icon will be yellow.



Relay Load Balancers

A Relay Load Balancer is a GO-Global Host that provides centralized control over one or more hosts. Relay Load Balancers maintain client connections and distribute GO-Global sessions across a set of load-balanced application hosts. Relay Load Balancers appear in the Admin Console on the first level of the list of **All Hosts** as nodes with one or more Dependent Hosts.

To configure a GO-Global Host to operate as a Relay Load Balancer

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Configuration** tab.
4. Type the name or IP address of the computer in the **Relay Load Balancer address** box.
5. Click **OK**.
6. A message box is displayed indicating that the change will not take effect until the **Application Publishing Service** on the Relay Load Balancer has been restarted. Click **OK**.
7. Stop and restart the **GO-Global Application Publishing Service** from the Services option in the Control Panel.

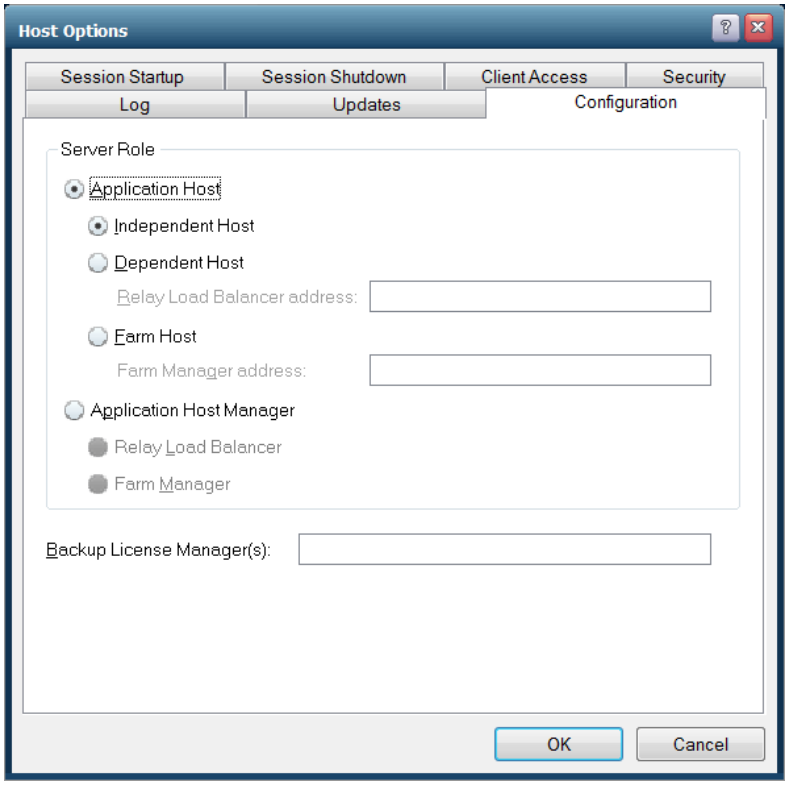
After configuring a host to run as a Relay Load Balancer with one or more Dependent Hosts, GO-Global load-balances client connections and ensures that sessions start successfully. If a session fails to start on the selected host, the Relay Load Balancer selects another host and tries again until it finds one that can support the session. The Relay Load Balancer starts new sessions on the Dependent Host with the lightest load, where the load on each Dependent Host is calculated as the number of sessions running on the Dependent Host divided by the **Maximum sessions on this host** value set in the Admin Console for the Dependent Host.

With Relay Load Balancers, all data transmitted between the clients and Dependent Hosts passes through the Relay Load Balancer. When setting up a relay server environment, be sure the same **Log Folder** path for the Relay Load Balancer exists on the Dependent Hosts. Otherwise, the **Sign In** dialog will not appear when users attempt to sign in to GO-Global. Create a log directory on the C: drive of each Relay Load Balancer (e.g., C:\Data\APS_LOGS) or use C:\Program Files\GraphOn\GO-Global\Log which already exists on the Dependent Host. Make sure this same path exists on the Dependent Host. In addition to changing the **Log Folder** path in the Admin Console, the \Log\Codes and \Log\Templates directories must be copied to the new location.

When a Relay Load Balancer is selected in the Admin Console, the number of processes running on all Dependent Hosts is not listed in the Admin Console's status bar.

A Relay Load Balancer requires a minimum of 1 GB of RAM and 2 processors. An additional 3 GB of RAM and 2 processors are required per 1,000 concurrent users.

Memory and CPU requirements for the Dependent Hosts are determined by the applications that are published and the number of users accessing the system. In general, a Dependent Host can support 12 “heavy” users/500 MHz CPU and 25 “light” users/500 MHz CPU. (“Heavy” is defined as a user running one or more large applications with continuous user interaction. “Light” is defined as a user running one application with intermittent user interaction.)



Dependent Hosts

A Dependent Host is a GO-Global Host that is connected to a Relay Load Balancer. GO-Global clients cannot connect directly to Dependent Hosts. Instead, they connect to the associated Relay Load Balancer, and the Relay Load Balancer selects one of the connected servers to host the session.

To configure a GO-Global Host to operate as a Dependent Host

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Configuration** tab.
4. Click **Application Host**.
5. Click **Dependent Host**.
6. Type the IP address of the Relay Load Balancer in the **Relay Load Balancer address** box.
7. Click **OK**.
8. A message box is displayed indicating that the change will not take effect until the **Application Publishing Service** has been restarted.
9. Click **OK**.
10. Stop and restart the **GO-Global Application Publishing Service** from the Services option in the Control Panel.

When the Application Publishing Service is restarted, the Dependent Host will appear beneath the Relay Load Balancer in the Admin Console's list of GO-Global Hosts. A Dependent Host colored yellow indicates that the host has been "orphaned;" in other words, that its Relay Load Balancer has gone down. If the Application Publishing Service is not running on a host, the host's icon will be red.

Users are authenticated on Dependent Hosts, not on Relay Load Balancers. As a result, Dependent Hosts can be located on a different network than their associated Relay Load Balancer. For example, Dependent Hosts can be located behind a firewall on an internal, Active Directory network, and the associated Relay Load Balancer can be located in a demilitarized zone (DMZ) that is outside the firewall. If **Integrated Windows authentication** is used, clients and Dependent Hosts must be located on the same domain, but the Relay Load Balancer can be located on a different domain.

The same set of applications must be installed on each Dependent Host. GraphOn recommends that each application have the same installation path on each host.

Taking a Dependent Host Offline

Administrators can prevent new users from connecting to a GO-Global Host by setting the **Maximum sessions on this host** to 0 in the **Session Startup** tab. This allows administrators to remove a Dependent Host from a Relay Load Balancer environment without losing any user sessions.

To take a Dependent Host offline

1. Select the desired Dependent Host from the list of All Hosts.
2. Click Tools | Host Options.
3. Click the **Session Startup** tab.
4. In the **Maximum sessions on this host** box, set the value to 0. This will prevent new users from connecting to the host.
5. Click **OK**.
6. Monitor the number of sessions running on the host. When the number of sessions reaches zero, shut down the Dependent Host.

Farm Manager

A Farm Manager is a GO-Global Host that is used to centrally manage a cluster of Farm Hosts. Unlike a Relay Load Balancer, Farm Managers do not load-balance connections to the Farm Hosts, and they do not relay data between clients and Farm Hosts. Farm Managers manage connections to Farm Hosts using a third-party load-balancer. A Farm Manager must be configured before configuring the Farm Hosts.

To configure a Farm Manager

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Configuration** tab.
4. Click **Application Host Manager**.
5. Click **Farm Manager**.
6. Click **OK**.
7. Restart the **Application Publishing Service**.

A Farm Manager requires a minimum of 1 GB of RAM and 2 processors. An additional 2 GB of RAM is required per 1,000 concurrent users.

Farm Manager Resource Requirements

Farm Managers centrally manage a collection of Farm Hosts. They manage information about joined Farm Hosts and client sessions. The main user data streams are not maintained via Farm Managers. However, there is still a per-user connection resource cost. Farm Managers do not run user applications directly, and can operate with modest server specifications. The primary resource a Farm Manager consumes is system RAM, with it having a relatively low CPU and Disk IO/space burden.

GraphOn recommends the following resources for Farm Managers:

Baseline (up to 2,000 concurrent users)

- CPU: 2-4 cores
- RAM: 8 GB
- Storage: Follow best practice for your Windows version, typically at least 80 GB. Depends on logging, page file location and other factors

Scaling

For every additional 500 concurrent users beyond the initial baseline:

- Add 1 GB RAM

Example Configurations

- 1,000 concurrent users: 8 GB RAM
- 3,000 concurrent users: 10 GB RAM
- 5,000 concurrent users: 14 GB RAM
- 10,000 concurrent users: 24 GB RAM

These are approximate values based on the provided scaling rule. Actual requirements may vary depending on usage patterns and hardware specifics.

Performance Monitoring

As with any Windows infrastructure, each use case is unique. Monitor the following metrics over time and during peak use to determine appropriate resource allocation and performance improvements:

Disk Performance

- IOPS (input/output operations per second)
- Bandwidth
- Read/Write speeds
- Queue depth
- Latency

Memory

- RAM use (%)
- Monitor for memory consumption approaching available physical memory

CPU Usage

- Per core (minimum, maximum, averages)
- Overall (minimum, maximum, averages)

By closely monitoring these data points, you can make informed decisions about resource allocation and performance enhancements for your specific use case.

Users must be an administrative user on any local or remote host they are administrating. If not, they will be prompted for a user name and password so that they can then enter an administrator user name and password for that host or manager.

Farm Host

A Farm Host is a GO-Global Host that is connected to a Farm Manager. GO-Global clients connect directly to Farm Hosts.

To configure a Farm Host

1. Select the desired host from the list of **All Hosts**.
2. Click **Tools** | **Host Options**.
3. Click the **Configuration** tab.
4. Click **Application Host**.
5. Click **Farm Host**.
6. In the **Farm Manager address** field, type the IP address of the Farm Manager.
7. Click **OK**.
8. Restart the **Application Publishing Service**.

GO-Global users/clients are not intended to connect directly to Farm Managers. For farm deployments, GraphOn recommends using a third-party load balancer, which forwards connections directly to various Farm Hosts. There are various free open source and proprietary hardware, software, and virtual-cloud load balancers available for this purpose.

Configuring a Third-Party Load Balancer

GO-Global's Farm Host and Farm Manager roles make it easy for administrators to manage farms of GO-Global Application Hosts that are accessed via third-party load balancers. Using these roles, administrators can manage and shadow sessions running across a farm, and they can configure settings on all Farm Hosts in a farm at once. And when new Farm Hosts join a farm, they automatically inherit the settings of the other hosts in the farm.

In addition, these new roles enable users who connect to GO-Global Hosts via third-party load balancers to disconnect from their sessions from one device and reconnect to their sessions from a different device. GO-Global automatically reconnects users to their sessions, even when the load balancer fails to connect a user to the host on which the user’s session is running.

For example, if a user with a session running on Host A disconnects from the session while at work, goes home, and then reconnects to the session from a home computer, GO-Global will ensure that the user is reconnected to his or her session. If the load balancer routes the user's connection to Host B, Host B will open a connection to Host A and relay the data between AppController and Host A.

To enable these capabilities:

1. Create a GO-Global Farm Manager:
   a. Install the GO-Global Host on a computer that is **not** connected to the third-party load balancer.
   b. Run the Admin Console and set the Server Role to **Farm Manager**.
   c. Restart the **Application Publishing Service**.

2. On each GO-Global Application Host that is accessible from the load balancer:
   a. Run the Admin Console and set the Server Role to Farm Host.
   b. Enter the address of the Farm Manager configured in step 1 in the **Farm Manager address** field.
   c. Restart the **Application Publishing Service**.

Administrators can provide High Availability for a farm by configuring a failover Farm Manager as follows:

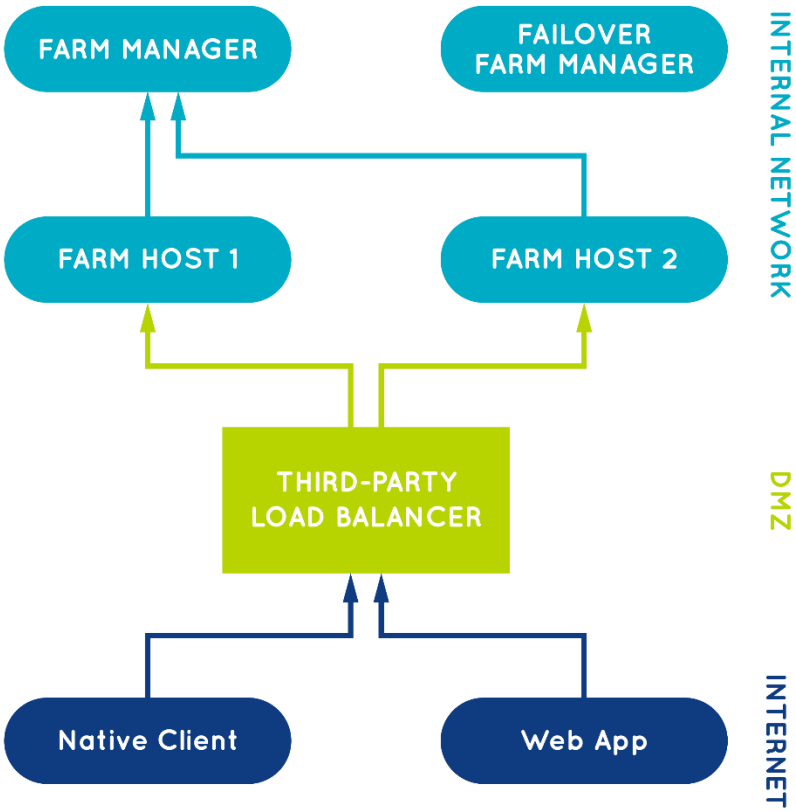
1. Create a failover Farm Manager:
   a. Install the GO-Global Host on another computer that is not connected to the third-party load balancer.
   b. Run the Admin Console and set the Server Role to **Farm Manager**.
   c. Restart the **Application Publishing Service**.

2. On each GO-Global Application Host that is accessible from the load balancer:
   a. Run the Admin Console and append a semicolon and the address of the failover Farm Manager to the address of the primary Farm Manager in the **Farm Manager address** field.
   b. Restart the **Application Publishing Service**.

The Farm Manager and Farm Host server roles are supported by the same infrastructure and design that has supported the GO-Global Relay Server and Dependent Host roles for many years. Unlike a Relay Server, however, a Farm Manager does not relay data between GO-Global clients and hosts and is, therefore, not subject to the same scalability limits as a Relay Server.

A Farm Manager keeps track of all sessions running in a farm, but unless an administrator is shadowing a session, no data from applications running in a session passes through the Farm Manager.

The diagram below illustrates a GO-Global configuration using a third-party load balancer in a DMZ, with the Farm Manager and Farm Hosts in the internal network.



Both AppController and the GO-Global Web App work with AWS Network Load Balancers, but only the GO-Global Web App works with AWS Application Load Balancers.

Load Balancer Affinity/Stickiness Options

When a third-party load balancer is used and the load balancer's affinity/stickiness option is not enabled, the load balancer will often route connections from AppController to a different host than the host to which the load balancer routed the Web App's connection. When this occurs, GO-Global is designed to relay the connection from the host that accepted AppController's connection to the host that accepted the Web App's connection.

For example, if the load balancer routes the Web App's connection to Host 1 and the **useApp** parameter is not specified or set to true, the Application Publishing Service on Host 1 sends a command to the Web App to start AppController. With this command, the Application Publishing Service includes a one-time password (OTP) and the address of Host 1. The Web App then starts AppController and passes these values to AppController on its command line.

When AppController starts and connects to the load balancer, if the load balancer's affinity/stickiness option is not enabled, the load balancer will often route AppController's connection to a different host (e.g., Host 2). AppController then sends the address of Host 1 (that was specified on its command line) to Host 2. Host 2 opens a connection to Host 1 and relays the data between AppController and Host 1. Then AppController sends the OTP to Host 1, and Host 1 verifies that it is the value it specified.

In this scenario, Host 1 obtains the address that it passes to the Web App from the **RelayConnectionAddress** property in its HostProperties.xml. The Application Publishing Service initializes the value of this property when it starts the first time. If the value of the property is already set, however, the Application Publishing Service does not change it.

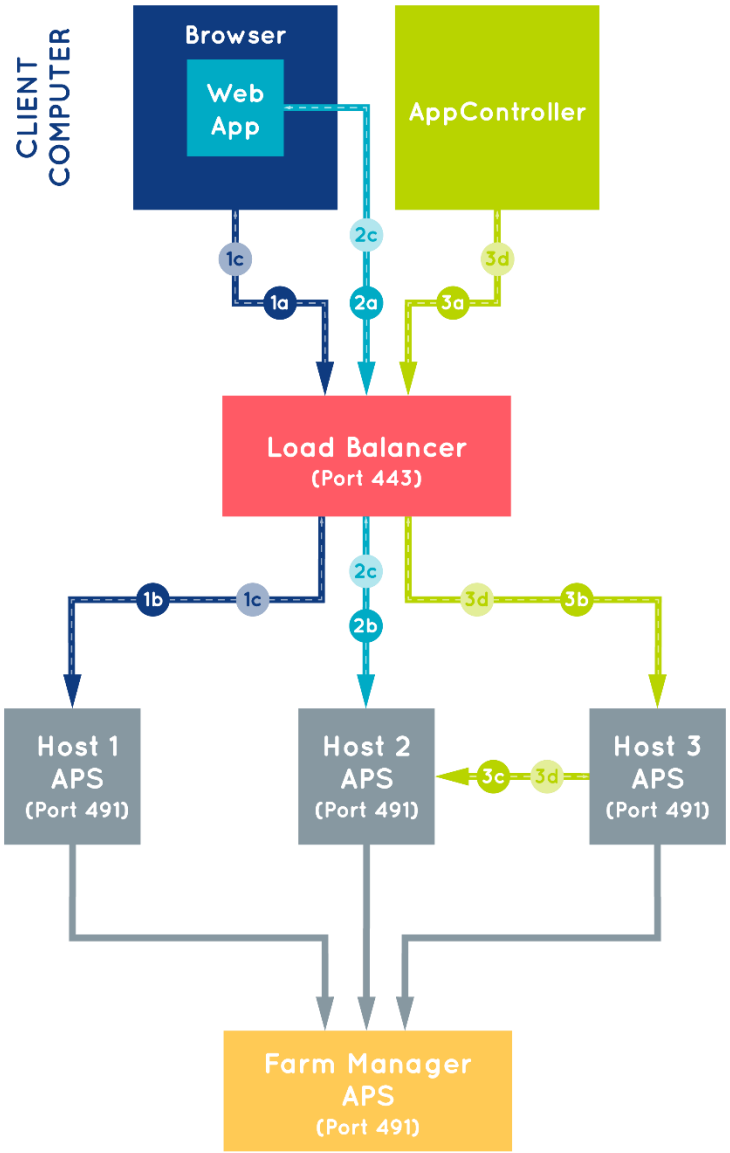
Starting a GO-Global Session from a Browser

Three separate connections are required to start a session that uses AppController:

1. The browser connects and downloads the Web App and its associated HTML and JavaScript pages.
2. The Web App connects and optionally orchestrates installing and starting GO-Global's native client, AppController.
3. AppController connects, and the Application Publishing Service (APS) starts the session. AppController displays the session's applications *outside* the browser's window by default. Alternatively, if the embed option is set to true, the session's applications are displayed *within* the browser by the Web App, and AppController provides access to client devices (e.g., printers, etc.).

   When AppController is not used (e.g., when useApp=false), only the first two connections are required. The session starts after the Web App connects, and the Web App displays the session's applications within the browser's window.

The diagram below illustrates how GO-Global starts a session from a browser.



1 Connection from the Browser

1a — Browser connects to the Load Balancer on the port specified by URL protocol (HTTPS=443)

1b — Load Balancer forwards connection to the Application Publishing Service (APS) on one of the target hosts on the configured port (e.g., 491)

1c — APS sends Web App and associated HTML and JavaScript files over connection to browser

2 Connection from the Web App

2a — Web App connects to the Load Balancer on the address and port specified in the URL or logon.html. By default, the Web App connects to the same address that the browser connected to in 1a (the address that follows https:// in the URL). This is generally what is desired. Conversely, administrators must generally specify the port (443) via GO-Global's port parameter in the URL or logon.html. Otherwise, the Web App will attempt to connect to the Load Balancer on GO-Global's default port, 491.

2b — Load Balancer forwards connection to the APS on one of the target hosts on the configured port (e.g., 491)

2c — APS negotiates WebSocket connection and then sends messages to Web App to install/launch AppController. These messages include the internal address of the host (e.g., Host 2), which is read from the RelayConnectionAddress property in the host's HostProperties.xml file.

3 Connection from AppController

3a — The Web App starts AppController, and AppController connects to the Load Balancer on the port specified in logon.html or URL (received from APS at 1C)

3b — Load Balancer forwards connection to APS on one of the target hosts on the configured port (e.g., 491)

3c — APS on Host 3 forwards connection to Host 2. (Host 2's RelayConnectionAddress received via communication at 2c.)

3d — APS on Host 2 authenticates connection using data transmitted at 2c, then starts a GO-Global session. Session data is transmitted over connection 3, which is relayed through the APS on Host 3.

Taking a Farm Host Offline

When using third-party load balancers with a Farm Manager, administrators can use the following procedure to remove hosts from the farm without losing any user sessions.

1. On all Farm Hosts, set the **Disconnected sessions terminate** option to either **Never** or **After**, with the **After** value set to at least 1 minute.

2. Remove the target host, i.e., the Farm Host you want to take offline, from the load balancer's target group. This will prevent new connections from being routed to the target host, and at some point, depending on the load balancer, it should close the open connections to the target host.

   When connections to the target host are closed, GO-Global clients will automatically reconnect to their sessions running on the target host via other Farm Hosts in the cluster. Specifically, they will open a new connection to the load balancer, the load balancer will route the connection to one of the active Farm Hosts, and the active Farm Host will relay the connection to the host that has been removed from the load balancer's target group.

3. Monitor the number of sessions running on the target host. When the number of sessions reaches zero, shut down the Farm Host.

When using an AWS Network Load Balancer, set **deregistration_delay.connection_termination.enabled** to true so connections will be closed when the target host transitions to the unused state.

License Server Configuration

When Independent Hosts are used with a third-party load balancer, GraphOn recommends that the hosts be configured to use an on-premises, central license server. If high-availability is required, the hosts should be configured to use a set of a set of Three-Server Redundant License Servers.

When cloud licensing is used in a configuration using a third-party load balancer, GraphOn recommends configuring the hosts to use a Farm Manager. In this case, GO-Global should be activated on the Farm Manager, not the Farm Hosts. If high availability is required, GO-Global should also be activated the failover Farm Manager, and the primary Farm Manager and backup Farm Manager should be configured as a Backup License Server for the other.

Similarly, when cloud licensing is used with a Relay Load Balancer. GO-Global should be activated on the Relay Load Balancer, not on the Dependent Hosts. And if a failover Relay Load Balancer is used, GO-Global should be activated on the failover Relay Load Balancer, and the primary and failover Relay Load Balancers should be configured as Backup License Managers for each other.

GO-Global Application Hosts, Application Host Managers and the GO-Global Activation Wizard cannot traverse proxy servers. To activate GO-Global with a cloud license, the Application Host or Application Host Manager must be able to connect directly to the GraphOn Cloud License Service, cloud.graphon.com (current IP address: 13.52.136.225) on port 443. Similarly, the GO-Global Activation Wizard must be able to connect directly to the GraphOn Portal, portal.graphon.com (current IP address: 52.8.15.135) on port 443. If these conditions are not met, the Activation Wizard will notify you that GO-Global is unable to communicate with the Cloud License Service. You must modify your firewall or proxy server to allow access to the above addresses and ports.

When an on-premises license is used in a configuration using an Application Host Manager and high-availability is not required, the license file should be installed on the Application Host Manager. Alternatively, when an on-premises license is used and high-availability is required, the primary and failover Application Host Managers must be configured to use a set of Three-Server Redundant License Servers.

With all these configurations, the **Licenses** tab on the Admin Console will report the same license information, regardless of which computer is selected.

Prior to version 6.1, GO-Global managed licenses from Application Hosts by default. With this configuration, administrators had to configure each Application Host to use a central license manager. Beginning with version 6.1, administrators no longer need to do this. GO-Global now manages licenses from the Application Host Manager by default. This enables administrators to add and remove Application Hosts from the Application Host Manager without having to make any licensing configuration changes.

Dependent Hosts that are upgraded from version 6.0 and older versions will continue to manage licenses from the Dependent Host. Administrators can change this after the upgrade by editing the value of the **ManageLicensesFrom** property in the **HostProperties.xml** file from Host to **Relay** on all the Dependent Hosts and the Relay Load Balancer.

Administering Relay Load Balancers and Dependent Hosts on Different Networks

When a user starts the Admin Console on a Relay Load Balancer or a Dependent Host, the Admin Console connects to the Relay Load Balancer and attempts to authenticate the user using Integrated Windows authentication. If the Admin Console is running on a Dependent Host and the associated Relay Load Balancer is located on a different network, a message such as the following is displayed:

Failed to log you on to Server8. This computer (Server4) and Server 8 may be located on different networks. Would you like to log onto Server 8 and administer it remotely?

Clicking **No** will return you to the **All Hosts** node of the Admin Console. Clicking **Yes** will initiate a special remote administration session on the Relay Load Balancer as follows:

1. The Admin Console on the Dependent Host starts the GO-Global Client.
2. The client connects to the Relay Load Balancer and starts a session. The **Sign In** dialog is displayed to the user.
3. The user signs in, specifying the user name and password of an account that is a member of the Administrators group on the Relay Load Balancer.
4. The Admin Console starts on the Relay Load Balancer. The user can now administer the Relay Load Balancer and all of its Dependent Hosts.
5. A maximum of two administration sessions can run on the Relay Load Balancer at any given time, regardless of the **Maximum sessions on this host** setting in the Admin Console and regardless of license restrictions.

Dependent Hosts inherit their list of published applications, server settings, and user settings from the Relay Load Balancer. Applications *must* be installed in the same directory on all Dependent Hosts. Applications do not need to be installed on the Relay Load Balancer. When a GO-Global Host is connected to a Relay Load Balancer, all of its server settings are synchronized with those of the Relay Load Balancer.
When any changes are made to the Relay Load Balancer's settings, they are also made to **All Hosts** connected to that Relay Load Balancer. The only settings that are allowed to vary are the maximum number of sessions and the name of the Relay Load Balancer. All other settings in the **Host Options** and **Application Properties** dialogs are grayed out and cannot be modified.

When setting up a Relay Load Balancer, if an application is *installed* but not *published* on the Dependent Host, you will need to publish the application on the Relay Load Balancer through the Admin Console. For example, if Adobe Reader 8.0 is installed on the Dependent Host at C:\Program Files\Adobe\Acrobat 8.0\Reader\AcroRd32.exe, open the Admin Console on the Relay Load Balancer and type this path location in the **Location** box in the **Add Application** dialog.

Before publishing an item on a mapped drive, verify that the drive is mapped to the same drive letter and location on the Dependent Hosts as it is on the Relay Load Balancer.

Host Selection

When a client connects to a Relay Load Balancer, the Relay Load Balancer attempts to start a session on the Dependent Host that has the lowest number of running sessions as a percentage of the maximum number of sessions allowed for the host.

If the session fails to start on the selected host, the Relay Load Balancer successively attempts to start the session on other available hosts until it finds one that can support the session.

If there are no available hosts (i.e., if the number of running sessions on All Hosts equals the maximum number allowed), GO-Global displays a message to the user:
You are already running as many sessions as you are allowed.

Otherwise, if the session cannot be started on any of the available hosts, the following message is displayed to the user:
GO-Global failed to launch the Program Window for your session.

In a Relay Load Balancer setting, GO-Global checks the maximum sessions settings on the Relay Load Balancer and its Dependent Hosts. The maximum sessions value on the Relay Load Balancer is the maximum number of sessions that can be run concurrently on all Dependent Hosts assigned to that Relay Load Balancer.

To modify the **Maximum sessions on this host** setting, open the Admin Console on the host, click Host Options | Session Startup.

Relay Load Balancer in a DMZ

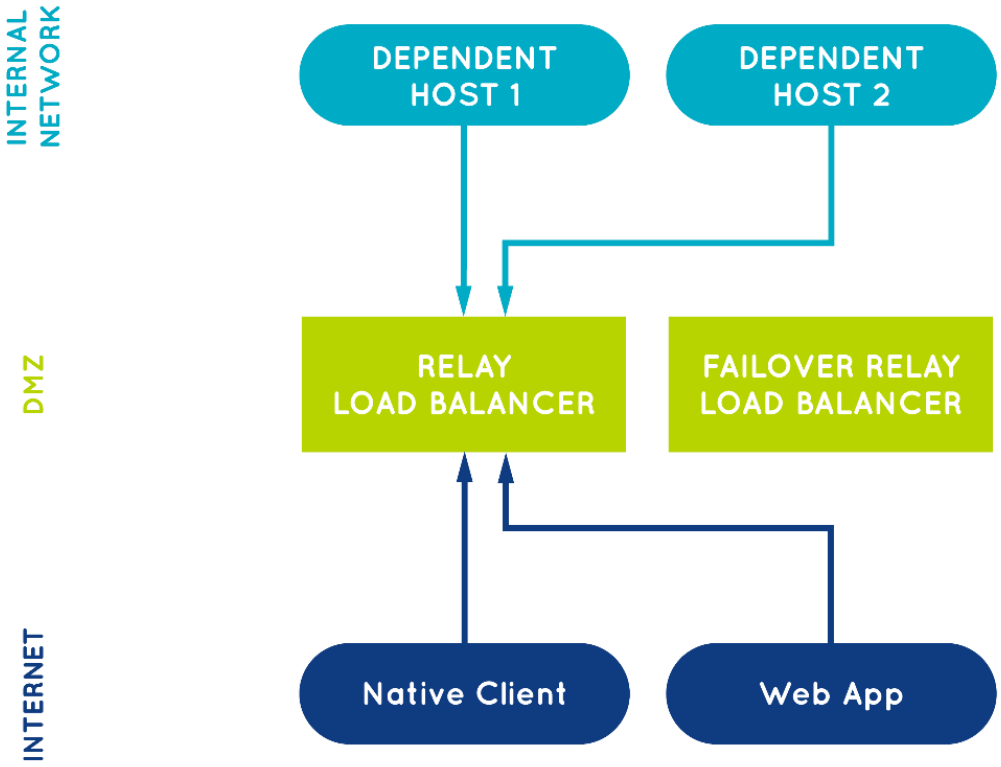
A Relay Load Balancer in a DMZ can be separated from its Dependent Hosts by a firewall, with the following requirements:

- The Dependent Host must be able to connect to the Relay Load Balancer from behind the firewall. Please note that the reverse is *not* required. The Relay Load Balancer does not need to be able to connect to the Dependent Host.

- The client must be able to connect to the Relay Load Balancer in the DMZ.

When a session starts on a Dependent Host, the Dependent Host opens a connection to the Relay Load Balancer. When the Relay Load Balancer receives data from the session's clients, it forwards the data to the session over this connection. Similarly, when the Relay Load Balancer receives data from the session over this connection, it forwards the data to the session's clients. The Relay Load Balancer generally has two network interfaces: one that is accessible from clients outside the DMZ, and one that is accessible from Dependent Hosts behind the firewall.

The diagram below illustrates the recommended configuration for providing access to hosts on an internal network. The arrows show the direction in which the connections are made. Hosts connect to the Relay Load Balancer, not the other way around. As a result, the internal firewall does not need to allow any connections from the DMZ to the internal network. With this configuration, neither machines on the internet nor machines in the DMZ can connect directly to the hosts on the internal network. It is a highly secure configuration.



Application Host Manager Recovery

By default, the Application Publishing Service is configured to automatically restart if the service fails. For example, if the Application Publishing Service stops on a Relay Load Balancer, clients are disconnected but sessions continue to run on the Dependent Hosts that were connected to the Relay Load Balancer. These Dependent Hosts will attempt to reconnect to the Relay Load Balancer every 15 seconds. When a Dependent Host reconnects to the Relay Load Balancer, it re-adds its sessions to the Relay Load Balancer and restores any state information associated with the disconnected sessions. Clients are then able to reconnect to their sessions. By default, clients automatically attempt to reconnect to the Application Host Manager 5 times.

To provide higher service availability, a failover Application Host Manager can be configured.

To configure a Failover Application Host Manager

1. Install the GO-Global Host on a separate computer, on the same network as the Application Host Manager. This computer will be the failover Application Host Manager. All clients and Dependent Hosts (or Farm Hosts) must be able to connect to the failover Application Host Manager. If clients connect to the cluster from the internet, the failover Application Host Manager must have a public address. If the deployment is a cloud environment such as Amazon Web Services, GraphOn recommends installing the failover Application Host Manager in a different Availability Zone than the primary Application Host Manager.

2. Configure the GO-Global Host to run as an Application Host Manager:
    a. Run the **Admin Console** on the computer.
    b. Click Tools | Host Options.
    c. Click the **Configuration** tab.
    d. Click **Application Host Manager**.
    e. If the primary Application Host Manager is a Relay Load Balancer, click **Relay Load Balancer**. If the primary Application Host Manager is a Farm Manager, click **Farm Manager**.
    f. Click **OK**.
    g. Restart the **Application Publishing Service**.

3. Export the published applications from the primary Application Host Manager and import them into the failover Application Host Manager:
    a. On the primary Application Host Manager, run Regedit as administrator.
    b. Select the following registry key:
    \HKEY_LOCAL_MACHINE\GraphOn\GO-Global\AppServer
    c. Click **File** | **Export**...
    d. Type a name for the file (e.g., Appserver.reg).
    e. Click **Save**.
    f. Copy the file to the failover Application Host Manager.
    g. Double-click the file.

h. Click **Yes** to import the file.
i. Click **OK**.

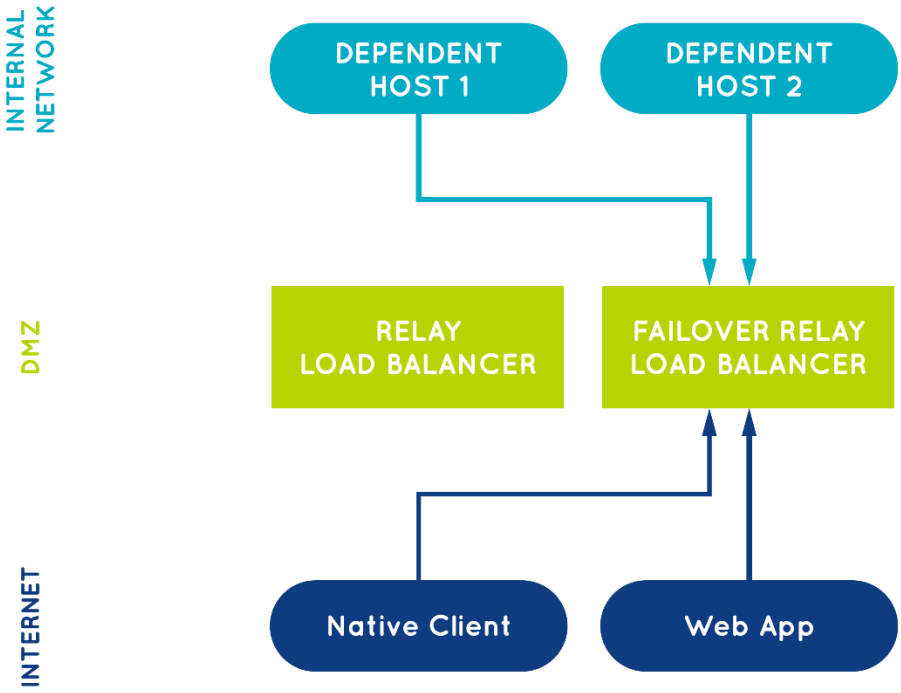
4. Configure each Application Host so it will connect to the failover Application Host Manager when it is unable to connect to the primary Application Host Manager:
   a. Run the Admin Console
   b. Click Tools | Host Options.
   c. Click the **Configuration** tab.
   d. Enter the addresses of both Application Host Managers in the **Relay Load Balancer address** or **Farm Manager** field, with their fully-qualified domain names. Enter the address of the primary Application Host Manager first, followed by a semi-colon, followed by the address of the failover Application Host Manager. For example: primary_relay_load-balancer.graphon.com;failover_relay_load_balancer.graphon.com
   e. Click **OK**.

If the Application Host Managers are Relay Load Balancers, specify the addresses of both the primary and the failover Relay Load Balancers in the URLs and shortcuts that are used to start the clients:

a. Provide users that connect via a browser with an HTML page or URL that sets the **host** parameter to the address of the primary relay server, followed by a semi-colon, followed by the address of the failover relay server
   For example:
   host=primary_relay_load-balancer_address;failover_relay_load_balancer_address

b. Provide users that connect via an installed client, with a shortcut that sets the –h command line argument equal to the address of the primary relay server, followed by a semi-colon, followed by the address of the failover relay server
   For example:
   -h primary_relay_load_balancer_address;failover_relay_load_balancer_address

In a Relay Load Balancer configuration, if the primary Relay Load Balancer fails for any reason, Dependent Hosts and clients automatically reconnect to the failover server and users are generally reconnected to their sessions within 1-2 minutes of the primary Relay Load Balancer failure. This is illustrated in the diagram below.

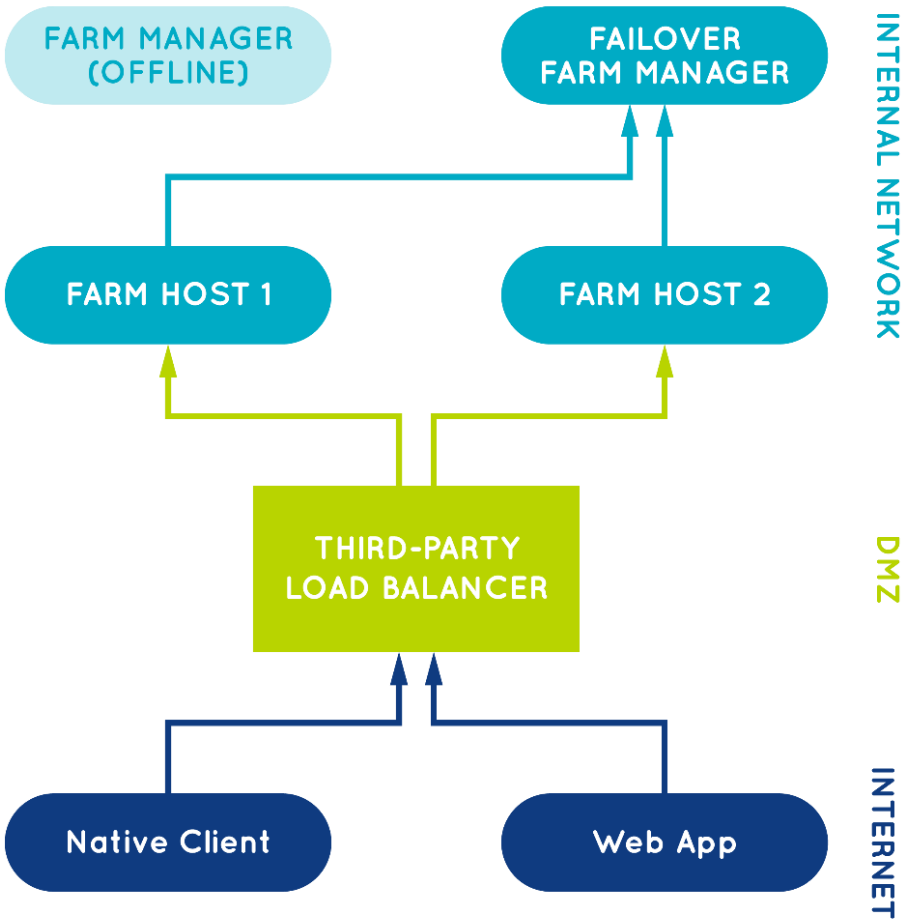


If users' sessions fail to reconnect automatically, increase the value of the **autoreconnect** parameter in client URLs, web pages and shortcuts to a number greater than 5 (the default).

When the failover Relay Load Balancer is active (i.e., when Dependent Hosts are connected to the failover Relay Load Balancer, users' sessions will take longer to start. For this reason, the primary Relay Load Balancer should be re-activated when it comes back online. To re-activate the primary Relay Load Balancer, terminate the aps.exe process on the failover Relay Load Balancer using Task Manager at a time when users are unlikely to be connected to the cluster. When the aps.exe process is terminated on the failover Relay Load Balancer, Dependent Hosts and clients will reconnect to the primary Relay Load Balancer. Then, after the cluster's Dependent Hosts have reconnected to the primary Relay Load Balancer, restart the **Application Publishing Service** on the failover Relay Load Balancer.

When the **Application Publishing Service** is stopped or restarted on a Relay Load Balancer via **Services**, GO-Global closes all the sessions that are running on the Relay Load Balancer's Dependent Hosts. Therefore, if you need to re-activate a primary Relay Load Balancer when there are sessions running on the cluster's Dependent Hosts, don't restart the Application Publishing Service on the failover Relay Load Balancer via Services; instead, terminate the aps.exe process on the failover Relay Load Balancer using Task Manager, as described above.

In a Farm Manager configuration, if the Farm Manager fails for any reason, Farm Hosts automatically reconnect to the failover Farm Manager. When a Farm Host is unable to communicate with a Farm Manager, new sessions will fail to start on the host, and the host will not appear in the Admin Console on the Farm Manager. Unlike with a Relay Load Balancer configuration, however, clients remain connected to their sessions even when the Farm Host is unable to communicate with a Farm Manager. In this way, running sessions are not affected by Farm Manager failures. This is illustrated in the diagram below.



Manually Copying Configuration Settings From one Host to Another

When an Application Host Manager (i.e., Relay Load Balancer or Farm Manager) is used, settings changes are automatically made on all hosts in the cluster. When an Application Host Manager is not used, however, host configuration settings, such as those specified in the Branding dialog, can be manually copied from one computer to another.

To manually copy configuration settings

1. Configure all settings on a sample host as you would like them.
2. Export the following registry key:
   HKEY_LOCAL_MACHINE\Software\GraphOn\GO-Global
3. Stop the **Application Publishing Service** on the target host.
4. Copy the following files from the sample host to the target host:
   %PROGRAMDATA%\Graphon\GO-Global\HostProperties.xml
   %PROGRAMDATA%\Graphon\GO-Global\DefaultWorkspaceProperties.xml
   %PROGRAMDATA%\Graphon\GO-Global\images*.*
5. Run the .reg file created in step 2.
6. Restart the **Application Publishing Service** on the target host.
7. Repeat steps 2-6 for the other hosts.

In a Farm Manager environment, the C:\ProgramData\GraphOn\GO-Global\ks\ks.dat file must be the same on all Farm Hosts.

TLS Configuration with Third-Party Load Balancers

When a third-party load balancer is used and the TLS protocol is required (e.g., when clients will connect to the load balancer over the internet), the TLS protocol may be terminated at either the load balancer or the GO-Global Hosts.

With web applications, it is generally desirable to terminate the TLS protocol at the load balancer because this places the load of negotiating the TLS connections on the load balancer, rather than the application hosts. This is important for web applications because web applications generally open many connections to application hosts for each user session. GO-Global, however, generally only opens one connection per session. Therefore, with GO-Global, there is less of a need to terminate the TLS protocol at the load balancer. There are situations, however, where it is desirable to do this.

To terminate TLS at the load balancer

1. Configure the GO-Global Hosts to use the TCP protocol and no encryption:
    1. Run the **Admin Console** on the Farm Manager.
    2. Click Tools | Host Options.
    3. Click the **Security** tab.
    4. Under **Protocol**, select **TCP**.
    5. Under **Encryption**, select **None**.
    6. Click **OK**.

2. If a failover Farm Manager is used, ensure that it has the same settings.
   This may be done by either:
    - Repeating step 1 on the failover Farm Manager
      -or-
    - Copying the **HostProperties.xml** file from the primary Farm Manager to the failover Farm Manager

3. Configure the load balancer to use the **TLS** protocol. For example, if using an Amazon Web Services Network Load Balancer, set the Protocol of the Listener to TLS and install the TLS certificate on the load balancer.

If the TLS certificate is a wildcard certificate, the domain specified by the certificate's Common Name must match the domain of the address that clients use to connect to the load balancer. Alternatively, if the TLS certificate is not a wildcard certificate, the certificate's Common Name must match the address that clients use to connect to the load balancer.

4. Enable the TLS option in AppController and/or the GO-Global Web App:
    - For AppController, add **-tls 1** to the AppController command line.
    - For the GO-Global Web App, add **tls=true** to the URL or set **tls=true** in the logon.html file.

When the TLS protocol is terminated at the load balancer, data is encrypted between the clients and the load balancer but is not encrypted between the load balancer and the hosts. When data must be encrypted end-to-end from the clients to the hosts, the TLS protocol should be terminated at the hosts.

Application Host Manager Considerations

When an Application Host Manager (i.e., Relay Load Balancer or Farm Manager) is configured to use TLS, the name entered into the **Relay Load Balancer** or **Farm Manager** field on the Application Hosts must match the Common Name, the wildcard domain, or one of the Subject Alternative Names (SAN) of the certificate. If they do not match, or if there is a problem with the certificate, the Application Hosts will fail to connect to the Application Host Manager, and they will not appear under the Application Host Manager in the Admin Console.

For information about using the TLS Protocol with Farms Hosts and Farm Managers, see:

- Terminating TLS at the GO-Global Hosts
- Application Host Manager Recovery

Troubleshooting TLS Issues Between Application Hosts & Application Host Managers

When an Application Host does not appear under underneath the Application Host Manager in the Admin Console's tree view, check the Application Publishing Service log. If it contains a message that the certificate is invalid, there is a TLS configuration problem.

Possible causes include:

- The name entered into the **Relay Load Balancer** or **Farm Manager** field on the Application Host does not match the Common Name, the wildcard domain, or one of the Subject Alternative Names (SAN) of the certificate.
- The certificate file on the Application Host Manager does not have one or more intermediate certificates concatenated.
- The certificate on the Application Host Manager is not in PEM format.
- The certificate on the Application Host Manager is not trusted by the Application Host (i.e., the root certificate in the certificate's certificate chain is not included in the list of Trusted Root Certificates on the Application Host.
- The certificate is expired or system date is incorrect.

When troubleshooting issues like this, it is sometimes helpful to run AppController on the Application Host and try to connect to the Application Host Manager. This can be helpful because AppController provides additional information about TLS errors.

To do this:

1. Browse to the GO-Global\Programs directory on the Application Host and double-click **AppController.exe**.
2. Type the address of the Application Host Manager into the **Connection** dialog. Type the address exactly as it is specified in the **Relay Load Balancer** or **Farm Manager** field of the Host Options dialog on the Application Host.
3. Click **Connect**.

If a TLS warning message is displayed, the dialog will describe the problem. For example, if it says the certificate is from an organization that you have not chosen to trust, the problem is most likely that an intermediate certificate is not concatenated. Alternatively, it could mean that the certificate's certificate chain is not included in the list of Trusted Root Certificates on the Application Host.

The message below illustrates three sequential warnings:

In this example, these issues were identified:

- The certificate on the Application Host Manager is not trusted by the Application Host (i.e., the root certificate in the certificate's certificate chain is not included in the list of Trusted Root Certificates on the Application Host.
- The certificate is expired or system date is incorrect.
- The name entered into the **Relay Load Balancer** or **Farm Manager** field on the Application Host does not match the Common Name, the wildcard domain, or one of the Subject Alternative Names (SAN) of the certificate.

If no TLS warning dialog is displayed, but a different error message is displayed (e.g., *No available hosts*), the TLS configuration is likely not the issue. For the purposes of this test, you can disregard any error messages that do not pertain to the ability of the client to open a connection to the Application Host Manager.

Terminating TLS at the GO-Global Hosts

Terminating TLS at the GO-Global Hosts has the following requirements:

- Independent hosts can use a single domain or SAN certificate, provided that the common name (CN) or SAN matches the host public FQDN. For example, independent-host1.example.com. Independent hosts can also use a wildcard certificate.

- Farm and Relay Load Balancer deployments require a wildcard or SAN certificate. For a SAN, all hostnames (and if in use, load balancer) must be present. For example: farmmanager1.example.com, farmhost1.example.com, loadbalance.example.com. All hosts must be able to resolve all the hosts' FQDN hostnames.

- GO-Global can work with all types of public certificate validation, including domain (DV), organization (OV) or extended (EV). GO-Global supports certificates issued by your company's private Certificate Authority (CA). The root certificate of your company's CA needs to be trusted by hosts and end user devices.

- When TLS is terminated at Farm Hosts, the **RelayConnectionAddress** must be a FQDN that resolves to the internal IP address of the Farm Host from all Farm Hosts in the farm and the domain name of the FQDN must match either the Common Name or a Subject Alternative Name of the TLS certificate.

To terminate TLS at the GO-Global Hosts

1. Configure the Farm Manager and Farm Hosts to use the TLS protocol:
   a. Run the **Admin Console** on the Farm Manager.
   b. Click Tools | Host Options.
   c. Click the **Security** tab.
   d. Under **Protocol**, select **TLS**.
   e. Under **Encryption**, select the desired encryption.
   f. Type or browse to the path of the server's certificate (e.g., server.crt) file in the **Certificate** box.
   g. Click **OK**.

The **server.crt** and corresponding **server.key** file must use the same filename and be placed in the same directory. We recommend using the C:\ProgramData\GraphOn\GO-Global\ks\certs directory. If the certificate has intermediate CAs, it will need to be concatenated.

If the TLS certificate is a wildcard certificate, the domain specified by the certificate's Common Name must match the domain of the address that clients use to connect to the load balancer. Alternatively, if the TLS certificate is not a wildcard certificate, the certificate's Common Name must match the address that clients use to connect to the load balancer.

2. If a failover Farm Manager is used, ensure that the certificate is a wildcard or SAN certificate and configure the failover Farm Manager to use the same settings as the primary Farm Manager.

   This can be done by either:

   - Repeating step 1 on the failover Farm Manager
     -or-
   - Copying the certificate and the HostProperties.xml file from the primary Farm Manager to the failover Farm Manager and restarting the Application Publishing Service

3. On each Farm Host:
   a. Copy the TLS certificate to the location specified at step 1f.
   b. Verify that the addresses of the primary and failover Farm Managers specified in the **Farm Manager address** field of the **Configuration** tab of the Host Options dialog meet the requirements of the TLS certificate's Common Name. For example, if the certificate is a wildcard or SAN certificate, ensure that the addresses match the domain name specified by the certificate's Common Name.

c. Verify that the Farm Host can connect to the primary and failover Farm Managers using the addresses that are specified in the **Farm Manager address** field of the **Configuration** tab of the **Host Options** dialog.

   This can be done by either:

   - Configuring internal DNS to map the addresses for the primary and failover Farm Managers to the internal IP addresses of the respective Farm Managers. If your internal and certificate FQDNs are not identical, then this is often implemented via a split DNS setup.

     -or-

   - Adding entries to the C:\Windows\System32\drivers\etc\hosts file on the Farm Host that map the addresses of the primary and failover Farm Managers to the internal IP addresses of the respective Farm Managers.

d. Copy %PROGRAMDATA%\GraphOn\GO-Global\ks\ks.dat from one Farm Host to every other Farm Host's %PROGRAMDATA%\GraphOn\GO-Global\ks\ directory. This ensures that all Farm Hosts use an identical copy of ks.dat for the password caching option.

e. Edit HostProperties.xml and update the value of **RelayConnectionAddress** to this Farm Host's FQDN. It must be an FQDN that resolves to the internal IP address of the Farm Host (and also resolvable from all Farm Hosts in the farm). The domain name of the FQDN must match either the Common Name (CN) or a Subject Alternative Name (SAN) of the certificate. For example, update the RelayConnectionAddress value on farmhost3 to farmhost3.example.com

4. Configure your third-party load-balancing rule to use the TCP protocol. The *health probe* can use HTTPS or TCP. For example, when using an Amazon Web Services Network Load Balancer, set the Protocol of the Listener to TCP.
   Note: If your load balancer front end uses port 443 instead of 491, edit logon.html on every Farm Host, replacing:
   // controlArgs.set(["port","491"]);
   with
   controlArgs.set(["port","**443**"]);

5. Do *not* enable the TLS option in AppController and/or the GO-Global Web App. In this case, the host will automatically instruct the client to use the TLS protocol.

6. Restart the **Application Publishing Service** on the Farm Manager.

TLS Configuration with Relay Load Balancers and Dependent Hosts

When a Relay Load Balancer is used, users' data is transmitted not only between users' clients and the Relay Load Balancer, but also between Dependent Hosts and the Relay Load Balancer. When sensitive data will be transmitted in users' sessions, the TLS protocol should be used. TLS secures the communication between clients and the Relay Load Balancer and between Dependent Hosts and the Relay Load Balancer.

The primary function of the TLS protocol is to ensure that clients are connected directly to the Relay Load Balancer and that there is no "man-in-the-middle" server between a client and the Relay Load Balancer capturing users' data. To ensure that there is no man-in-the-middle, the client compares the address that it used to connect to Relay Load Balancer to the Common Name *or one of the Subject Alternative Names* of the Relay Load Balancer's TLS certificate. If these do not match, the client will display a warning to the user. For example, if a user attempts to connect to a Relay Load Balancer using its IP address, the client will display a warning because the IP address will not match the Common Name *or one of the Subject Alternative Names* in the Relay Load Balancer's certificate.

Similarly, when a Dependent Host connects to a Relay Load Balancer, the Dependent Host compares the address that it used to connect to the Relay Load Balancer to the Common Name or one of the Subject Alternative Names of the Relay Load Balancer's certificate. If they don't match, the Dependent Host will reject the connection. The Dependent Host will reject the connection rather than display a warning because there is no way for the Application Publishing Service on the Dependent Host to display a message to the administrator.

More specifically, when the TLS protocol is selected on the Relay Load Balancer, the address specified in the **Relay Load Balancer address** field on the **Server Role** tab of the **Host Options** dialog on each Dependent Host must match the Common Name or one of the Subject Alternative Names of the Relay Load Balancer's certificate. It may not, for example, be set to the IP address of the Relay Load Balancer. If it is, the Dependent Host will fail to connect to the Relay Load Balancer.

In addition to matching the Common Name or one of the Subject Alternative Names of the certificate, the address specified in each Dependent Host's **Relay Load Balancer address** field must resolve to the internal IP address of the Relay Load Balancer. Otherwise, the Dependent Host won't be able to connect to the Relay Load Balancer.

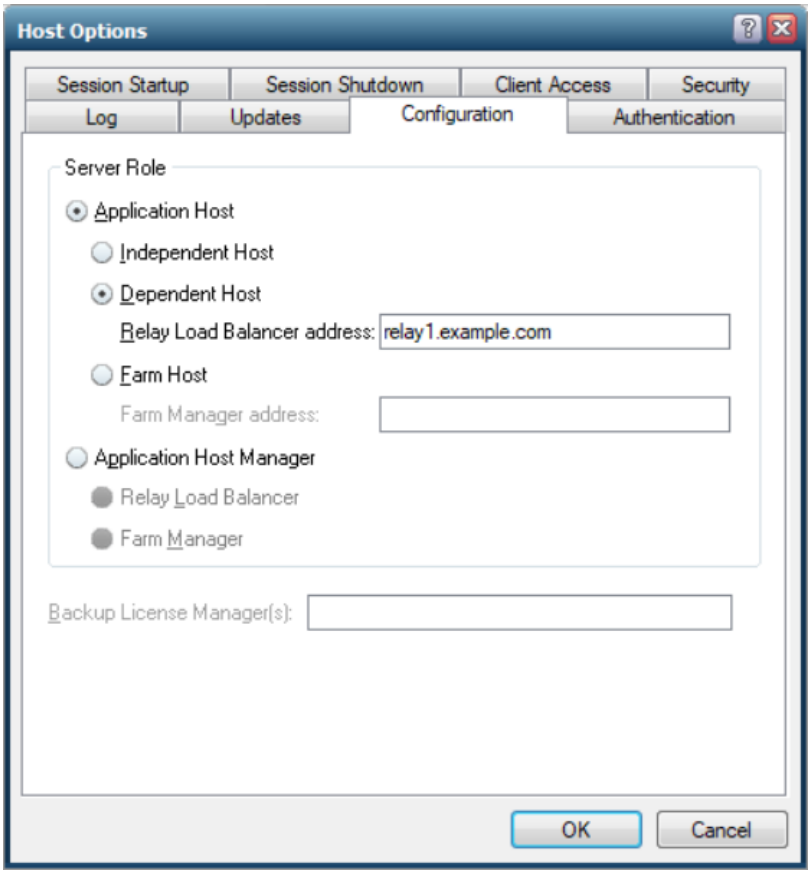
This can be done by either:

- Configuring internal DNS to map the **Relay Load Balancer address** to the internal IP address of the Relay Load Balancer
  -or-
- Adding and entry to the C:\Windows\System32\drivers\etc\hosts file on each Dependent Host that maps its **Relay Load Balancer address** to the internal IP address of the Relay Load Balancer

In summary, when the TLS protocol is enabled on a Relay Load Balancer, the following addresses must match the Common Name or one of the Subject Alternative Names of the Relay Load Balancer's certificate:

- The address that clients use to connect to the Relay Load Balancer, e.g., the address specified after https:// when users connect from a browser

- The address that Dependent Hosts use to connect to the Relay Load Balancer, which is specified in the **Relay Load Balancer address** field on the **Configuration** tab of the **Host Options** dialog on the Dependent Hosts.



If the Relay Load Balancer's certificate is a wildcard certificate, only the domain names of the addresses must match the Common Name or one of the Subject Alternative Names of the certificate.

If a failover Relay Load Balancer is used, the certificate must be a wildcard certificate, and it must be installed on both the primary Relay Load Balancer and the failover Relay Load Balancer. In addition, the address of the failover Relay Load Balancer must be mapped to the internal IP address of the failover Relay Load Balancer via DNS or the Dependent Host's C:\Windows\System32\drivers\etc\hosts files.

In Relay Load Balancer environments, the TLS certificate does not need to be installed on Dependent Hosts because Dependent Hosts connect *to* Relay Load Balancers; Relay Load Balancers do not connect to Dependent Hosts.

When a Relay Load Balancer is used, connections from browsers should specify HTTPS, (e.g., https://relay_lb_address/), but the TLS option should *not* be specified in the URL. Similarly, the TLS command line options should *not* be specified when AppController is used to connect to a Relay Load Balancer. The TLS protocol will be selected automatically when it is enabled on the Relay Load Balancer.

CHAPTER VIII

Authentication

8

Standard Authentication

Standard authentication is the default method for authenticating users on a GO-Global Host. Standard authentication allows users to sign in to GO-Global via the **Sign In** dialog by typing their user name and password. Once authenticated, users are added to the host's INTERACTIVE group and given the same access rights as if they had signed in to the host at its console.

To enable Standard authentication

1. Click Tools | Host Options.
2. Click the **Authentication** tab.
3. Click **Standard authentication (prompt for user name and password)**.
4. Click **OK**.

When Standard Authentication is used, GO-Global creates a Windows session and runs GO-Global's logon.exe program in the session whenever users connect to the GO-Global Host. The logon.exe program creates GO-Global's **Sign In** dialog, and GO-Global provides remote access to the dialog from the GO-Global Client in the same way that it provides remote access to other applications that run in the GO-Global session.

Creating a Windows session consumes a significant amount of memory. Because of this, Standard Authentication is not recommended for internet deployments where malicious actors can easily open a number of connections to a GO-Global Host and exhaust its resources, making it unavailable for users. For internet deployments, GraphOn recommends OpenID Connect authentication. With OpenID Connect authentication, users must authenticate before GO-Global creates a Windows session. In addition, most OpenID Connect identity providers have protections against other forms of distributed denial-of-service (DDoS) attacks.

Integrated Windows Authentication

Integrated Windows authentication allows users to connect to a GO-Global Host and start a session without having to sign in to the host and re-enter their user name and password. When Integrated Windows authentication is the only option enabled, the user's user name and password are never transmitted over the network. Instead, GO-Global simply runs the user's session in the same security context as the GO-Global Client.

Integrated Windows authentication is only available to users who sign in from Windows computers that are members of either the same domain as the GO-Global Host or Trusted Domains of the GO-Global Host. It is only supported when AppController for Windows is installed on the client computer. It is not supported when users connect to the host using the GO-Global Web App or any of the non-Windows versions of AppController. If users will be connecting to the host from any of these platforms, Standard Authentication must be enabled in addition to Integrated Windows Authentication.

When users connect to a GO-Global Host using Integrated Windows authentication, they are added to the host's NETWORK group instead of its INTERACTIVE group. As members of the NETWORK group, users can access most of the same resources on the host that they would be able to access had they signed in to the host interactively. However, when users access resources that reside on other computers on the network, they might be required to re-enter their user name and password. And if network resources are unable to request a username and password, access might be denied.

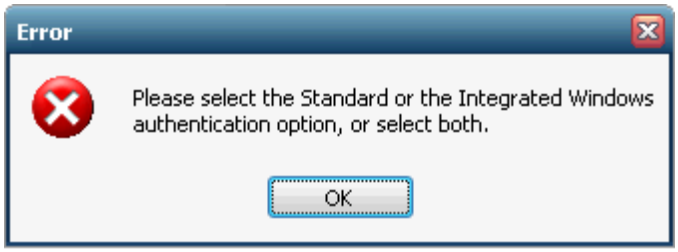
To access other computers on the network, the Active Directory must be configured to allow authentication credentials to be passed to other computers. Microsoft refers to the right to pass authentication credentials to a third or more computers as "delegation." Delegation is supported on Active Directory networks with the proper settings. Please refer to your Microsoft Windows operating system documentation for instructions on properly configuring an Active Directory Domain Controller. See Configuration Requirements for Delegation Support for more information.

The **Cache passwords on the host** option, described in the following section, can be enabled to obtain an INTERACTIVE group logon with Integrated Windows Authentication.

To enable Integrated Windows Authentication

1. Click Tools | Host Options.
2. Click the **Authentication** tab.
3. Enable **Integrated Windows authentication**.
4. Click **OK**.

GO-Global requires that either Standard authentication or Integrated Windows authentication be enabled. If neither one of these authentication methods is selected, and you click **OK** to close the dialog, the following error message is displayed:



If both Standard authentication *and* Integrated Windows authentication are enabled, the GO-Global Host will first attempt to log the user on via Integrated Windows authentication. If this fails, GO-Global will then attempt to log the user on with Standard authentication by presenting the **Sign In** dialog and requiring a user name and password.

Granting Launch and Activate COM Rights to Standard Users

By default, Windows does not grant standard users who have not signed in to Windows interactively by entering a username and password the right to launch and activate COM objects. As a result, applications such as Windows File Explorer that rely on COM interfaces may only run or work properly for users who are members of the Administrators group when Integrated Windows Authentication is used. Therefore, when Integrated Windows Authentication is enabled, grant standard users *Launch and Activation* COM rights as follows:

1. Run dcomcnfg.
2. Navigate to Component Services | Computers | My Computer.
3. Right-click **My Computer** and click **Properties**.
4. Select the **COM Security** tab.
5. Under Launch and Activation Permissions, click the **Edit Default...** button.
6. Click the **Add** button. (*Note*: The default permissions grant full rights to the INTERACTIVE and Administrators groups. This is why this works for all users authenticated via a username and password (INTERACTIVE users) and members of the Administrators group when Integrated Windows Authentication is used.
7. Add the **Domain Users** group.
8. Click the **Allow** checkboxes next to **Local Launch** and **Local Activation**.
9. Click **OK**.
10. Click **OK**.

Password Caching on the Host

When a user signs in to a GO-Global Host with standard authentication (either with a user name and password supplied by the **Sign In** dialog, parameters, or command-line arguments), that user is added to the host's INTERACTIVE group. Alternatively, a user that signs in to a GO-Global Host using integrated Windows authentication is added to the host's NETWORK group. By default, members of the INTERACTIVE group have greater access to the host's resources than members of the NETWORK group. As a result, a user that signs in via Integrated Windows authentication may encounter "access denied" errors under several conditions.

Areas restricted from members of the NETWORK group include DCOM (also known as OLE and COM/COM+) security limitations, file security limitations, and application specific security checking. Administrators should verify that all resources (files, services, etc.) that Integrated Windows authenticated users need to access have the proper security settings to allow that access.

To avoid these errors, administrators can enable delegation to allow processes running in GO-Global sessions to access specified services on the network. This procedure is described in the Configuration Requirements for Delegation Support section.

Alternatively, administrators can work around these limitations by enabling the **Cache passwords on the host** option. Doing so allows users to sign in with full INTERACTIVE access rights without having to enter their user name and password every time they connect. Users are prompted for a password when first connecting to the host or following a password change. Passwords are encrypted and stored within their respective profiles. With subsequent connections to GO-Global, users are automatically signed in and added to the host's INTERACTIVE group. They are granted the same access rights had they signed in to the host at its console.

GO-Global encrypts passwords using an RSA algorithm with a 512-bit key that is stored on the host. The encryption key is stored in the C:\ProgramData GraphOn\GO-Global\ks\ks.dat file. Only members of the host's Administrators group and the SYSTEM account can read this file.

To enable password caching on the host

1. From the Admin Console click Tools | Host Options.
2. Click the **Authentication** tab.
3. Enable **Integrated Windows authentication**.
4. Enable **Cache passwords on the host**.
5. Click **OK**.

The ks.dat file needs to be copied from one Farm Host in a farm to all Farm Hosts in the farm.

Password Caching on the Client

Client-side password caching allows users who are not members of the GO-Global Host's domain to sign in to GO-Global without having to enter their user name and password every time they connect to the server. When **Cache password on the client** is enabled, the **Sign In** dialog includes a **Remember me on this computer** check box. If the user enables this, after the first manual authentication, the user's logon credentials are encrypted on the host, transmitted over the network, and stored on client computers in user-private directories.

When the user makes subsequent connections to the host, the cached password is transmitted back to the host, where it is decrypted. The **Sign In** dialog is displayed with the user name and password and with **Remember me on this computer** checked. If the user disables the **Remember me on this computer** option, the user's credentials will be deleted from the client computer.

GO-Global caches passwords on the client using an RSA algorithm with a 512-bit key that is stored on the host. The encryption key is stored in the %ALLUSERSPROFILE%\GraphOn\AppController\ks\ks.dat file. Only members of the host's Administrators group and the SYSTEM account can read this file.

To enable client-side password caching

1. From the Admin Console click Tools | Host Options.
2. Click the **Authentication** tab.
3. Enable **Standard authentication (prompt user for user name and password)**.
4. Enable **Cache passwords on the client**.
5. Click **OK**.

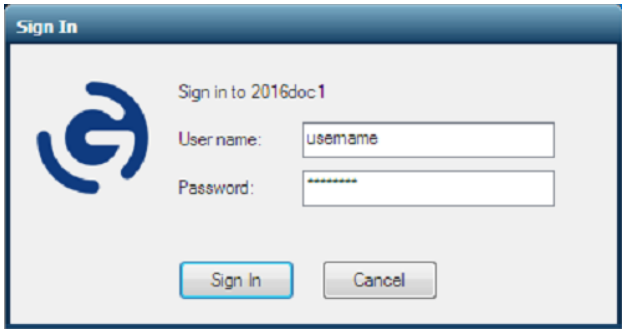
On most platforms, the cached password is stored in the user's home directory in a .dat file named for the GO-Global Host. The table below provides example locations of the cached password. In the examples, *user1* is the user name, and *hostname.domain.com* is the address of the GO-Global Host.

Platform	Password Locations
macOS	/Users/user1/.AppController/hostname.domain.com.dat
Windows	\Users\user1\AppData\Roaming\GraphOn\AppController
Linux	/home/user1/.AppController/hostname.domain.com.dat

Client-side password caching is supported on all GO-Global clients.

Bypassing the Sign In Dialog

By default, when **Cache password on the client** is enabled and the user has enabled **Remember me on this computer**, the **Sign In** dialog is displayed with the user name and password, when the user connects to the host.



Administrators can opt to *not display* the **Sign In** dialog to the user when **Cache password on the client** is enabled by setting the **showLogonCachedPassword** property in the Host Properties XML file to false.

To prevent the Sign In dialog from being displayed

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\HostProperties.xml in a text editor.
3. Find the **showLogonCachedPassword** property and change its associated value to "false".
4. Save HostProperties.xml.
5. Start the **Application Publishing Service**.

Administrators can override the value of the **showLogonCachedPassword** property by adding the **showlogon** parameter to the command line or the logon URL. If **showlogon 0** is added to the shortcut's command line, or **showlogon=false** is added to the logon URL, the **Sign In** dialog will *not* be displayed to the user, regardless of the **showLogonCachedPassword** property value.

For example,

To bypass the Sign In dialog via a shortcut (when Cache password on the client is enabled)
Add the argument -showlogon 0 to the AppController shortcut.
For example,
"C:\Program Files (x86)\GraphOn\AppController\AppController.exe" -showlogon 0

To bypass the Sign In dialog via the logon page (when Cache password on the client is enabled)
Add showlogon=false to the URL.
For example,
http://hostname/goglobal/logon.html?showlogon=false

Password Change

Users can change passwords when:

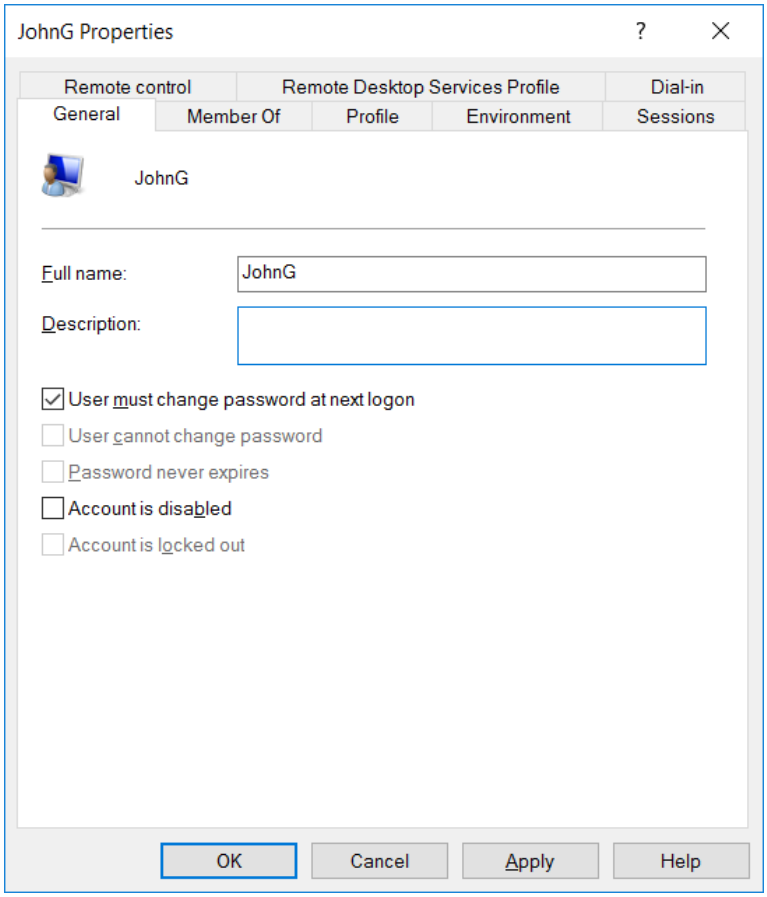
a. The administrator requires the user to change his or her password at the next logon;
b. The security policy is configured to prompt users to change passwords before expiration; and
c. The user's password has expired.

Changing Passwords at Next Logon

Administrators can require a user to change his or her password by checking the **User must change password at next logon** option in the **Administrator Properties** dialog. (For Local accounts, this dialog can be accessed by clicking My Computer | Local Users and Groups | Users | *UserName* | Properties).

To sign in when the *User must change password at next logon* option is enabled for a user's account

1. Run the GO-Global client (e.g., browse to http://hostname/goglobal/).
2. Type the user name and password in the **Sign In** dialog. If the user account does not exist in the domain in which the GO-Global Host resides, include the domain name in the **User name** field as a prefix (e.g., domain\username).
3. Click **OK**.
4. Click **OK** to the following message: “You are required to change your password at first logon.”
5. Type a new password in the New Password and Confirm New Password fields of the Change password dialog.
6. Click **OK**.



Prompting Users to Change Passwords Before Expiration

By default, users are prompted to change their passwords whenever they log on within 14 days of their password's scheduled date of expiration. Administrators can modify the change password "prompt" period by editing the **Prompt user to change password security** setting. For example, the local security setting can be viewed and changed by clicking Start | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Option.

To sign in during the password change "prompt" period

1. Run the GO-Global client (e.g., browse to http://hostname/goglobal/).
2. Type the user name and password in the **Sign In** dialog.
3. Click **OK**.
4. The following message is displayed:
   Your password will expire in x day(s). Do you want to change your password now? Yes/No
   If the user clicks **No**, the GO-Global session will start. If **Yes**, the **Change Password** dialog is displayed.
5. Type a new password in the **New Password** and **Confirm New Password** fields.

Prompting Users to Change Passwords After Expiration

To sign in after a password has expired

1. Run the GO-Global client (e.g., browse to http://hostname/goglobal/).
2. Type the user name and password in the **Sign In** dialog. If the user account does not exist in the domain in which the GO-Global Host resides, include the domain name in the **User name** field as a prefix (e.g., domain\username).
3. Click **OK**.
4. Click **OK** to the following message:
   Your password has expired and must be changed.
5. Type a new password in the **New Password** and Confirm **New Password** fields of the **Change Password** dialog.
6. Click **OK**.

Password Change and Integrated Windows Authentication

When Integrated Windows Authentication is enabled, GO-Global relies on the operating system of the client to change passwords. For example, GO-Global supports the following scenario:

1. The administrator edits a user's settings and specifies that the **User must change password at next logon**.
2. Upon logging on, the user is prompted to change his or her password.
3. The user changes the password and signs in to the client computer.
4. The user starts the GO-Global client and connects to a GO-Global Host.
5. The password has already been changed, so the user is authenticated on the host without being prompted for a password, unless the **Cache passwords on the host** option is enabled. In this case, the user will be prompted to enter a new password.

If, however, the administrator specifies that the **User must change password at next logon** after the user has logged on to the client computer, and the user subsequently connects to a GO-Global Host that has Integrated Windows authentication enabled, authentication may fail. If it fails and both the **Integrated Windows authentication** and **Cache passwords on the host** option are enabled, the user will be prompted to sign in and make a password change as described above.

In the Admin Console's dialog boxes, you can easily get Help by right-clicking an item, and then clicking **What's This?** A pop-up window will appear, displaying a brief explanation of the item. You can also get Help by clicking ? on the title bar of a dialog box and then selecting an item.

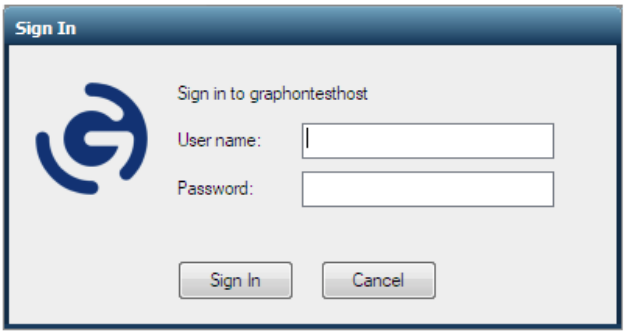
Two-Factor Authentication

Two-Factor Authentication (2FA), also known as Multi-Factor Authentication (MFA), provides an extra layer of security by optionally requiring end users to enter a 6-digit code from a time-based one-time password (TOTP) authenticator app on a device (smart phone, PC, etc.) in addition to their user name and password. This significantly reduces the risk of brute force and dictionary attacks, which is especially critical as more end users access corporate work computers while working from insecure home networks. GO-Global's native 2FA feature does not require any external services. It requires that all users have a device with an authenticator app such as Google Authenticator or Authy, or a password manager such as Bitwarden installed.

To enable two-factor authentication

1. Click Tools | Host Options.
2. Click the **Authentication** tab.
3. Enable **Require two-factor authentication**.
4. Click **OK**.

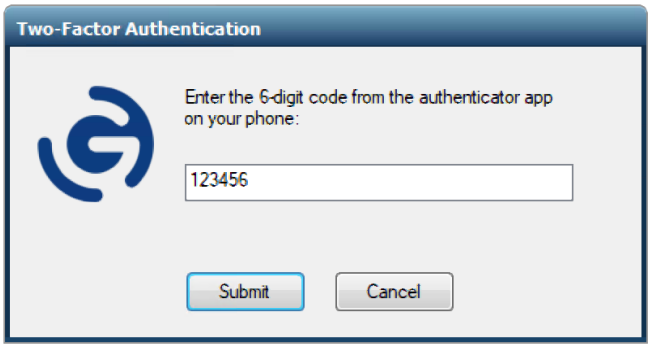
When users connect to a GO-Global Host that requires two-factor authentication, they are prompted to enter their user name and password via the **Sign In** dialog:



They are then prompted to register for two-factor authentication:

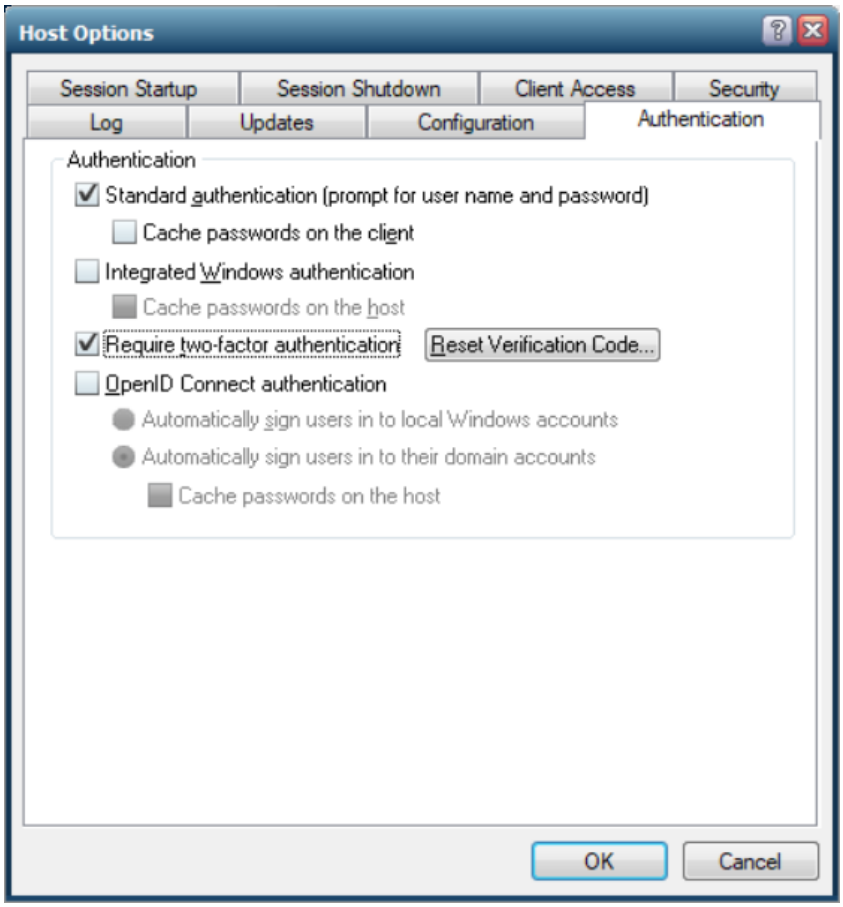
Following the prompts, users scan the QR code using an authenticator app on their phone:

After scanning the QR code and clicking **Next** on the Two-Factor Authentication dialog, users are prompted to enter a 6-digit code from the app on their phone.



When users who have already registered for two-factor authentication connect to a GO-Global Host, they are first prompted to enter their user name and password via the **Sign In** dialog, then prompted to enter the six-digit code from their authenticator app.

When two-factor authentication is enabled in multi-host environments, roaming profiles should also be enabled. This is because the verification codes used in two-factor authentication are stored in users' User Profiles. When roaming profiles are enabled, users only need to scan a QR code once, regardless of how many hosts there are. Alternatively, when roaming profiles are not enabled, users will be prompted to scan a QR code every time they connect to a new host.
Therefore, roaming profiles should be enabled in multi-host environments when two-factor authentication is enabled.



Resetting User Verification Codes

The Admin Console allows administrators to reset a specific user's verification code, if that user deleted the authenticator app or lost his or her phone, for example. Administrators can also reset the verification code for all users.

To reset the user verification code for a specific user or specific users

1. Click Tools | Host Options.
2. Click the **Authentication** tab.
3. Click the **Reset Verification Code** button.
4. Select **Reset the verification codes of specific users**.
5. Type the user's **User Principal Name (UPN)** in the form of user@example.com. To reset multiple users' verification codes, type their User Principal names, separated by a comma.
6. Click **Ok**.

To reset the user verification codes for all users

1. Click Tools | Host Options.
2. Click the **Authentication** tab.
3. Click the **Reset Verification Code** button.
4. Select **Reset the verification codes for all users**.
5. Click **Ok**.

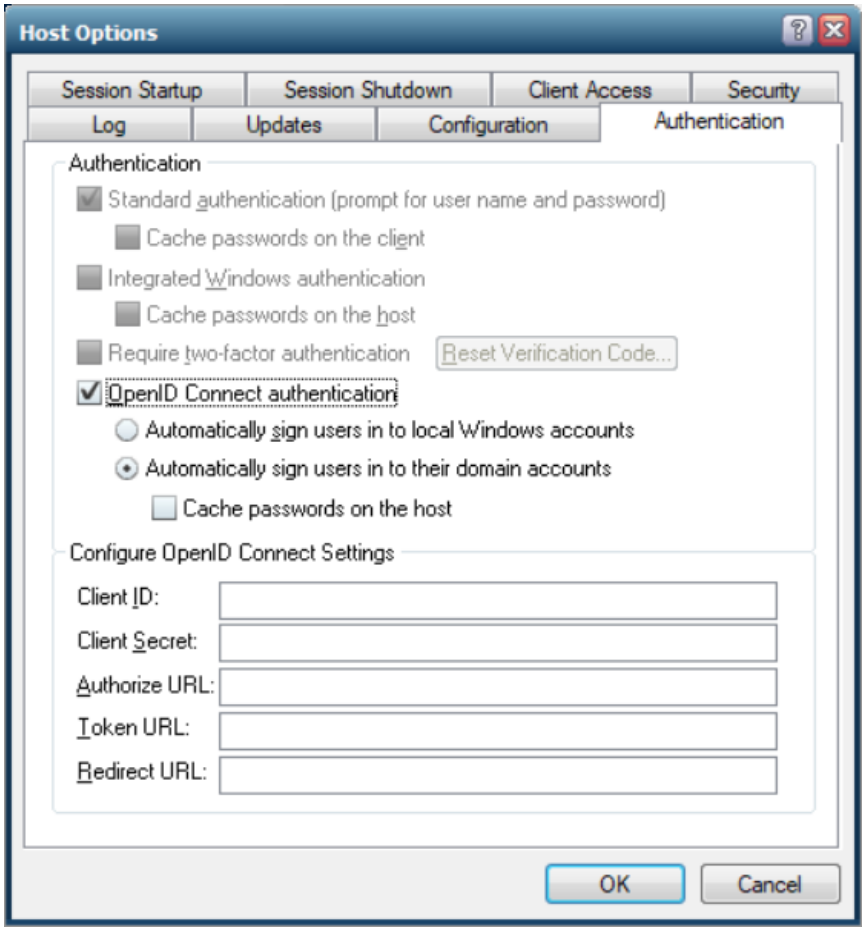
When users sign in to a host using a local workgroup account rather than a domain account, administrators cannot reset users' verification codes from the Admin Console. This is because local workgroup accounts do not have User Principal Names.

To work around this, an administrator can directly delete the verification code file from the user's profile. The file is located in the user's profile at %APPDATA%\GraphOn\GO-Global\mfa.txt (i.e., C:\Users\exampleUser\AppData\Roaming\GraphOn\GO-Global\mfa.txt). (Users do not have access to this file.)

OpenID Connect Authentication

OpenID Connect (OIDC) authentication provides users with single sign-on support via OIDC identity providers such as Okta and Active Directory Federated Services (ADFS). It enables users who sign in to an enterprise web application or portal using an identity provider to access GO-Global Hosts from their browsers without having to re-enter their credentials. OIDC also enables hosting providers to delegate user management and authentication to their customers, and it enables users to authenticate to GO-Global Hosts using a wide variety of third-party smart cards and multi-factor authentication devices and products.

After a user has authenticated via OIDC, GO-Global gives administrators several options for authenticating the user automatically on Windows. For example, if the identity 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 create a local Windows account for the user and automatically sign the user in to that account.



Single sign on support is an add-on option. **OpenID Connect authentication** will be grayed out (disabled) unless the feature has been purchased.

To enable OpenID Connect Authentication

1. Click Tools | Host Options.
2. Click the **Authentication** tab.
3. Enable **OpenID Connect authentication**.
4. Select one or neither of the following options:

   - **Automatically sign users in to local Windows accounts.** When this is enabled, GO-Global will automatically create a local user account for users that don't have a domain account.

- **Automatically sign users in to their domain accounts.** When this is enabled, GO-Global attempts to perform an S4U login using the user's UPN, which it obtains from the OIDC identity provider after a successful OpenID Connect login. By itself, an S4U login will enable users to access resources on the GO-Global Host, but users will not be able to authenticate to services running on the network. To access services running on the network, administrators must either enable constrained delegation as described in the Configuration Requirements for Delegation Support section or enable the **Cache passwords on the host** option.

If an application that is hosted by GO-Global can run under a local account on the GO-Global Host, **Automatically sign users in to local Windows accounts** should be selected. Alternatively, if the application requires access to resources that are managed by Active Directory, **Automatically sign users in to their domain accounts** must be selected. In this latter case, the identity provider must be integrated with the Active Directory so it can provide GO-Global with the UPN of the user.

If neither **Automatically sign users in to local Windows accounts** nor **Automatically sign users in to their domain accounts** is selected, users will be prompted to sign in to Windows as specified by the other options on the **Authentication** tab. For example, if both OpenID Connect authentication and Standard Authentication are enabled, users will be prompted to sign in twice. First, they will be prompted to sign in to the OpenID Connect identity provider. Then after successfully authenticating with the OpenID Connect identity provider, they will be prompted to enter the username and password of a Windows account.

5. Type the Client ID string from your OpenID Connect server configuration in the **Client ID** box.
6. Type the Client Secret string from your OpenID Connect server configuration in the **Client Secret** box.
7. Type the authorize URL used to authenticate users with your OpenID Connect server in the **Authorize URL** box.
8. Type the token URL used to authenticate users with your OpenID Connect server in the **Token URL** box.

9. In the **Redirect URL** box, type the URL that the identity provider must use to redirect users back to the GO-Global Host after they have successfully authenticated. This should be the same base URL that users use to access the GO-Global Host with *callback.html* appended to the end. For example, if you are using a separate web server like IIS and TLS is not enabled, the callback URL would be **http://hostname/goglobal/callback.html**.

   Alternatively, if you are using GO-Global's integrated web server and TLS is not enabled and GO-Global is configured to accept connections on its default port, 491, the callback URL would be **http://hostname:491/callback.html**.
10. Click **OK**.

Matching Active Directory Users to Identity Provider Accounts

GO-Global provides several options for deriving a user's UPN from claims in an OIDC ID token. User accounts must match in one of three ways on the Active Directory (AD) and identity provider.

There are three ways this can be achieved:

- The user's native User Principal Name (UPN) already *matches* the identity provider username. For example, the local AD domain is **example.com** and the identity provider domain is also **example.com**. By default, GO-Global searches for a valid UPN in the email, UPN, sub and userid fields of the ID token, in that order. Alternatively, administrators can specify the claim that contains the UPN via the **OpenIDConnectUserNameField** property in HostProperties.xml.
- Add a **UPN suffix** and use that for AD usernames so the AD UPN and identity provider's UPN's match. For example, the local AD domain is **company.local** but add a UPN suffix for users called **example.com**. The identity provider domain is also **example.com**.
- Set the user's AD mail attribute to match that of the identity provider's UPN and modify a setting in HostProperties.xml. In some deployments, there is no claim in the ID token that matches the user's AD UPN. For example, in a hosting environment where the customer's identity provider is used, the customer's domain (e.g., **customercompany.com**) will not match the AD domain of the hosting environment (e.g., **hostedapp.com**). As the customer's identity provider is used, administrators of the hosting environment, will not be able to add a claim to users' OIDC ID tokens that specifies the AD UPN.

  In situations such as this, administrators can configure GO-Global to look up the user's AD UPN via the user's email address. This is achieved by setting the value of the **OpenIDConnectUserLookupByEmail** property in HostProperties.xml to true on all applicable hosts. When this property is set to true, GO-Global searches the Active Directory for a user account with an email attribute that matches the OIDC ID token's email claim.

Storing User names in Alternate Fields

By default, GO-Global obtains the Windows user name from the User Principal Name or email address specified by the identity provider in the user's OpenID Connect ID token. If, however, the identity provider is configured to store the user's Windows user name in an alternate field, administrators can configure GO-Global to use the alternate field by entering the name of the field in the **OpenIDConnectUserNameField** property in the HostProperties.xml file.

To set the OpenIDConnectUserNameField property

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\HostProperties.xml in a text editor.
3. Find the **OpenIDConnectUserNameField** property and change the value to the name of the claim in the user's OpenID Connect token which contains the User Principal Name that GO-Global should use to authenticate the user on Windows.
4. Save the file.
5. Restart the **Application Publishing Service**.

When **Automatically sign users in to local Windows accounts** is enabled, local user account names are synthesized from the User Principal Name or email address obtained from the OpenID Connect authentication. Because local accounts cannot contain '@' or '.' these are replaced with '_' and '-' respectively. As an example, the email address **sales@graphon.com** would be synthesized to sales_graphon-com.

Windows has a 20-character limit on local account names. If the synthesized account name is longer than 20 characters, GO-Global truncates the name to 20 characters.

Passwords for these accounts are made up of characters randomly selected from the lower-case alphabet, the upper-case alphabet, numbers, and the **!@#$%&** special characters. The length of the password that GO-Global generates will equal the minimum length password specified for users on the computer unless the minimum length is less than 7. In that case, GO-Global will generate a password that is 14 characters longer than the minimum length requirement. For example, if the computer's minimum password length is 6, GO-Global will generate a password that is 20 characters long, in the following format: 8tw@m4b9Dek#vR76@t6%. If GO-Global is unable to obtain the computer's minimum password length, it will generate a password that is 14 characters in length.

If the minimum length requirement is set via Group Policy, enable Group Policy in the **Session Startup** tab the Host Options dialog. These passwords are not saved or reused. The password is changed with every OpenID Connect authentication.

Permissions for Windows applications hosted in GO-Global sessions are not managed by identity providers like Okta or ADFS. They are managed in Windows or Active Directory.

Integrating with Active Directory is a function of the identity provider. Active Directory Federated Services (ADFS) is automatically integrated with Active Directory. Other identity providers provide their own integrations. Organizations that are using an identity provider will have already configured this. Organizations that are just setting this up will need to consult their identity provider's documentation on how to set this up.

For more information about Okta, visit: https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-main.htm.

When using Azure, be sure to use the **OAuth 2.0 authorization endpoint (v1) and the OAuth 2.0 token endpoint (v1)** URLs. The v2 endpoint URLs will not work.

When using ADFS, select **Server application** when creating the OIDC application.

Using the Active Directory *mail* attribute of a Domain User Account

By default, GO-Global obtains the Windows user name from the User Principal Name (UPN) or the email address specified by the identity provider in the user's OpenID Connect ID token. If the user's Windows UPN user name is not identical to the email address, administrators can configure GO-Global to use the Active Directory *E-mail* field. In this situation, the OIDC email address would be used to search the Active Directory *E-mail* field.

To enable this option, change the value of the **OpenIDConnectUserLookupByEmail** property in the HostProperties.xml to true.

To use the Active Directory *mail* attribute of a domain user account

1. Stop the **Application Publishing Service**.
2. Locate the file HostProperties.xml in the C:\ProgramData\GraphOn\GO-Global directory.
3. Open HostProperties.xml in a text editor and locate the **OpenIDConnectUserLookupByEmail** property.
4. Set **OpenIDConnectUserLookupByEmail** to true.
5. Save the file.
6. Restart the **Application Publishing Service**.

Granting Launch and Activate COM Rights to Standard Users

By default, Windows does not grant standard users who have not signed in to Windows interactively by entering a user name and password the right to launch and activate COM objects. As a result, applications such as Windows File Explorer that rely on COM interfaces may only run or work properly for users who are members of the Administrators group when OpenID Connect Authentication is used.

Therefore, when OpenID Connect Authentication is enabled, grant standard users Launch and Activation COM rights as follows:

1. Run dcomcnfg.
2. Navigate to Component Services | Computers | My Computer.
3. Right-click **My Computer** and click **Properties**.
4. Select the **COM Security** tab.
5. Under Launch and Activation Permissions, click the **Edit Default...** button.
6. Click the **Add** button. (*Note*: The default permissions grant full rights to the INTERACTIVE and Administrators groups. This is why this works for all users authenticated via a username and password (INTERACTIVE users) and members of the Administrators group when OpenID Connect authentication is used.
7. Add the **Domain Users** group.
8. Click the **Allow** checkboxes next to **Local Launch** and **Local Activation**.
9. Click **OK**.
10. Click **OK**.

Kerberos Authentication Within Sessions Started Via OIDC Authentication

When users authenticate to a GO-Global Host using OpenID Connect authentication, administrators must perform additional steps to enable applications to use Kerberos authentication and automatically authenticate to backend services and databases, such as SQL Server, which is used as the example in the steps below.

Administrators must perform the following additional steps:

- Configure the backend service to use Kerberos authentication (not NTLM)
- Configure the service and Windows delegation so the GO-Global Host computer is allowed to access the service
- Enable GO-Global's Kerberos authentication extension for the application's process

These steps are described in the examples below, using SQL Server as the backend service:

A. To configure SQL Server to use Kerberos authentication, in the SQL Server Management Console Connect dialog, uncheck the **Trust server certificate** option.

B. To configure the SQL Server service and Windows delegation so the GO-Global Host computer is allowed to access the service, perform the following steps:

   1. Configure SQL server to run under a normal domain user (service) account (e.g., **domainname\sqluser**) under SQL Server Configuration Manager | SQL Server Services | SQL Server | Properties | Log on.

   2. Grant the service account user rights to "Write service principal name" (Active Directory Users and Computers | Computers | [SQL Service Computer] | Properties | Security | Advanced | **sqluser** | Edit | Write service principal name). ***Note:*** This change should enable the SQL Server Service to create the Service Principal Name (SPN) when it is restarted. If it doesn't, you can create the SPN manually.

3. If necessary, create SPNs manually:
   a. Sign in to the computer running SQL Server as an administrator.
   b. Run CMD.
   c. Create the two SPNs for the MSSQL service with the following commands:
      - setspn -S MSSQLSvc/**computername.domainname.com domainname\sqluser**
      - setspn -S MSSQLSvc/**computername.domainname.com**:1433 **domainname\sqluser**

4. Verify that the SPNs had been created by running the following command, which lists the SPNs under the account: setspn **domainname\sqluser** -L

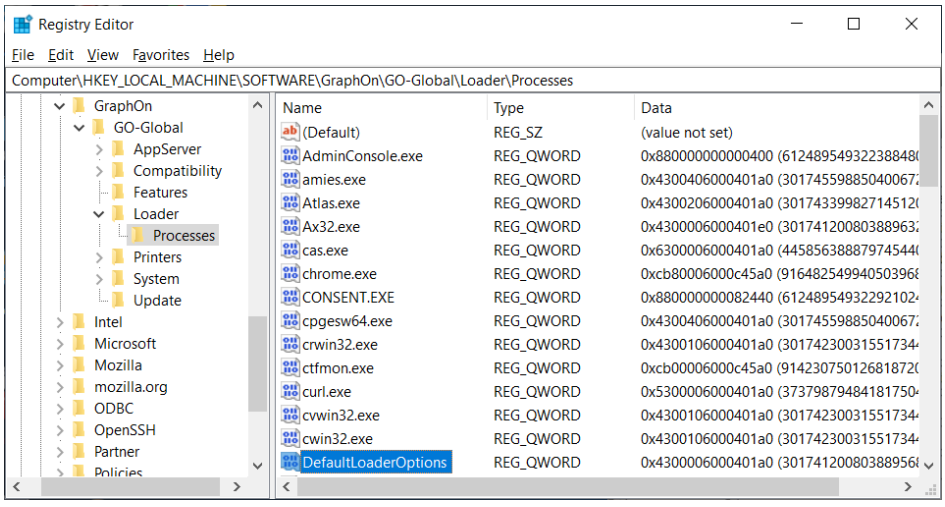
5. Configure delegation to allow the GO-Global Host to access these two SPNs under the **sqluser** account.

C. To enable GO-Global's Kerberos authentication extension for the application's process, add the following QWORD registry value:

   HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\Loader\Processes\smss.exe = [**DefaultLoaderOptions**] + 0x0100000000000000.

   DefaultLoaderOptions is the current value of HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\Loader\Processes\DefaultLoaderOptions registry value.

   For example,
   If DefaultLoaderOptions is 0x0**4**300006000401a0, set the value for ssms.exe to 0x0**5**300006000401a0



Important: The **DefaultLoaderOptions** value will likely change in the future. If the value of DefaultLoaderOptions on your computer is not 0x0**4**300006000401a0, do not set the value of the ssms.exe entry (or any other process) to 0x0**5**300006000401a0 to match the value in the example. Instead, calculate the value for the entry by adding 0x0100000000000000 to the value of the DefaultLoaderOptions as described above.

With this configuration, SQL Server Management Studio should be able to connect to the database. Once you have this working with SQL Server Management Studio, enable GO-Global's Kerberos authentication for the desired application. Create a QWORD named ***applicationprocessname.exe*** with a hex value of 0x05300006000401a0.

HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\Loader\Processes**applicationprocessname.exe** = 0x05300006000401a0.

For example, if your application's process name is MyLauncher.exe, create a **QWORD** registry value named MyLauncher.exe and set the hex value to 0x05300006000401a0.

CHAPTER IX

Security Options

9

Security Options

Through the **Security** tab of the **Host Options** dialog, administrators can select the transport mode of communication between clients and the GO-Global Host and select the level of encryption for data transmitted between client and host. Administrators can also modify the host port setting and enable Integrated Windows authentication and password caching.

Modifying the Host Port Setting

For users to access GO-Global through a firewall or router, administrators are able to modify the host port setting for the Application Publishing Service. The Application Publishing Service must be running on a dedicated port. Conflicts may arise if another service is running on the same port. The default port number for both TCP and TLS is 491.

To modify the Host Port setting

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Security** tab.
4. Type a new port number in the **Port** box.
5. Click **OK**.

The port can only be set to 443 if there is no web server on the computer configured to accept HTTPS connections. (Web servers accept HTTPS connections on port 443.)

After modifying the host port setting, you will need to append the **port** parameter. Use the port parameter followed by the new port number.
For example, **http://hostname/goglobal/?port=1667**

Users running GO-Global from a shortcut will need to append the **-hp** argument (followed by the new port number) to the shortcut. For example,
"C:\Program Files\GraphOn\AppController\AppController.exe" -h server1 -hp 1667

Users can also specify the port number in the **Connection** dialog when signing in to GO-Global. In the **Host Address** box, type the host name or IP address, followed by a colon and the port number. For example, server1:1667. If it's an IPv6 address, the IP address of the host must be in brackets.
For example, [fe80::29c:29ff:fe95:519a]:491

If the new port number is not specified by either of these methods, users will be unable to sign in to GO-Global.

After changing the host port, you must restart the **Print Spooler Service** and the **Application Publishing Service** for client printing to work on a port other than the default port 491.

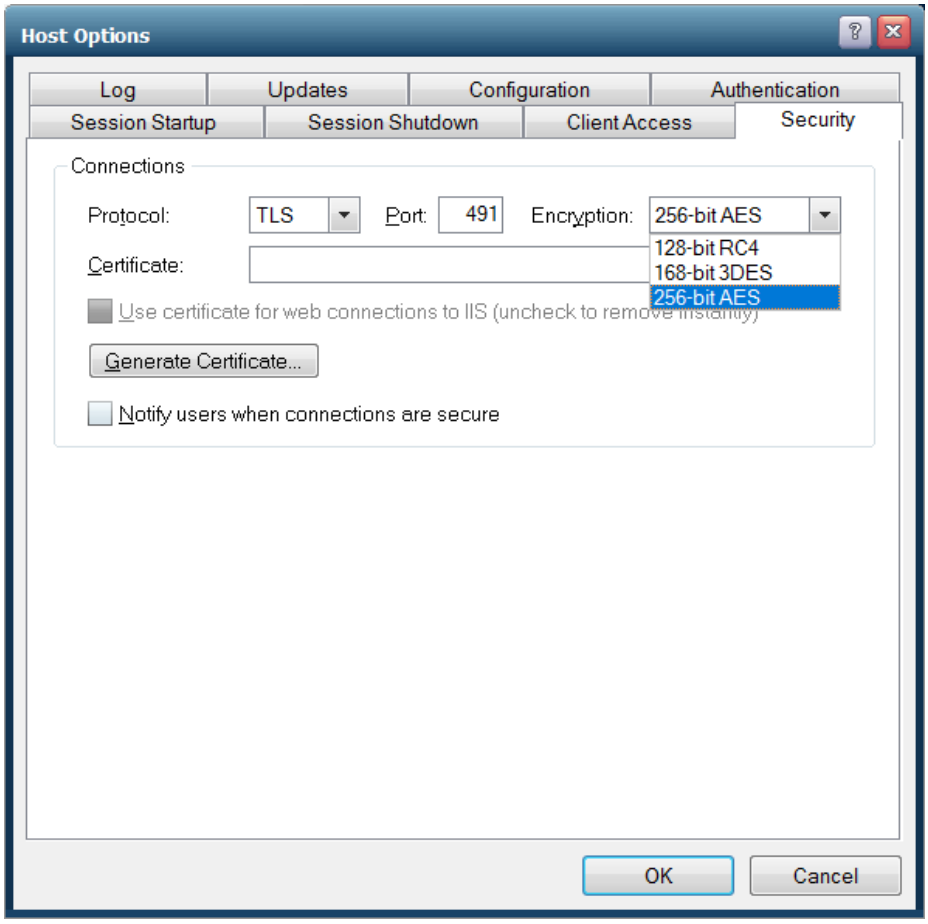
Encrypting Sessions

For purposes of security, administrators can optionally encrypt all data transmitted between the client and the host. This includes the client's user name and password, which are supplied during logon, and any application data submitted by the client or returned by the host.

When TCP transport mode is selected, GO-Global uses **56-bit DES** encryption. The DES key is exchanged using RSA Public-Key Cryptography Standards. The RSA keys are 512-bits. When TLS protocol mode is selected, the following encryption algorithms are also available: **128-bit RC4**, **168-bit 3DES,** and **256-bit AES**.

To encrypt a host's sessions

1. Click Tools | Host Options.
2. Click the **Security** tab.
3. From the **Encryption** list, select an encryption level.
4. Click **OK**.

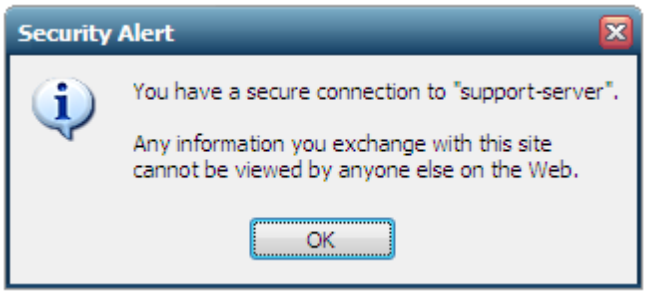


After encryption is enabled, all succeeding GO-Global sessions will be encrypted. Sessions that are active when the feature is enabled will remain unencrypted. The next time the user signs in to the GO-Global Host, however, his or her session will be encrypted. The user must sign off the GO-Global Host, and sign back in for the session to be encrypted.

When encryption is enabled, all connections to that GO-Global Host use the selected protocol and encryption algorithm, including connections from Admin Consoles, clients, and Dependent Hosts. When a Relay Load Balancer is used, GO-Global provides linked encryption. Specifically, the Application Publishing Service on the Relay Load Balancer decrypts the data it receives from the client and re-encrypts it before it forwards the data to the Dependent Host. Similarly, it decrypts the data it receives from the Dependent Host and re-encrypts it before it forwards it to the client.

Notifying Users of a Secure Connection

When the TLS protocol is selected, you can opt to notify users with a Security Alert when connections are secure.



To notify users when connections are secure

1. From the Admin Console, click Tools | Host Options.
2. Click the **Security** tab.
3. From the **Protocol** list, click **TLS**.
4. Type or browse to the path of the server's certificate file in the **Certificate** box.
5. Click the **Notify users when connections are secure** option.
6. Click **OK**.

Selecting TLS Protocol

GO-Global provides support for both Transmission Control Protocol (TCP) and Transport Layer Security (TLS) as methods for communication between Windows and GO-Global Hosts. GO-Global's support for TLS provides two primary benefits over its support for TCP: a) protection against man-in-the-middle (MITM) attacks, and b) stronger encryption. Therefore, TLS should be used whenever GO-Global is used to access sensitive information and the network communication is not secured via some other means (e.g., via a VPN).

TLS is the successor to the Secure Socket Layer (SSL) protocol. TLS is an improved version of SSL. When administrators select the TLS Protocol, the GO-Global Host uses OpenSSL's implementation of Transport Layer Security (TLS) to exchange encryption keys with the client. The GO-Global Host negotiates the key exchange using the highest version of TLS supported by the GO-Global Client or browser. The GO-Global Host does not include support for SSLv2, SSLv3, TLSv1.0, or TLSv1.1, so the key exchange will never be negotiated using these vulnerable protocols.

When selecting the TLS protocol, a TLS certificate file must be specified. Certificates are required to secure communication between GO-Global clients and hosts.

You can generate trusted certificates for GO-Global Hosts using the Strong Encryption Certificate Wizard. This allows administrators to enable strong encryption and TLS security without purchasing a certificate from a third-party Certificate Authority. For more information, see the section below, Strong Encryption Certificate Wizard.

You can obtain a certificate from a trusted Certificate Authority (CA) such as Verisign or Thawte, or you can create your own certificate authority and then sign your server certificates from this authority. Wildcard TLS certificates are also supported. For more information, see Obtaining a Trusted Server Certificate.

To select TLS Protocol

1. From the Admin Console, click Tools | Host Options.
2. Click the **Security** tab.
3. From the **Protocol** list, click **TLS**.
4. Type or browse to the path to the server's certificate (e.g., server.crt) file in the **Certificate** box.
5. Click **OK**.

When **TLS protocol** is selected and a separate web server is used (i.e., GO-Global's integrated web server is not used), HTTPS must be enabled on the web server if users will be accessing the GO-Global Host via a web browser.

When a Relay Load Balancer is used:

- The certificate must be installed on the Relay Load Balancer but does not need to be installed on the Dependent Hosts.
- On the Dependent Hosts, the value in the **Relay Load Balancer address** field on the **Configuration** tab of the **Host Options** dialog must match the certificate's Common Name or one of the Subject Alternative Names.

When a Farm Manager is used:

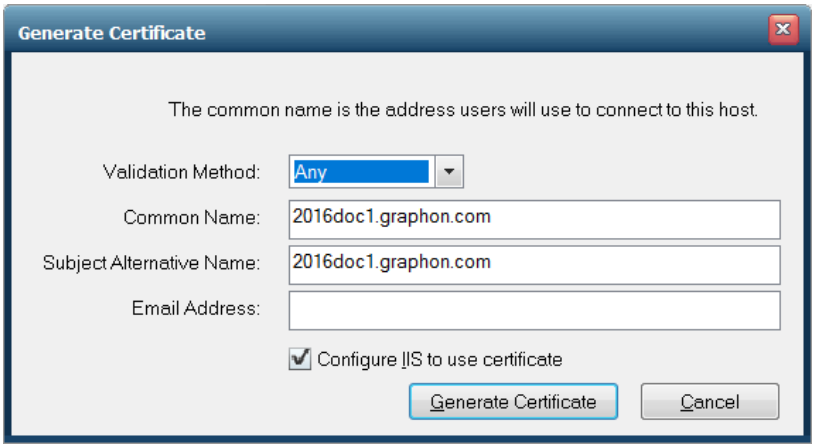
- The certificate must be installed on the Farm Manager and on each Farm Host.
- On the Farm Hosts, the value in the **Farm Manager address** field, must match the certificate's Common Name or one of the Subject Alternative Names.

Strong Encryption Certificate Wizard

Using the **Strong Encryption Certificate Wizard**, administrators can generate trusted TLS certificates for GO-Global Hosts. This allows administrators to enable strong encryption and TLS security without purchasing a certificate from a third-party Certificate Authority.

To generate a TLS certificate

1. Click Tools | Host Options.
2. Click the Security tab.
3. Select **TLS** from the Protocol menu.
4. Click the **Generate Certificate** button.
5. Select the **Validation Method** that will be used to verify that the addresses specified in the **Common Name** and **Subject Alternative Name** fields resolve to the computer. Select **DNS** validation for wildcard certificates and for computers not accessible from the internet. Otherwise, select **HTTP** validation.



6. Edit the **Common Name**, if desired. This is the exact address (Fully Qualified Doman Name) of the host that users will connect to when using GO-Global.
7. Edit the **Subject Alternative Name**, if desired. This is the alternate address of the host users will connect to when using GO-Global.
8. Provide an **Email Address** to which certificate renewal notifications will be sent.
9. The certificate that is generated will automatically be configured for use in the Integrated Web Server. To configure Internet Information Server (IIS) to use the certificate, enable the **Configure IIS to use Certificate option**.
10. Click **Generate Certificate** to generate and install a trusted TLS certificate on the host.
11. If the DNS method was selected, create the DNS TXT records for Domain, Name, and Value, as provided in the **Validation Tokens** dialog. The values can be selected and copied. Then click **Validate**.

The Strong Encryption Certificate Wizard populates the **Common Name** field with the host computer's **Fully Qualified Domain Name** (FQDN). The Common Name *must be* set to the exact value (address) that users will use to connect to the GO-Global Host. In order to pass the validation challenge, the name(s) used in the HTTP-01 or DNS-01 challenge *must be* resolvable via public DNS. For this reason, certificates for .local or other internal or non-public domains cannot be generated using the Strong Encryption Certificate Wizard.

After successfully generating a certificate, the GO-Global host will install the certificate and its key in the following locations:

Certificate/Key Directory	Description
C:\ProgramData\GraphOn\GO-Global\ks\certs	The location where the certificates/keys are copied to after successful generation by either win-acme or Posh-ACME. These are left untouched and kept in their original naming conventions.
C:\ProgramData\GraphOn\GO-Global\ks	The location where the certificates/keys get copied to and renamed, so that GO-Global can utilize them. (gg_cert.key and gg_cert.pem)
C:\Windows\System32\config\systemprofile\AppData\Local\Posh-ACME	The location where Posh-ACME keeps cached certificates/keys, and other metadata regarding previous requests (e.g., order data and account data.)
C:\ProgramData\GraphOn\GO-Global\ks\win-acme-cache	This is where we have configured win-acme to keep cached certificates/keys.

Obtaining a Trusted Server Certificate

As an alternative to using the Strong Encryption Certificate Wizard, customers can use server certificates from other Certificate Authorities. To obtain a server certificate from a CA that is trusted by the client operating system, consult the documentation from the CA of your choice using the following information as a guide. The CA will require a Certificate Signing Request (CSR). A CSR is a Base64 encoded ASCII file, that includes identification details and your public key that will be used to *digitally sign* your certificate.

To generate a CSR on Windows

1. Review the list of third-party OpenSSL tools for Windows at https://wiki.openssl.org/index.php/Binaries. A popular choice is the **slproweb** from Shining Light Production, and the installer commonly used is the latest (non-light) version.
2. After installing openssl, navigate to its directory with **command prompt (cmd.exe).**
   For example, cd C:\Program Files\OpenSSL-Win64\bin\
3. Type the following command to generate a private key:
   ```
   openssl.exe genrsa -out server.key 2048
   ```
4. Type the following command to create a CSR:
   ```
   openssl.exe req -sha256 -new -key server.key -out server.csr
   ```

Running this command will prompt you for the attributes to be included in your certificate, as follows:

- **Country Name**: US
- **State**: your state
- **Locality**: your city
- **Organization**: your company name
- **Organizational Unit**: your department
- **Common Name**: your server's name
- **E-mail Address**: your email address

Unless you are using a wildcard TLS certificate, either the Common Name or a Subject Alternative Name (SAN) must match the host name of the GO-Global Host (i.e., the name that users will specify when connecting to the host). Any variation in the name will cause the client to issue a warning when connecting. The output of the above command will be a file named **server.csr**, which can be sent to your CA.

Since GO-Global's TLS implementation is based on the OpenSSL toolkit, the tools are the same as those used in other OpenSSL-based products, such as the Apache mod_ssl package. Follow instructions provided by your CA for the mod_ssl package to obtain a certificate for your server.

When your CA sends you the signed server certificate file, rename it to server.crt or server.pem. Copy this file and the **server.key** file (generated in step 4 above) to the C:\ProgramData\GraphOn\GO-Global\ks directory on the Relay Load Balancers, if they are used. Otherwise, if a Relay Load Balancer is not used, copy the file to the C:\ProgramData\GraphOn\GO-Global\ks directory on all Application Hosts and Application Host Managers. By default, this directory is only accessible by Administrators or the System account. Finally, select the signed certificate file in the Admin Console, as described below.

To select the server certificate

1. From the Admin Console, click Tools | Host Options.
2. Click the **Security** tab.
3. In the **Protocol** list, select **TLS**.
4. Type or browse to the path (C:\ProgramData\GraphOn\GO-Global\ks) of the certificate (e.g., server.crt) file in the **Certificate** box.
5. Click **OK**.

GO-Global requires that the certificate and its associated key be in PEM format (Base64 encoded ASCII) with a file extension of crt or pem. When requesting a certificate from a third-party CA, GraphOn recommends requesting it in PEM format. If your provider can't supply the correct format, there are many online guides available to assist you in converting specific certificate formats to Base64 encoded ASCII PEM using openssl.

For more information about converting certificates, visit https://knowledge.digicert.com/solution/SO26449.html

Using an Intermediary TLS Certificate with GO-Global

When using an intermediary TLS certificate with GO-Global, you must concatenate your existing certificate with the intermediary certificate. The following example uses the Go Daddy intermediary certificate.

The root certificate is required when using an intermediary TLS certificate with GO-Global's mobile apps.

1. Take the .crt and .key files that are being used on the GO-Global Host.
2. Download the intermediary certificate (e.g., GODaddyCA.crt). This should have come with the original certificate purchase.
3. Concatenate your .crt and the intermediary .crt file as follows:
   test_server.crt+GODaddyCA.crt server.crt
4. Rename the key file from step 1 to **server.key** so that it matches the newly created **server.crt** file.

5. Copy these two files onto the GO-Global Host in a secure location. We recommend using the C:\ProgramData\GraphOn\GO-Global\ks directory.
6. Launch the Admin Console. Click Tools | Host Options. Click the **Security** tab.
7. Change the **Protocol** to **TLS** and set the encryption level, if needed.
8. Browse to the TLS certificate server.crt in c:\data and click **OK.** You should not see an error message at this point if you have .crt and .key files with the same prefix.
9. Enable **Notify users when connections are secure** for testing purposes.
10. Click **OK**.
11. Start a GO-Global session from a different system.

Sometimes there will be more than one intermediary certificate that will also need to be concatenated.

For information about concatenating certificates, visit https://www.sectigo.com/knowledge-base/detail/How-to-Merge-or-Concatenate-your-SSL-Certificates-and-Private-Key-in-a-single-file/kA03l00000117PB

Using an Intermediary TLS Certificate on iOS and Android

For AppController on iOS and/or Android to trust a server certificate, it must be able to trust the entire certificate chain, including any intermediate certificates and all root certificates.

To make a server certificate that will provide the entire certificate chain

1. Obtain the certificate files for the intermediate and root certificates in the certificate chain of the server certificate being used on the GO-Global Host.
2. Concatenate all the certificate files into a single file as follows: test_server.crt+intermediate.crt+root.crt server.crt.

There may be 0 or more intermediate files and 1 or more root files. If your .crt file is self-signed, you will just need to rename your .crt file to server.crt.

3. Rename the key file from step 1 to **server.key** so that it matches the newly created **server.crt** file.
4. Copy these two files onto the GO-Global Host in a secure location. We recommend using the C:\ProgramData\GraphOn\GO-Global\ks\certs directory.
5. Launch the Admin Console. Click Tools | Host Options. Click the **Security** tab.
6. Change the protocol to **TLS** and increase the encryption level to 256-bit AES, if you have a high-encryption license. If not, leave it at 56-bit.

7. Browse to the certificate **server.crt** in c:\data and click **OK**. You should not see an error message at this point if you have .crt and .key files with the same prefix.
8. Enable **Notify users when connections are secure** for testing purposes.
9. Click **OK**.
10. Start a GO-Global session from an iOS or Android device.

Resolving TLS Issues

When a Relay Load Balancer is configured to use TLS, the name entered into the **Relay Load Balancer** field on the *Dependent Hosts* must match the Common Name or one of the Subject Alternative Names of the Relay Load Balancer's certificate. (The name entered into the **Relay Load Balancer** field on the *Relay Load Balancer* does *not* need to match the **Common Name** of the Relay Load Balancer's certificate.)

To verify that the Relay Load Balancer and Dependent Host are properly configured

1. Run the Admin Console and verify that the Dependent Host appears below the Relay Load Balancer in the tree view. If it does not, the Dependent Host is not connected to the Relay Load Balancer.
2. If the Dependent Host does not appear below the Relay Load Balancer in the tree view, check the **Application Publishing Service** log on the Dependent Host. If it contains a message that the certificate is invalid, there is a TLS configuration problem.
3. If there is a TLS certificate error message in the Dependent Host's Application Publishing Service log, browse to the GO-Global\Programs directory on the Dependent Host and double-click **AppController.exe** to run the GO-Global client.
4. Type the address of the Relay Load Balancer into the **Connection** dialog. Type the address exactly as it is specified in the **Relay Load Balancer** field of the **Host Options** dialog on the Dependent Host.
5. Click **Connect**.

If a TLS warning message is displayed, the Dependent Host will not be able to connect to the Relay Load Balancer. Resolve the issue described in the TLS warning message. Then the Dependent Host should be able to connect to the Relay Load Balancer.

If no TLS warning dialog is displayed, but a different error message is displayed (e.g., No available hosts), the TLS configuration is fine. For the purposes of this test, you can disregard any error messages that do not pertain to the ability of the client to open a connection to the Relay Load Balancer.

Session Reconnect

Session reconnect allows sessions to be maintained on a GO-Global Host without a client connection. If the client's connection to the host is lost, intentionally or unintentionally, the user's session and applications remain running on the GO-Global Host for the length of the session timeout specified in the Admin Console. Session reconnect allows users to return to their GO-Global session in the exact state they left it. Through the Program Window users can select to disconnect, rather than exit from GO-Global, and can return to their session as they left it — without having to shut down their open applications and running processes.

If the network connection is lost or if users unintentionally disconnect from GO-Global, their session state is preserved for the length of time specified in the Admin Console. After a user is authenticated through normal logon procedures, GO-Global determines if the user has an active session. If so, that session resumes and appears exactly as it did prior to disconnection. If not, a new session is started. Users are also able to disconnect from one client and reconnect to the session from another client.

When attempting to reconnect to a disconnected session, users are required to specify their logon credentials. After the host validates them, the host reconnects them to the disconnected session. If the session is hosted on a server that is part of a load-balanced configuration, the user is routed to his or her session without any indication that the session is on a load-balanced server. If Integrated Windows authentication is available, users are automatically re-authenticated and re-connected to their session.

CHAPTER X

Branding

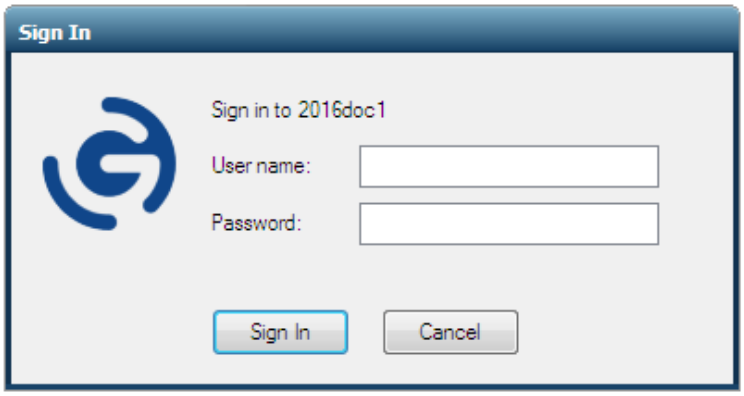
10

Branding

Branding allows administrators to edit and customize the text, labels, and images that end users see on the Sign In dialog, the Program Window, the Two-Factor Authentication dialogs, and the web interface for AppController.

Branding the Sign In Dialog

On the **Sign In** dialog, the dialog's title bar, field labels, buttons, text, and image can all be branded or localized.



To brand the Sign in dialog

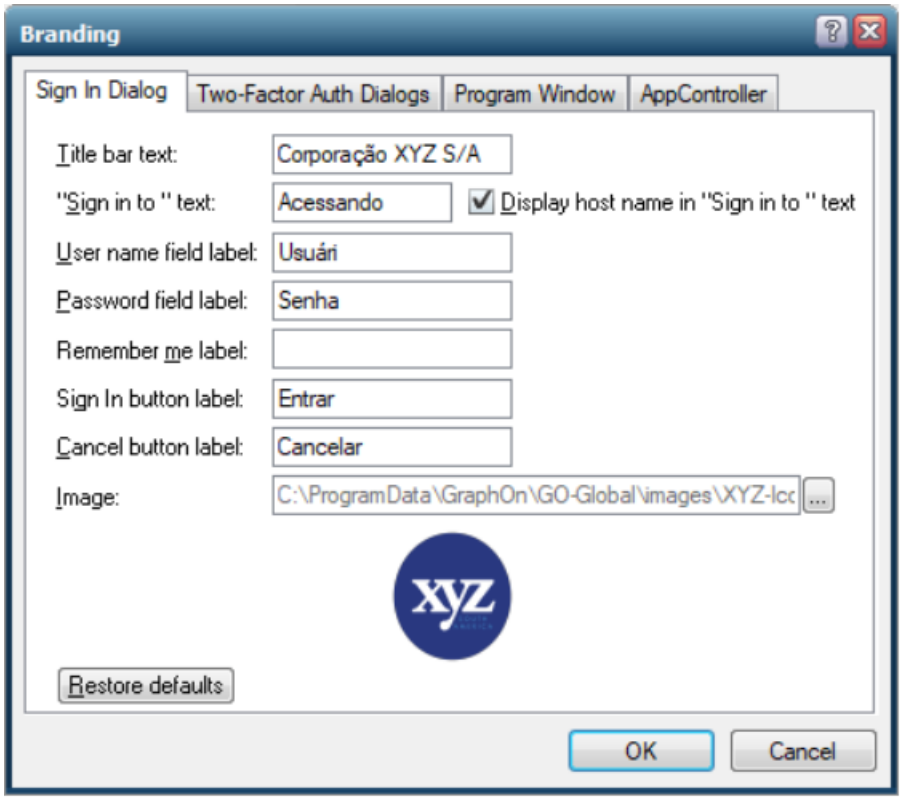
1. From the Admin Console, click Tools | Branding.
2. Click the **Sign In Dialog** tab.
3. Edit any of the following:
    - The text on the **Title bar**.
    - The "Sign in to " text.
    - The label of the **User name** field.
    - The label of the **Password** field.

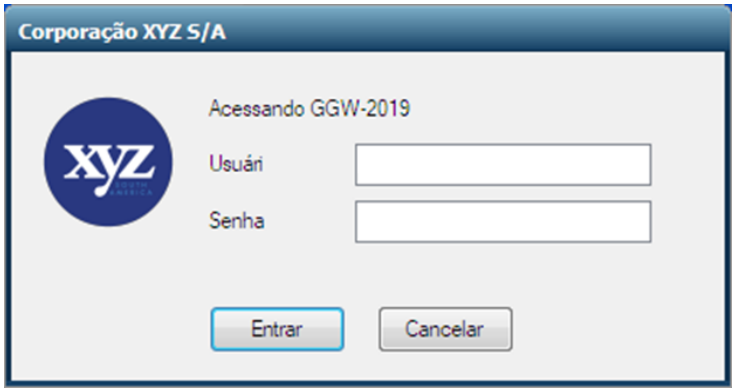
- The label of the **Remember me on this computer** option. (This field will only be displayed on the Branding dialog if **Cache passwords on the client** is enabled on the host.)
- The label on the **Sign In** button.
- The label on the **Cancel** button.

4. To browse for a new image, click the **Image** browse button. The following formats are supported: .jpg, .jpeg, .bmp, .ico, .png, .gif, and .tif. The replacement image is resized to 40x40 pixels.
5. Click the **Display host name in "Sign in to" text** to hide the name of the host that users sign in to. The host name is displayed on the Sign In dialog by default.
6. Click **OK**.

To revert to the original text and image, click the **Restore defaults** button.

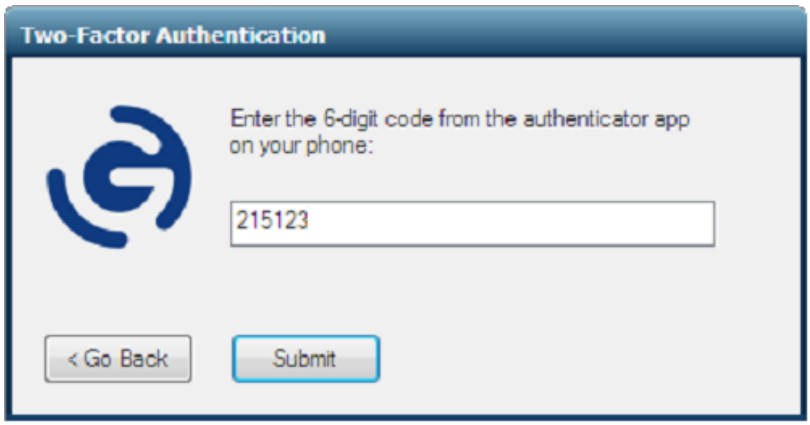
In the example below, the **Title bar** text**, "Sign in to"** text, **User name** and **Password** labels, **Sign In** and **Cancel** buttons, and the image have all been branded and localized.

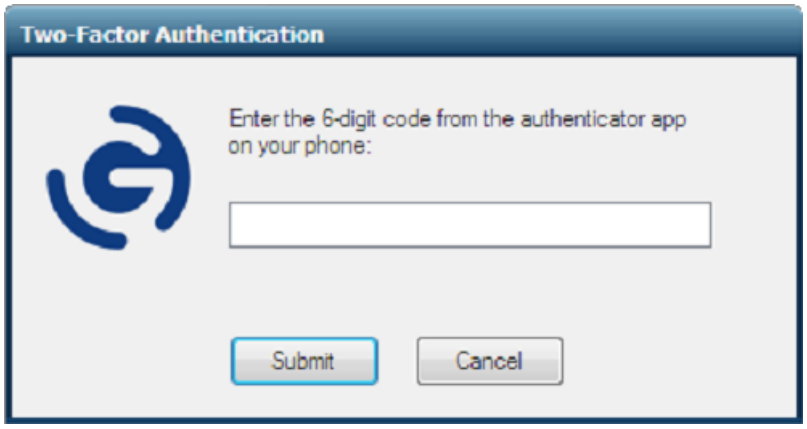


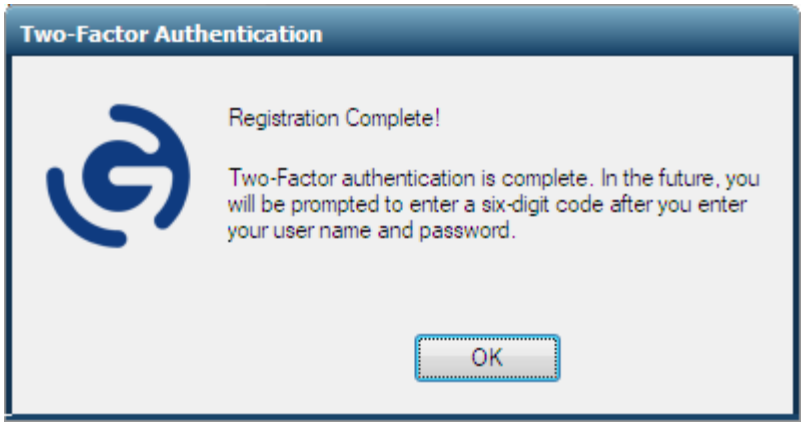


Branding the Two-Factor Authentication Dialogs

The title bars, text, and images on the following four Two-Factor Authentication dialogs can be branded and localized.

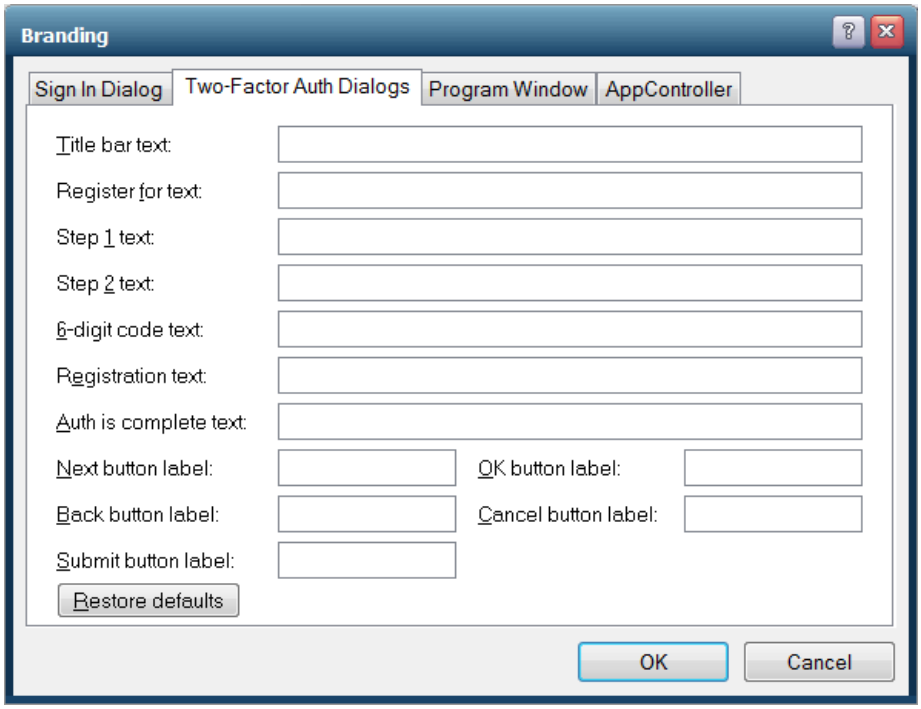

Two-Factor Authentication
Enter the 6-digit code from the authenticator app on your phone:
215123
< Go Back
Submit


Two-Factor Authentication
Enter the 6-digit code from the authenticator app on your phone:
Submit
Cancel


Two-Factor Authentication
Registration Complete!
Two-Factor authentication is complete. In the future, you will be prompted to enter a six-digit code after you enter your user name and password.
OK

To brand the two-factor authentication dialogs

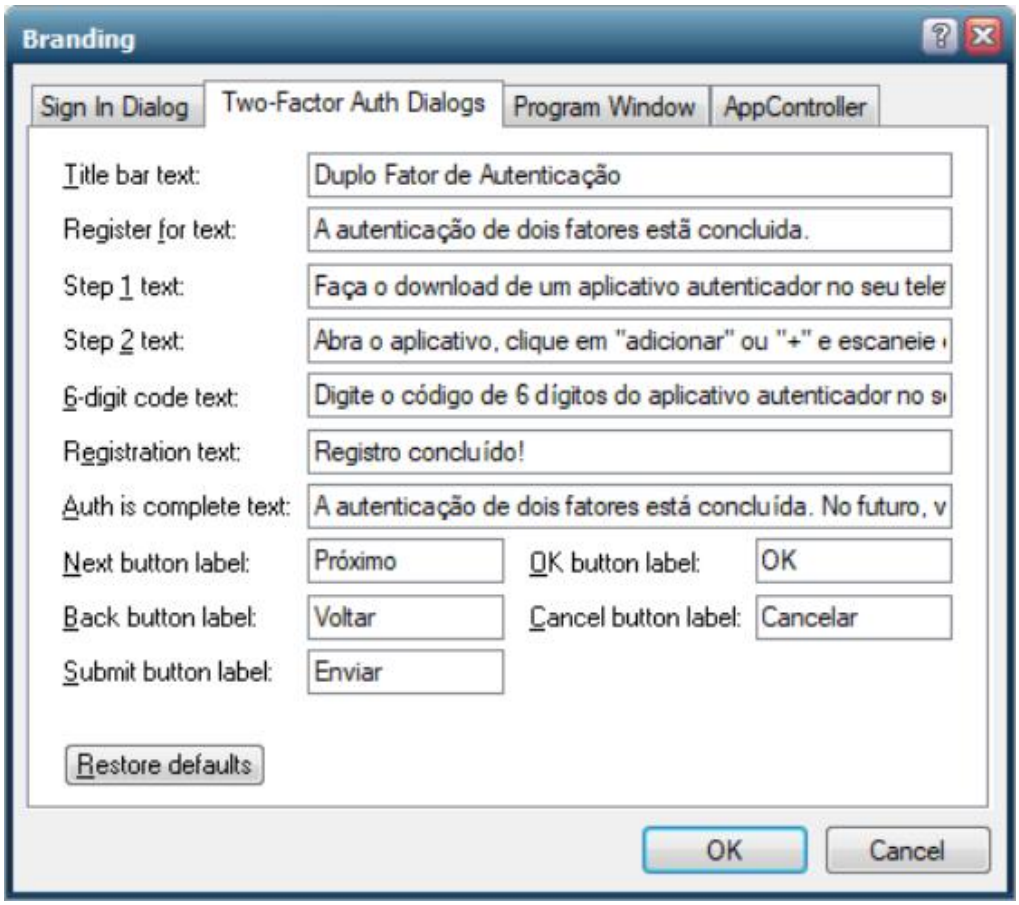
1. From the Admin Console, click Tools | Branding.
2. Click the **Two-Factor Auth Dialogs** tab.

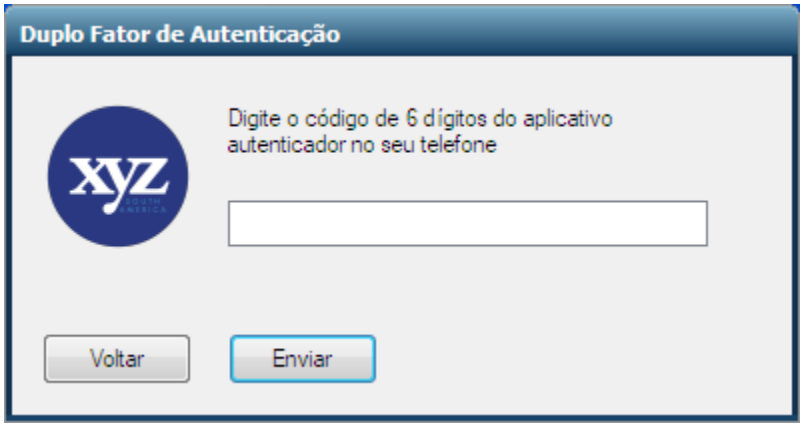


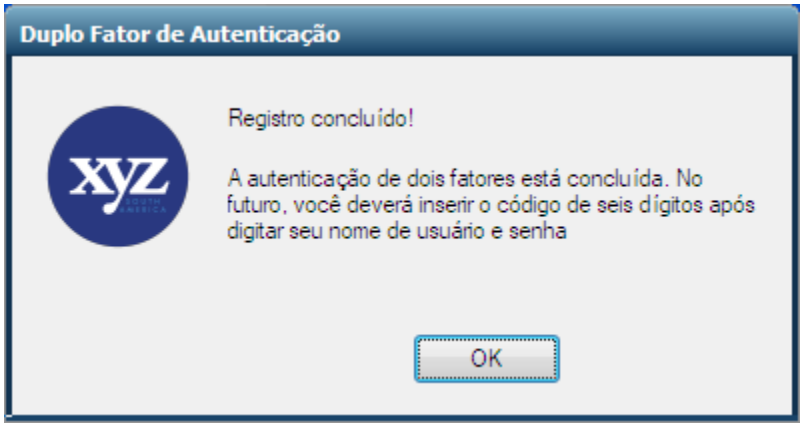
3. Edit any of the following:
    - The text on the **Title bar**.
    - The Register for text.
    - The **Step 1** text.
    - The **Step 2** text.
    - The **6-digit code** text.
    - The **Registration** text.
    - The **Auth is complete** text.
    - The **Next** button label.
    - The **OK** button label.
    - The **Back** button label.
    - The **Cancel** button label.
    - The **Submit** button label.
    - The label on the **Cancel** button.
4. Click **OK**.

To revert to the original text and image, click the **Restore defaults** button.

In the following examples, the two-factor authentication dialogs have been branded and localized.





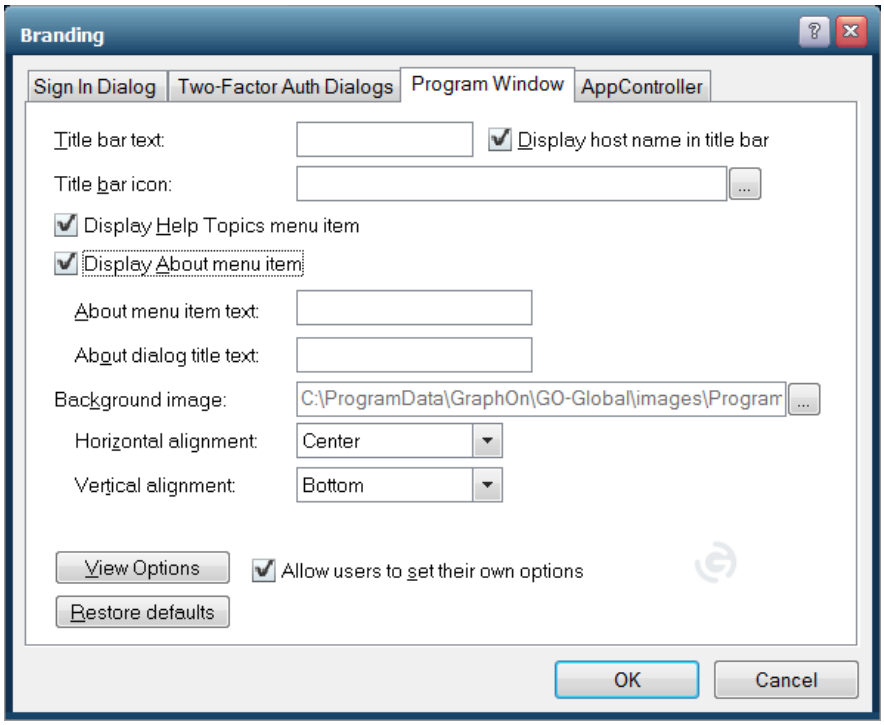


Branding the Program Window

The Program Window is the application that contains the user interface for launching applications via GO-Global. The Program Window displays a list of Windows applications that the user is authorized to run.

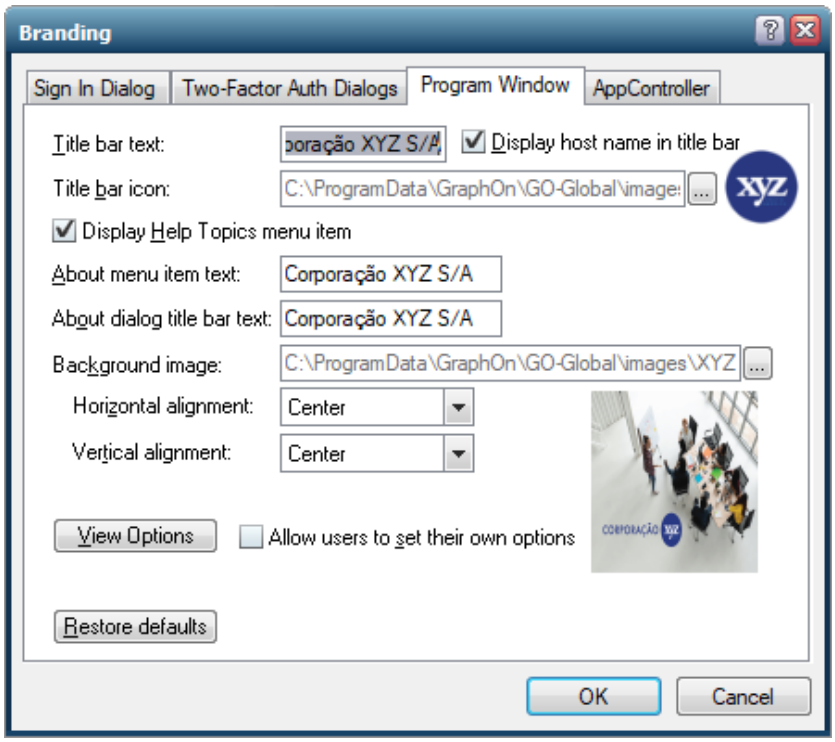
To brand the Program Window

1. From the Admin Console, click Tools | Branding.
2. Click the **Program Window** tab.
3. Edit any of the following:
   - The text on the Program Window's **title bar**.
   - The text on the Program Window's **Help | About** menu option.
   - The text on the Program Window **About dialog** title bar.



4. Click **Display host name in title bar** to hide the name of the host that users sign in to. The host name is displayed on the Program Window's title bar by default.
5. To browse for a new title bar icon, click the **Title bar icon** browse button. This must be an .ico file.
6. Click **Display Help Topics menu item** to remove the Help Topics from the menu. Help Topics are displayed by default.
7. Click **Display About menu item** to remove the About dialog from the menu and the About button from the toolbar.
8. To browse for a new background image, click the **Background image** browse button. The following formats are supported: .jpg, .jpeg, .bmp, .ico, .png, .gif, and .tif. The background image can be positioned left, center, right using the **Horizontal alignment** dropdown menu. The image can also be positioned top, center, bottom using the **Vertical alignment** dropdown menu.
9. Click **OK**.

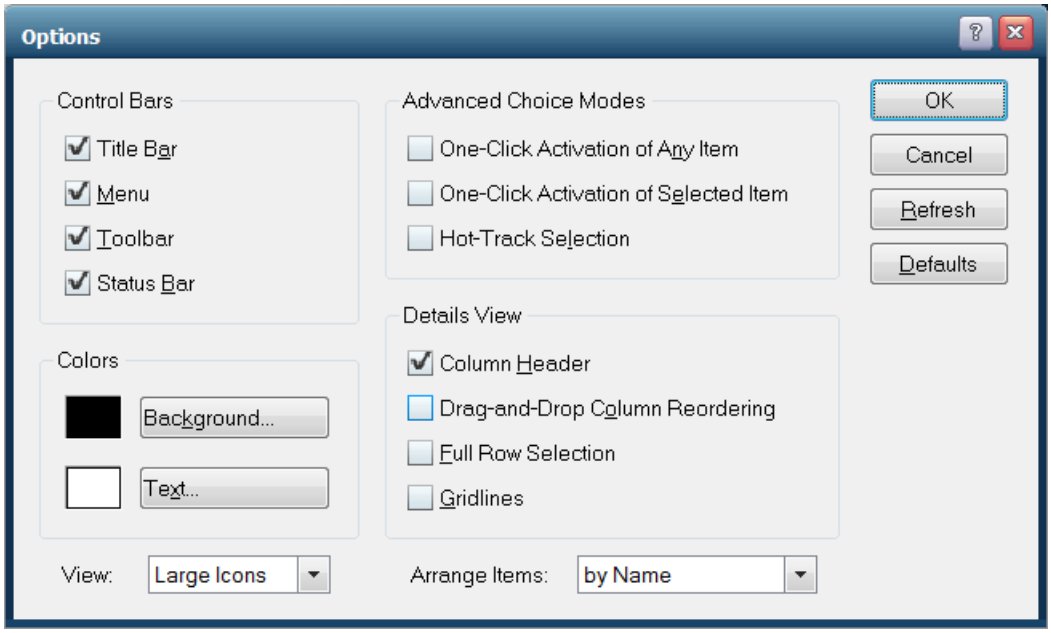
In the example below, the Program Window has a branded title bar text, title bar icon, and background image.



By default, users are allowed to set their own View options in the Program Window. To prevent users from setting their own View options, uncheck **Allow users to set their options**.

You can view and customize the default display of the Program Window by clicking the **View Options** button on the Program Windows tab. You can turn the title bar, menu, toolbar, and status bar on or off, as well as select any of these options:

- **One-Click Activation of Any Item:** Opens an item with one mouse click
- **One-Click Activation of Selected Item:** Opens a selected item with one mouse click
- **Hot-Track Selection:** Automatically selects an item when the cursor is placed over the item



The following options can be displayed when viewing items in Details view:

- **Column Header:** Displays the column header
- **Drag-and-Drop Column Reordering**: Enables drag-and-drop reordering of columns
- **Full Row Selection**: Highlights an item's full row when an item is selected
- **Gridlines:** Displays gridlines around items and subitems

To select the default color for the Program Window's background and text, click the **Background** or **Text** button to access the dialog box containing a palette of colors from which to choose.

You can also select the default **View** in the Program Window to display items as large icons, small icons, as a list with small icons, or as a detailed list.

The **Arrange Items** option allows you to select the default sorting order of items in the Program Window. Sorts items by the following:

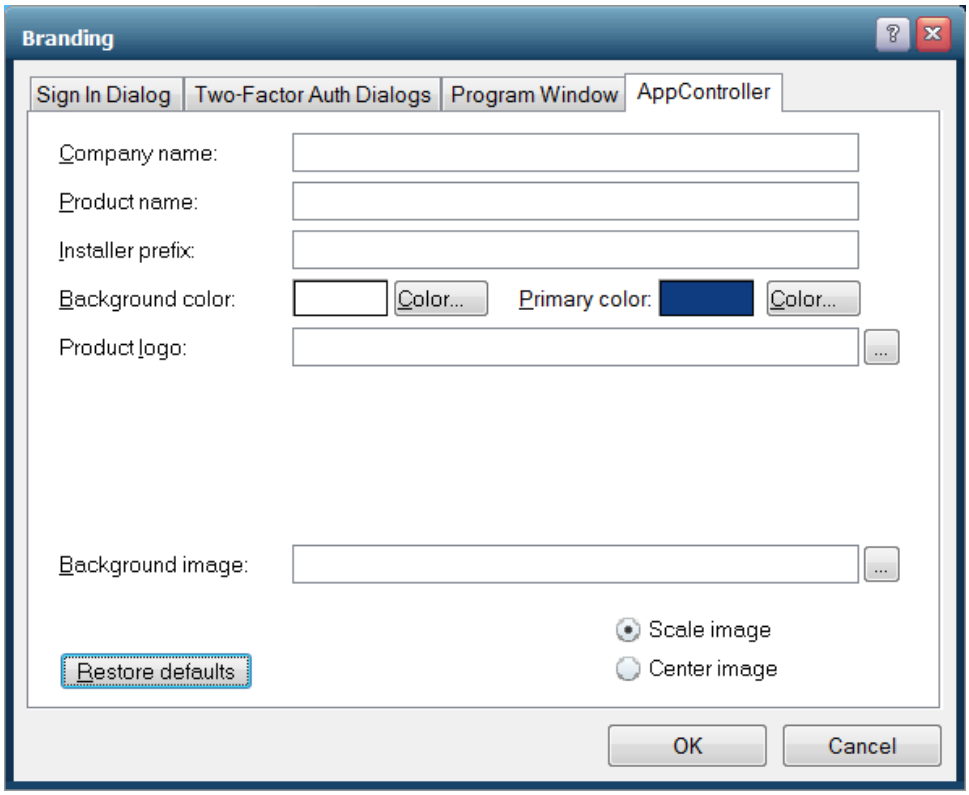
- **By Name:** Sorts items alphabetically by name.
- **By Location:** Sorts items by location.
- **By Type:** Sorts items by type.
- **By Size:** Sorts items by size, from smallest to largest.
- **By Date Accessed:** Sorts items by date of last access, from oldest to most recent.
- **By Date Created:** Sorts items by date of creation, from oldest to most recent.
- **By Date Modified:** Sorts items by date of last modification, from oldest to most recent.

When you are finished, click the **Ok** button to close the Options dialog, and for the selections to take effect. The **Cancel** button will close the dialog without saving any changes. The **Refresh** button reverts to your most recently saved settings, and the **Defaults** button reverts to the settings saved in your registry.

Changes to the **View Options** dialog of the Program Window only apply to users who have not yet signed into GO-Global. These changes will not apply to users who have already signed in and have an existing GO-Global user profile. When running the Program Window, users can access the Options dialog by clicking View | Options to customize the display of the Program Window. However, if **Allow users to set their options** is disabled, the Program Window's View for all users will be those specified in the Admin Console. When users run the Program Window, the **View** option is not displayed on the menu bar, nor is the **View** option displayed in the right-click context menu.

Branding the AppController Web Interface

AppController is the unbranded, customizable application that that can be started from a computer's desktop, a mobile device, or a web browser. The AppController web interface can be localized and branded with a customer's name and logo.



To brand the AppController Web Interface

1. From the Admin Console, click Tools | Branding.
2. Click the **AppController** tab.
3. Brand any of the following:
   - Company name
   - Product name
   - Installer prefix (By default, the installer is named *GO-Global.AppController.exe*. The Installer prefix will replace *GO-Global*.)
4. Select a **Background color** for when AppController is run inside the browser window by clicking the **Colors** button. Select a color from the color picker dialog and click **OK**.
5. Select a **Primary color** by clicking the **Colors** button. Select a color picker and click **OK**. This color will appear on the title bars and buttons in the dialog boxes.
6. To browse for a new **Product logo**, click the **Browse** button. The following formats are supported: .jpg, .jpeg, and .png.

7. To select a **Background image** for the AppController installation web pages, click the browse button. The following formats are supported: .jpg, .jpeg, and .png. To resize the image to fit the browser window, click **Scale image**. Click **Center image** to retain the image's resolution and display it in the center of the browser window.
8. Click **OK**.

To revert to the original text and images, click the **Restore defaults** button.

Following are examples of an AppController web interface that has been branded and localized. The product logo and background image have been branded, and the company name, product name, and installer prefix have been changed.

Branding options are stored in the C:\ProgramData\GraphOn\GO-Global\HostProperties.xml file under the group="Branding." Images are stored in C:\ProgramData\GraphOn\GO-Global\images. When a Relay Load Balancer or Farm Manager is used, settings changes are automatically made on all hosts in the cluster. When a Relay Load Balancer or Farm Manager is not used, branding options can be manually copied from one computer to another. For more information, see Manually Copying Configuration Settings from One Host to Another.

CHAPTER XI

Printing

11

Printing

GO-Global supports client-side printing on all client platforms. By default, GO-Global automatically detects the client's default printer information once the user has signed in to the GO-Global Host. This includes the default printer's port and printer driver. GO-Global will use the Universal Printer Driver if it is enabled.

When running applications on GO-Global Hosts, users can print to network printers and to printers that are directly connected to their computers (e.g., via serial, parallel and USB ports).

Administrators can control which, if any, printers are made available to users using the **-ac** and **printerconfig** GO-Global startup parameters.
When running GO-Global from a shortcut, use the -ac parameter with "all", "none" or "default" to respectively make all, none or only the default printer available from applications running on the GO-Global Host. For example, to make all printers available, create a shortcut with the target specified as follows:
"C:\Program Files\GraphOn\AppController\AppController.exe" -ac all

Similarly, when running GO-Global from the logon page, use the **printerconfig** parameter with "all", "none" or "default". For example, the following parameter will make all printers available: **http://hostname/logon.html?printerconfig=all**

If no options are specified, GO-Global automatically configures the user's default printer only.

The **Print Spooler Service** must be running on the GO-Global Host in order to configure client printers.

Designating Access to Printer Drivers

GO-Global can obtain printer drivers from the following sources:

- **Universal Printer Driver**: GO-Global includes a **Universal Printer Driver** that can print to any client printer. Enable this option to allow the use of the Universal Printer Driver for configuring client printers.
- **Windows Printer Drivers:** Enable the **Windows Printer Drivers** option to allow printers to be configured using already installed native drivers.

When only the **Universal Printer Driver** is enabled, only the Universal Printer Driver will be used as a printer driver. No native drivers will be used. This is the default setting.

When **Windows Printer Drivers** is enabled, native printer drivers that are installed on the host will be used. If a printer's native driver is not installed, or if a printer's native driver is a Type 4 printer driver (which GO-Global does not support), that printer will be configured to use the Universal Printer Driver if the **Universal Printer Driver option** is checked. Otherwise, if the Universal Printer Driver option is not checked, the printer will not be available to users.

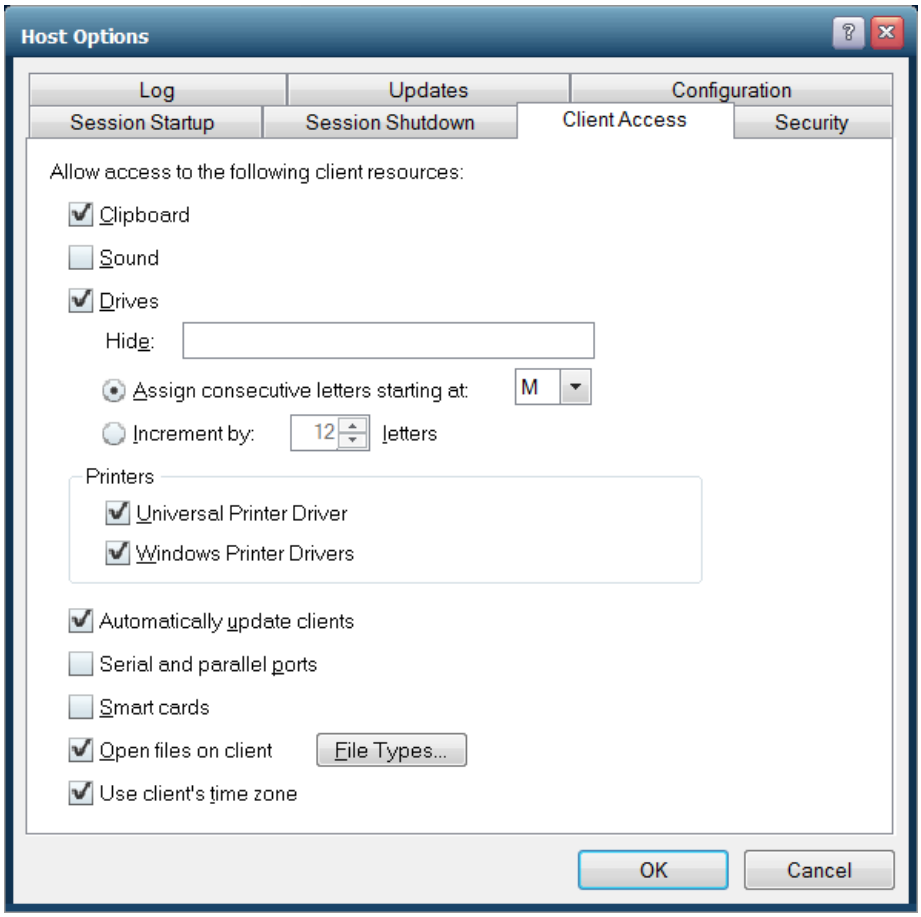
When neither the **Universal Printer Driver** or **Windows Printer Drivers** is enabled, no printers will be configured and client printing is disabled.

The Universal Printer Driver is supported on Windows, Linux, and macOS. When printing with the Universal Printer Driver, the user (or group) needs to have full access to the temp directory.

A printer named **Preview PDF** is configured in each session when the Universal Printer Driver is enabled. Documents printed to this printer are automatically converted to a .pdf file and displayed on the client computer. Users can save, print, or email the document at their discretion. A PDF reader, such as Adobe Reader, is required on the client computer in order to use the Universal Printer Driver's PDF conversion feature.

The Universal Printer Driver allows users to change all printer settings on Windows clients. On non-Windows clients, it only allows users to change standard settings like page orientation and paper size. When users on Linux and macOS clients require access to a printer's advanced settings, administrators should enable the Windows Printer Drivers option and install the required printer drivers on the GO-Global hosts.

Administrators set access to printer driver sources through the **Host Options** dialog.



To designate access to printer drivers

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the box beside the desired driver source or sources.
5. Click **OK**.

Client-side printing is enabled by default. Administrators disable client-side printing through the Admin Console's **Host Options** dialog.

To disable support for client printers

1. In the Admin Console, select the desired host from the list of All Hosts.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Disable **Universal Printer Driver** and **Windows Printer Drivers**. When neither of these options is selected, client printing is disabled.
5. Click **OK**.

Printer Configuration

When GO-Global clients connect to a host, **proxy printers** are automatically created on the host and serve as an interface for printing to the client printer. Proxy printers are printers GO-Global sets up on the host as a bridge between the applications running in a GO-Global session and the client printers. Proxy printers can be configured automatically or manually.

Native printer drivers are preferred when configuring proxy printers — *if* they are available and *if* settings allow them to be used. Alternatively, the **Universal Printer Driver** can be used when the native driver is not available.

There are several methods an administrator can use to manage which printer drivers should be used when creating proxy printers. Settings from client printers are replicated in their proxy printer counterpart. A session's proxy printers are removed when the session ends. Proxy printers are not removed when a session disconnects. All proxy printers on the system are removed when the Application Publishing Service starts.

When a proxy printer is configured, there is a hierarchy of preferences when selecting a native printer driver. If the **Windows Printer Drivers** option is disabled in the Admin Console, this hierarchy is not applied.

Native drivers are selected in the following order:

- **Printers Applet.** A user's manual selection of a printer driver in the Printers Applet takes precedence over all other driver selection methods.
- **Mapped Printer Drivers.** MappedPrinterDrivers.xml contains a list of driver names that can be used for each driver. This file is generated by the Application Publishing Service, but can also be manually edited by administrators.
- **Client driver name.** The driver with the exact name of the driver that is installed on the client is used to configure the proxy printer.

Administrators can set a wait time for GO-Global to configure client printers before performing user session initialization tasks and starting applications. Administrators can do this by changing the value of the **PrinterConfigWaitTime** property in the DefaultWorkspaceProperties.xml page. For more information, see Setting a Printer Configuration Wait Time.

Printers Applet

GO-Global's Printers Applet allows users to add and remove printers, set the default printer, change printer drivers, edit the settings of printers using native printer drivers, and print test pages. The Printers Applet is accessible via the Program Window. It lists all the client printers that are configured and all the host printers that the user has access to. The list of printers depends on the printer drivers setting in the Admin Console as well as the -ac and printerconfig parameters.

Icons in the Printers Applet are described below.

	Indicates that the printer is installed on the client
	Indicates the default printer, which is installed on the client
	Indicates the printer is installed on the host
	Indicates the default printer, which is installed on the host

Settings made with the Printers Applet are saved the next time the user signs in to GO-Global. These settings take precedence over command-line options. Printer changes made in the Printers Applet take effect immediately. Users do not need to restart their session.

Adding and Removing Printers

When a printer is added or removed via the Printers Applet, it does not add or remove it from the client computer, it only determines which printers are configured for use with GO-Global.

To add a client printer

1. From the Program Window, click File | Printers.
2. Click the **Add** button.
3. From the **Add Printer** dialog, select the desired printer and click **Add**. This adds the printer to the list of configured printers and is now available for use.

When a printer is added through the Printers Applet, it gets configured at startup regardless of the -ac command-line option or printerconfig parameter.

To remove a printer

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Remove** button.

Removing a printer from the list prevents it from being configured the next time the user starts a GO-Global session. The printer can be re-added to the list at any time by clicking the **Add** button and selecting it from the list.

Setting the Default Printer

Users can specify their default printer in the Printers Applet. The default printer is indicated by a black circle and checkmark above the printer. Any printer, including host printers, can be designated as the default.

To set the default printer

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Set Default** button.

Editing Default Printer Settings

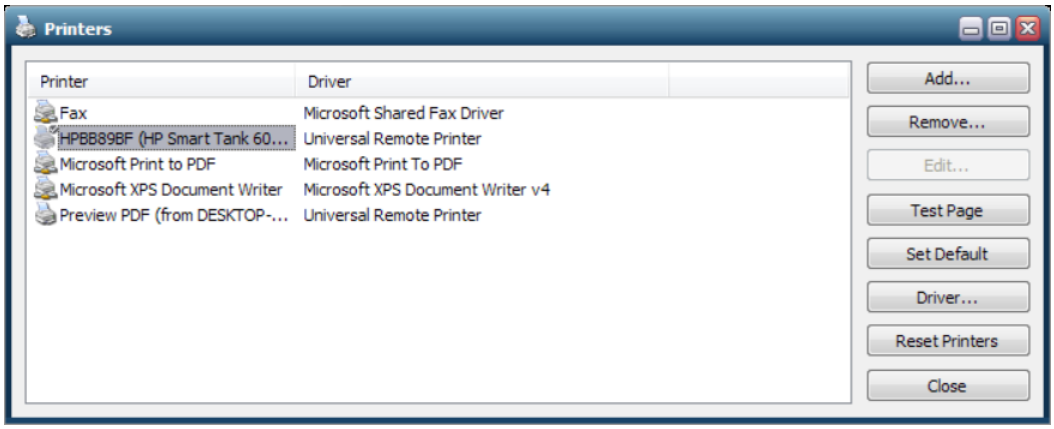
Through the Printers Applet, users can edit the default settings of printers using native printer drivers such as layout, page orientation and paper size.

When the default settings of a printer are changed through the Printers Applet, the changes apply to all applications that are subsequently started by the user on the GO-Global Host, both within the current session and in future sessions. Changes made within the Printers Applet do not affect applications that are running locally on the client computer

To edit printer settings

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Edit** button.
4. Edit the properties, as desired, and click **Ok**.

When AppController for Windows version 6.3.1 or later is used, the **Edit** button is disabled for printers using the Universal Printer Driver. This is because AppController for Windows provides direct access to all the printer's options. In this case, the default options for the printer are configured via **Devices and Printers** on the client computer, not via the GO-Global's Printers Applet.



Printer settings are stored under the user's User Profile. In multi-host environments where a relay load balancer is used, roaming profiles must be enabled to ensure that users' printer settings are replicated across all the hosts in the cluster.

Printing a Test Page

From the Printers Applet, users can print a test page to verify that the printer has been properly configured and to check if a printer is printing graphics and text correctly. A test page also displays information such as the printer name, model, and driver software version, which may be helpful for troubleshooting printer problems.

To print a test page

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Test Page** button.

Changing a Printer's Driver

Through the Printers Applet, users can select different drivers for their printers. This is useful if a driver is not working properly or if a user wants to switch between native drivers and the Universal Printer Driver.

To select a new driver

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Driver** button to open the **Select Printer Driver** dialog, which lists the drivers currently installed on the GO-Global Host machine.
4. Select a new driver, and click **Ok**. The printer is now configured with the new driver.

When only the Universal Printer Driver has been designated as a driver source in the Admin Console, users are unable to change drivers. Users cannot change the driver for GO-Global's Preview PDF printer or for server-based printer.

Resetting Printer Settings

At any time, users can reset printer data to its default settings, including preferences and printer settings. This may be useful if printers are not configuring properly or if users are experiencing printer issues.

To reset printer settings

1. From the Program Window, click File | Printers.
2. Click **Reset Printers**.

Resetting printer settings removes all proxy printers from the session. Users must restart their session in order to print to client printers again. This also resets the default printer to its original default setting.

Mapping Printer Drivers

Administrators can map printer drivers by editing **MappedPrinterDrivers.xml**. For most GO-Global deployments, administrators will not need to edit this file. It is used for specifying which driver to use when a host's driver name does not identically match the client's, or when the administrator wants to override native drivers and force clients to use a different printer driver or the Universal Printer Driver.

To specify a different printer driver

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn\GO-Global.
2. Open the file in WordPad and search for the client printer driver name, for example,
   <driver name="HP LaserJet 2100 Series PS">
   <alternate_driver name= "HP LaserJet 2100 Series PS"> </alternate_driver>
   </driver>
3. Delete the alternate driver name from the alternate_driver entry. In the example above, delete HP LaserJet 2100 Series PS and replace it with the desired printer driver.
4. Save the file. This change will take effect the next time the user starts a GO-Global session.

For example:

<driver name="HP LaserJet 2100 Series PS">
<alternate_driver name= "HP LaserJet 2200 Series PS"> </alternate_driver>
</driver>

In the example above,
<driver name="HP LaserJet 2100 Series PS">
is the driver that is used on the client.

<alternate_driver name= "HP LaserJet 2200 Series PS" >
is the driver that should be mapped to on the host.

Mapping printer drivers can also be used to force printers to use the Universal Printer Driver.

To force the printer to use the Universal Printer Driver

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn\GO-Global.
2. Open the file in WordPad and search for the client printer driver name, for example,
   <driver name="HP LaserJet 2100 Series PS">
   <alternate_driver name= "HP LaserJet 2100 Series PS"> </alternate_driver>
   </driver>
3. Delete the driver name from the value field. In the example above, delete HP LaserJet 2100 Series PS and replace it with Universal Remote Printer, as follows:

<driver name="HP LaserJet 2100 Series PS">
<alternate_driver name="Universal Remote Printer"> </alternate_driver>
</driver>

4. Save the file.

The next time users connect to the host, their printer will be configured using the Universal Printer Driver.

Multiple alternate drivers can be specified using additional <alternate_driver> entries.

To designate an additional driver

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn\GO-Global.
2. Open the file in a text editor and search for the client printer driver name. For example,
   <driver name="HP LaserJet 2100 Series PS">
   <alternate_driver name="HP LaserJet 2100 Series PS"> </alternate_driver>
   </driver>
3. Specify an additional driver. For example, add HP LaserJet 2200 Series PS to the list, as follows:
   <driver name="HP LaserJet 2100 Series PS">
   <alternate_driver name="HP LaserJet 2100 Series PS"> </alternate_driver>
   <alternate_driver name="HP LaserJet 2200 Series PS "> </alternate_driver>
   </driver>
4. Save the file.

Administrators can add an unlimited number of drivers. GO-Global attempts to configure client printers using the drivers in the order they are specified.

To remove printer driver mapping

1. Open **MappedPrinterDrivers.xml** in a text editor and delete the entire modified line. For example, delete:
   <driver name="HP LaserJet 2100 Series PS">
   <alternate_driver name=" HP LaserJet 2100 Series PS "> </alternate_driver >
   </driver>
2. Save the file.

The **MappedPrinterDrivers.xml** file can be deleted to remove any prior changes. The file is recreated when users sign in to the host.

Client printers are temporarily installed on the GO-Global Host for the duration of the client's session. Printer drivers are installed permanently. Administrators can view the list of printers and drivers in the Printers folder on the GO-Global Host.

Exporting Printer Settings to a File

Most printers store their settings in the Windows DEVMODE structure. GO-Global saves the contents of each printer's DEVMODE structure when users sign out and restores these settings when printers are re-created when users sign back in. In some cases, printing problems may arise when a printer does not store all of its settings in the DEVMODE structure.

Administrators can add the entry, **<export_printer_settings>true</export_printer_settings>** to **MappedPrinterDrivers.xml** so when a user saves the settings for a printer, the settings will be written to a file rather than to the Windows DEVMODE structure.

To export printer settings to a file

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn\GO-Global.
2. Open the file in a text editor and search for the client printer driver name, for example, <driver name="HP LaserJet 2100 Series PS">
   <alternate_driver name="HP LaserJet 2100 Series PS"> </alternate_driver>
   </driver>
3. Add the entry <export_printer_settings>true</export_printer_settings>, as follows:
   <driver name="HP LaserJet 2100 Series PS">
   <alternate_driver name="HP LaserJet 2100 Series PS">
   <export_printer_settings>true</export_printer_settings> </alternate_driver>
   </driver>
4. Save the file.

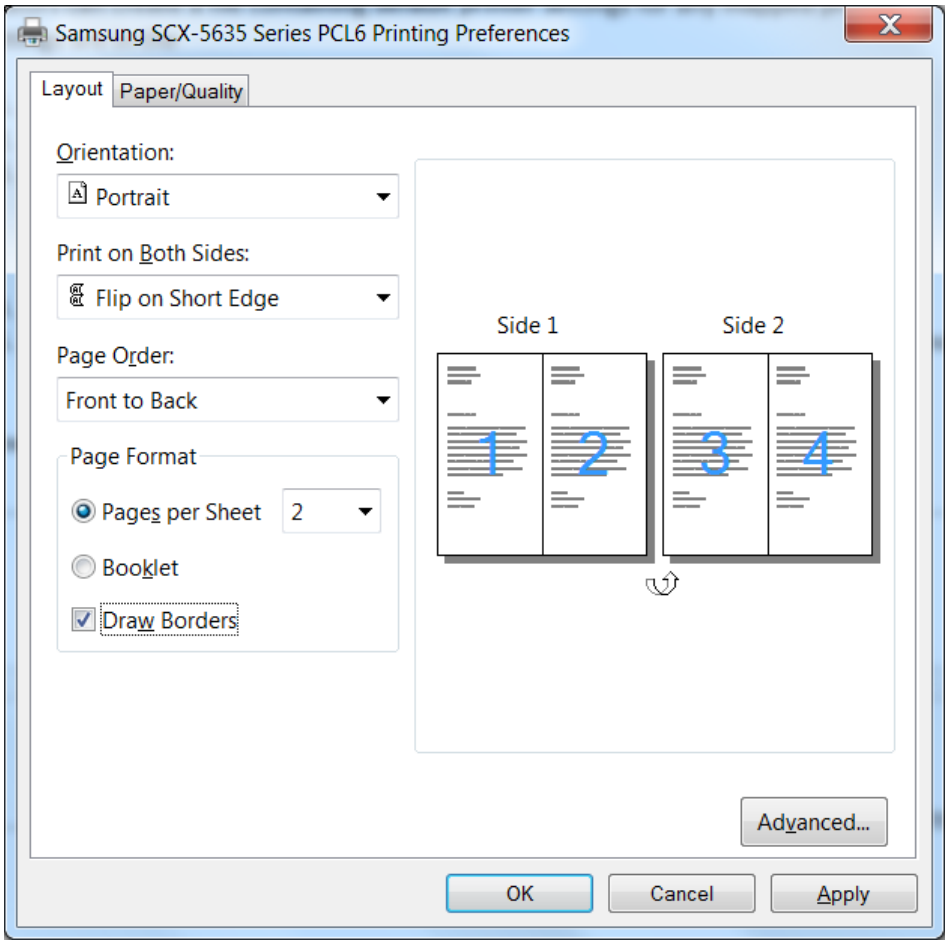
If <export_printer_settings> is set to false, printer settings will be stored in the DEVMODE structure.

Creating a Default Printer Setting File for a Mapped Printer

Administrators can create a file containing default printer settings for any mapped printer. Adding the entry **<default_printer_settings_file>** and specifying a printer settings file in **MappedPrinterDrivers.xml** allows administrators to specify default settings for a printer if the user's individual file does not exist, either because **<export_printer_settings>** is set to false or the user hasn't made any changes to the printer settings yet. After setting printer preferences, export the settings to a file, then add the default printer settings file to **MappedPrinterDrivers.xml**. The default settings file should be saved in a public location so it is accessible to all users.

To set printer preferences

1. From the Control Panel, select **Devices and Printers**.
2. Right-click the desired printer and select **Printing Preferences**.
3. Edit the printer's preferences and click **Apply**.
4. Click **OK** to close the **Printing Preferences** dialog.



To export the new printing settings to a file

Run a Command Prompt as Administrator and type the following command:

rundll32.exe printui.dll PrintUIEntry /Ss /n "*printer name*" /a "*full path to settings file*"

For example:
rundll32.exe printui.dll PrintUIEntry /Ss /n "HP Officejet Pro 8600" /a "*C:\printersettings\Officejet.dat*"

To create a default printer settings file in MappedPrinterDrivers.xml

1. Stop the **Application Publishing Service**.
2. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn\GO-Global.
3. Add the following:

   <driver name="*printer driver name*">
   <alternate_driver name="*alternate driver name*">
   <export_printer_settings>true</export_printer_settings>
   <default_printer_settings_file>*full path to settings file*
   </default_printer_settings_file>
   </alternate_driver>
   </driver>

   For example:
   <driver name="HP Officejet Pro 8600">
   <alternate_driver name="OfficeJet Driver 1">
   <export_printer_settings>true</export_printer_settings>
   <default_printer_settings_file>C:\printersettings\Officejet.dat</default_printer_settings_file>
   </alternate_driver>
   </driver>

Do not add the quotation marks around the path specified in the default_printer_settings_file.

4. Save the file.
5. Load the **MappedPrinterDrivers.xml** in a browser. Verify that the browser displays the file's contents correctly and does not report any errors.
6. Start the **Application Publishing Service**.

To test the default printer settings file

1. Open the **Printer Properties** dialog on the host.
2. Click the **Stocks** tab and create a new user-defined stock.
3. Run the following in a command prompt on the host:

   rundll32.exe printui.dll PrintUIEntry /Ss /n [printer name] /a [full path to settings file]

   Be sure to put the printer name and the path in quotation marks.
   For example:

   rundll32 printui.dll PrintUIEntry /Ss /n "ZDesigner GC420d" /a "C:\temp\default_settings.dat"
4. Stop the Application Publishing Service.
5. In MappedPrinterDrivers.xml, add the following:

```
<mappedprinterdrivers version="2.0">
<driver name="ZDesigner GC420d">
<alternate_driver name="ZDesigner GC420d">
<export_printer_settings>true</export_printer_settings>
<default_printer_settings_file>C:\temp\default_settings.dat
</default_printer_settings_file>
</alternate_driver>
</driver>
</mappedprinterdrivers>
```

Do not add the quotation marks around the path specified in the default_printer_settings_file.

6. Save the file.
7. Load **MappedPrinterDrivers.xml** in a browser. Verify that the browser displays the file's contents correctly and does not report any errors.
8. Start the **Application Publishing Service**.
9. Start a GO-Global session and add the client printer.
10. Open the Printers Applet and check the **Stock** tab in the printer properties. The user-defined stock will be listed.

Client Printer Naming Customization

GO-Global installs a printer on the host for each printer that is configured on the client machine. These printers are called proxy printers and are the printers that are seen by users when printing via GO-Global. Since multiple users connect to a GO-Global Host, these printers must be filtered so that users see only their own printers. This requires that each printer be assigned a unique identifier.

Through the Registry, administrators can specify the format of these proxy printer names and include information such as the user's name, the client computer's IP address, and the client machine name. The **PrinterNameFormat** Registry key is created after a GO-Global session is started.

Administrators can choose from the following tokens to create a suffix to the printer string name:

Token	Description	Example
%U	The user name	Wilson
%I	The client IP address	192.168.100.147
%M	The client's unique ID (GUID)	800fb6b5770-ed9e-11df-82ae-000874b1cdb1
%C	The client machine name	HRWorkstation
%S	The GO-Global session ID	7

To customize the client printer name

1. Run the Registry Editor (regedit.exe)
2. From the Registry Editor, expand the **HKEY_LOCAL_MACHINE** key.
3. Locate the **PrinterNameFormat** key: [HKLM\Software\GraphOn\GO-Global\AppServer\PrinterNameFormat]
4. Right-click **PrinterNameFormat** and select **Modify**.
5. In the **Value data** field, type one or more of the client printer customization tokens.
6. Close the Registry Editor.

The PrinterNameFormat key is set to (from %C) by default. Using the above examples, printer names would appear as: PrinterName (from HRWorkstation)

Any special characters other than % in the PrinterNameFormat string are taken literally, since they are not tokens.

There are 12 characters that are not allowed. These characters are ! , \ = / : * ? " < > and |. If any of these characters are used in the string, they are replaced with a hyphen.

Adjusting the Printable Area

In some cases, applications that print using the GO-Global Universal Printer Driver (UPD) will have areas of the document that are clipped — when portions of the document near the edges of the page are not printed. To address this issue, define the printable area of a document with an alternate .PPD file.

To install the alternate .PPD file

1. Download **UniversalRemotePrinter.ppd** from: https://releases.graphon.com/files/UniversalRemotePrinter.ppd
2. Stop the **Application Publishing Service**.
3. Rename the *original* **UniversalRemotePrinter.ppd**, then copy the *alternate* UniversalRemotePrinter.ppd to the following folder: C:\Windows\System32\spool\drivers\x64\3
4. Delete **UniversalRemotePrinter.bpd** if it exists.
5. Start the **Application Publishing Service**.

If there are any issues with the alternate .PPD, use the same process above to revert to the original .PPD.

The UniversalRemotePrinter.ppd file defines driver settings for the Universal Printer Driver. In the default version of this file, the area to which the driver can print is the full extent of a page. This means that text or images can be printed to the edges of a page. Most printers are not physically capable of this. The alternate .PPD file defines a 1/4 inch (6.35 mm) margin for the defined paper sizes. This allows applications to predict the printable area and thereby lay out print jobs without clipping.

PDF Conversion and PDF Printing Libraries

GO-Global's PDF Conversion and PDF Printing libraries improve the speed and quality of printing using the Universal Printer Driver.

When upgrading from earlier versions of GO-Global, GO-Global will continue to use the old libraries by default. To enable the *new* libraries, change the values of both the **PDFConverter** and **PDFPrinter** properties in HostProperties.xml from 1 to 2.

To enable the PDF Converter and PDF Printer Libraries

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\HostProperties.xml in a text editor.
3. Find the **PDFConverter** property and change its associated value to 2.
4. Find the **PDFPrinter** property and change its associated value to 2.
5. Save HostProperties.xml.
6. Start the **Application Publishing Service**.

GO-Global clients must be updated to version 6.3.1 or later in order to use the new printing libraries. This enhancement is supported on the Windows client only.

CHAPTER XII

Mobile App Console

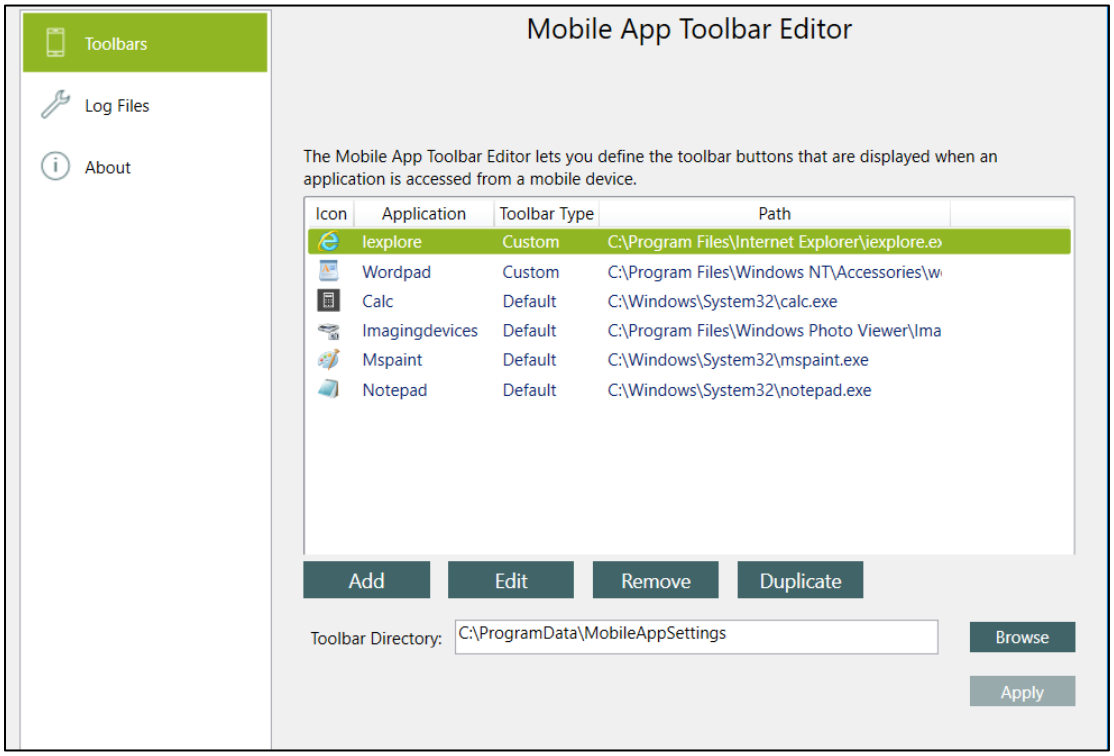
12

Mobile App Toolbar Editor

The Mobile App Toolbar Editor is used to define the toolbar buttons and menus that are displayed when an application is accessed from a mobile device. Both the buttons and the menu items will appear in the toolbar at the bottom of the application. Menu items can include submenu items, which appear in another toolbar directly above the main toolbar.

To open the Mobile App Toolbar Editor

1. From the Admin Console, click Tools | Mobile App Console.
2. Select **Toolbars**.

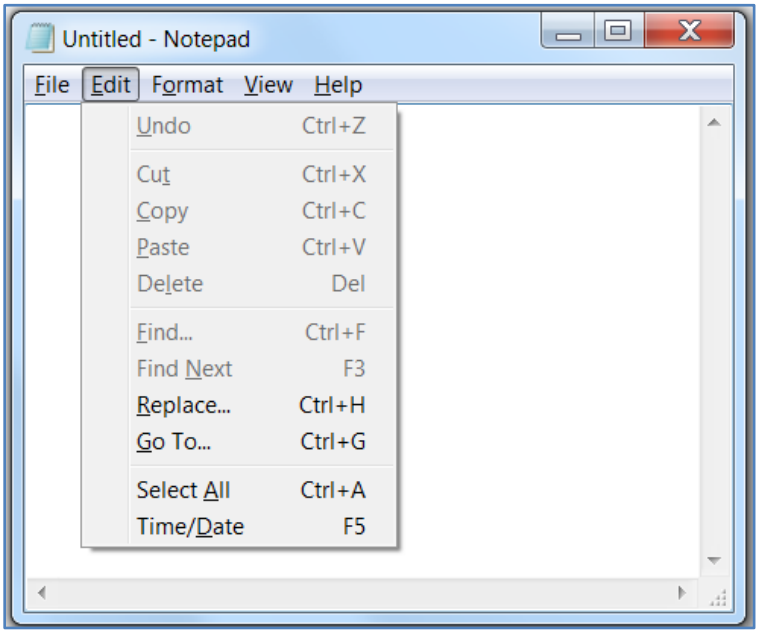


Applications that are published in the Admin Console will be listed, and each will be configured to use the default toolbar.

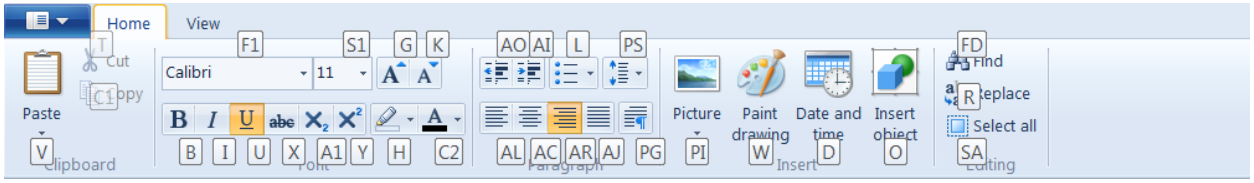
The **Add**, **Edit**, **Remove** and **Duplicate** buttons apply only to the custom toolbars, and not to the applications. For example, clicking the **Remove** button will remove the custom toolbar from the selected application. The application will still be published in the Admin Console and will still be available to users.

Creating Custom Toolbars

Check the menus of the applications you are creating custom toolbars for, to verify shortcut keys. Every application has its own shortcuts, and shortcuts that work in one might not work in another.



In applications that have toolbars, such as Microsoft Word and WordPad, click Alt + H while in the Home tab, to display available shortcuts.

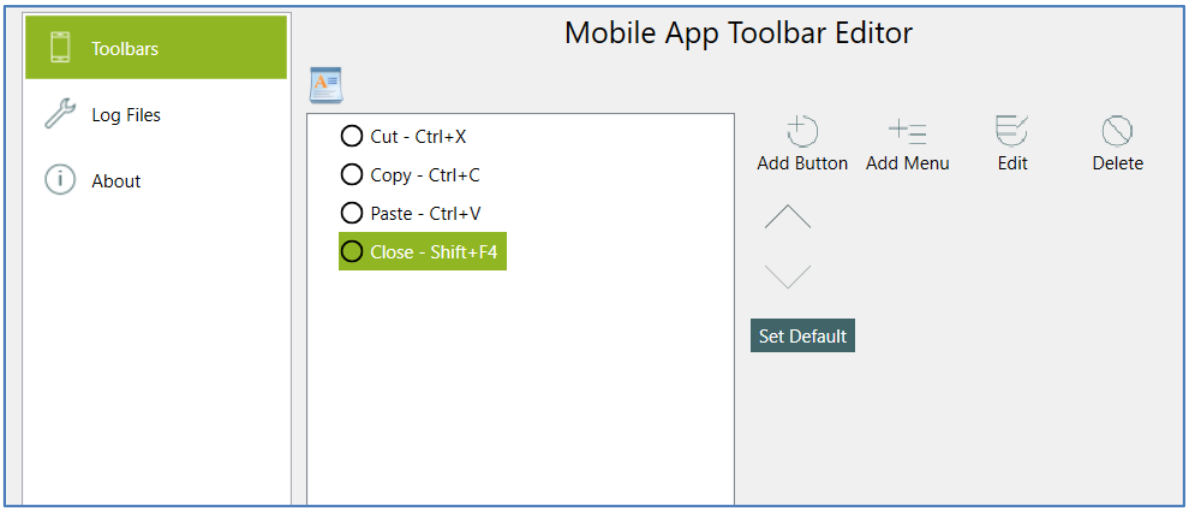


In the following instructions for creating a custom toolbar, WordPad is used as the example application.

To add a button

1. Select an application from the list of applications and click the **Edit** button.
2. Click the **Add Button** to open the **Add button** dialog.
3. Type a name for the new button in the **Label** field.
4. Add the associated shortcut. Do this by using the shortcut keystrokes on your keyboard. For example, press Ctrl + X on the keyboard, and this will appear in the **Shortcuts** field.
5. Click **Add**. This will add the button and the shortcut to the toolbar list.
6. Click **Apply**. This button will now appear in the application's toolbar on the mobile client device. You can continue to add buttons or menu items, or click the **Custom Toolbar List** button to add toolbar and menu items to a different application.

In the example below, buttons for **Cut** (Ctrl + X), **Copy** (Ctrl + C), **Paste** (Ctrl + V), and **Close** (Shift + F4) have been added to the custom toolbar:

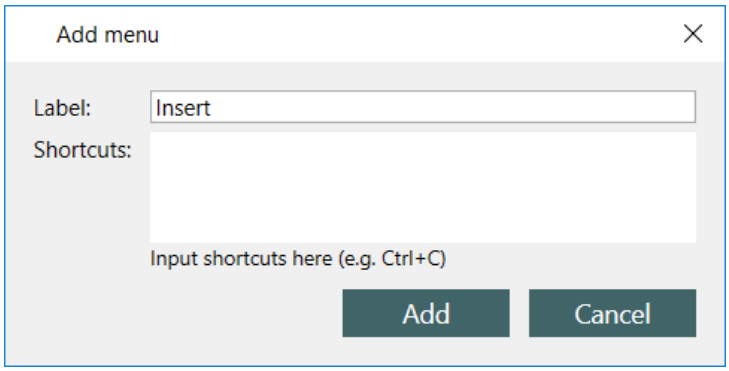


A menu item is similar to a toolbar button but can have up to three submenu items.

To add a menu item

1. Select an application from the list and click the **Edit** button.
2. Click the **Add Menu** button to open the **Add menu** dialog. Type the menu item name in the **Label** field.
3. For menus, the Shortcuts field is typically left blank. However, if you want the application to perform an action when the menu is opened, type the shortcuts for the action in the **Shortcut** field.
4. Click **Add**.

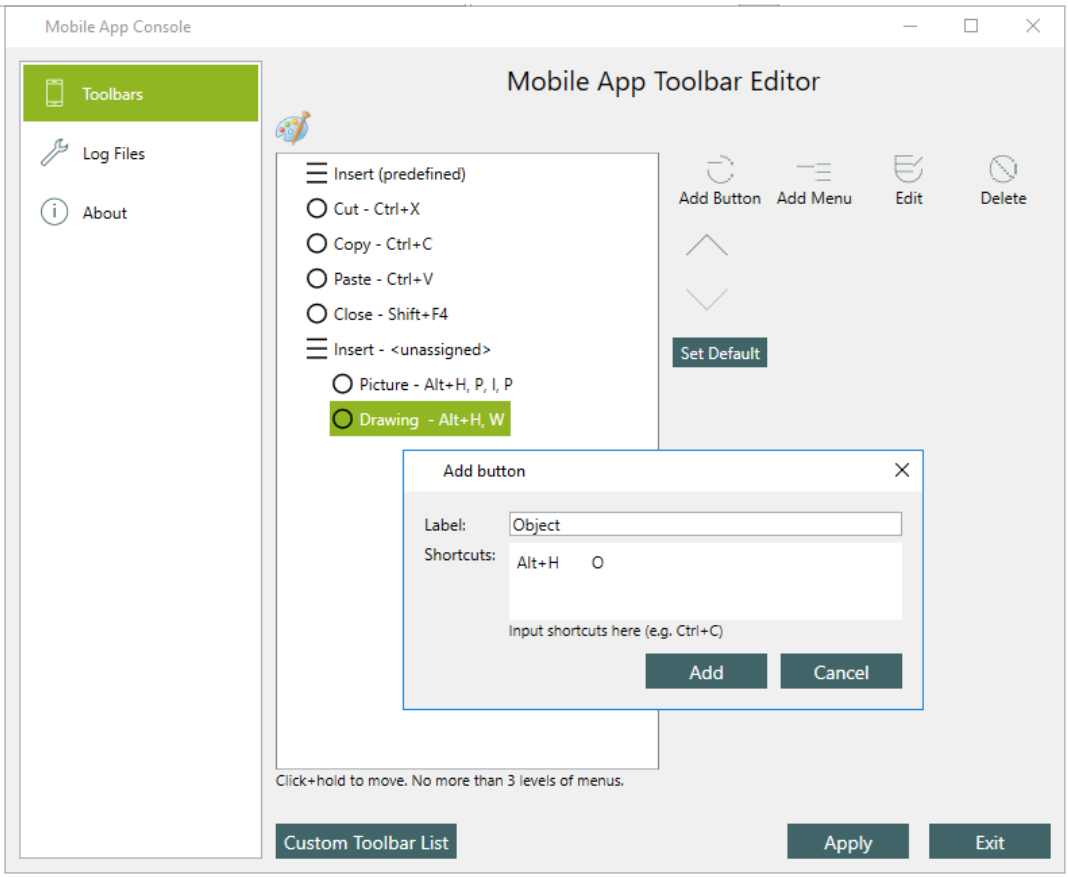
5. Click **Apply**. This menu item will now appear in the application's toolbar on the client device.



To add a button to a menu

1. Highlight the menu item from the toolbar list and click **Add Button**.
2. In the **Add button** dialog, type a name for the new button in the **Label** field.
3. Type the shortcut(s) for the action in the **Shortcuts** field.
4. Click **Add**.
5. Click **Apply**.

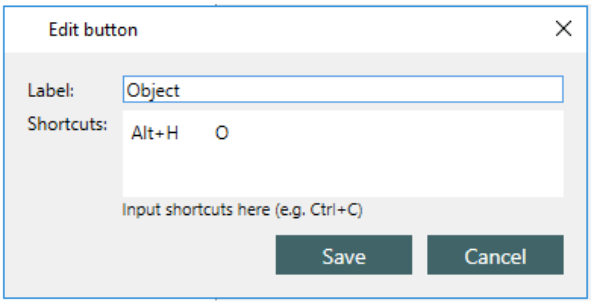
In the example below, an **Insert** menu was created, with buttons for inserting pictures, drawings, and objects. To insert an object in WordPad using shortcut keys, a user would click Alt + H, then O. By creating the submenu button for Object in the Toolbar Editor, with the appropriate shortcut keys (i.e., Alt + H, then O), a user on a mobile device can click the **Object** button on the custom toolbar to insert an object into a document.



You can add up to ten items per menu level and up to five shortcuts per button.

Editing toolbar buttons and menu items

1. To edit a button or menu item, highlight the item from the list and click **Edit**.
2. To delete an existing shortcut, hover the mouse over the text in the **Shortcuts** field. Click the x that appears over the gray highlighted text.
3. Type a new shortcut.
4. Click **Save**.

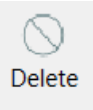


To move a button or menu item up or down

Highlight the item in the toolbar list and click the **Move up** or **Move down** button.

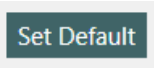
To delete a button or menu item

Highlight the item in the toolbar list and click the **Delete** button.



To revert to the default toolbar

Click the **Set Default** button. This will delete the custom toolbar settings.



Adding a custom toolbar for an application's child program

Some applications published in the Admin Console will launch one or more child programs that perform a subset of the application's tasks. In some cases, an application's main functionality may be provided by an unpublished child program. In these cases, you can add a toolbar for a child program using the **Add** button, and you can copy an existing toolbar to the child program using the **Duplicate** button.

To create a toolbar for a child process

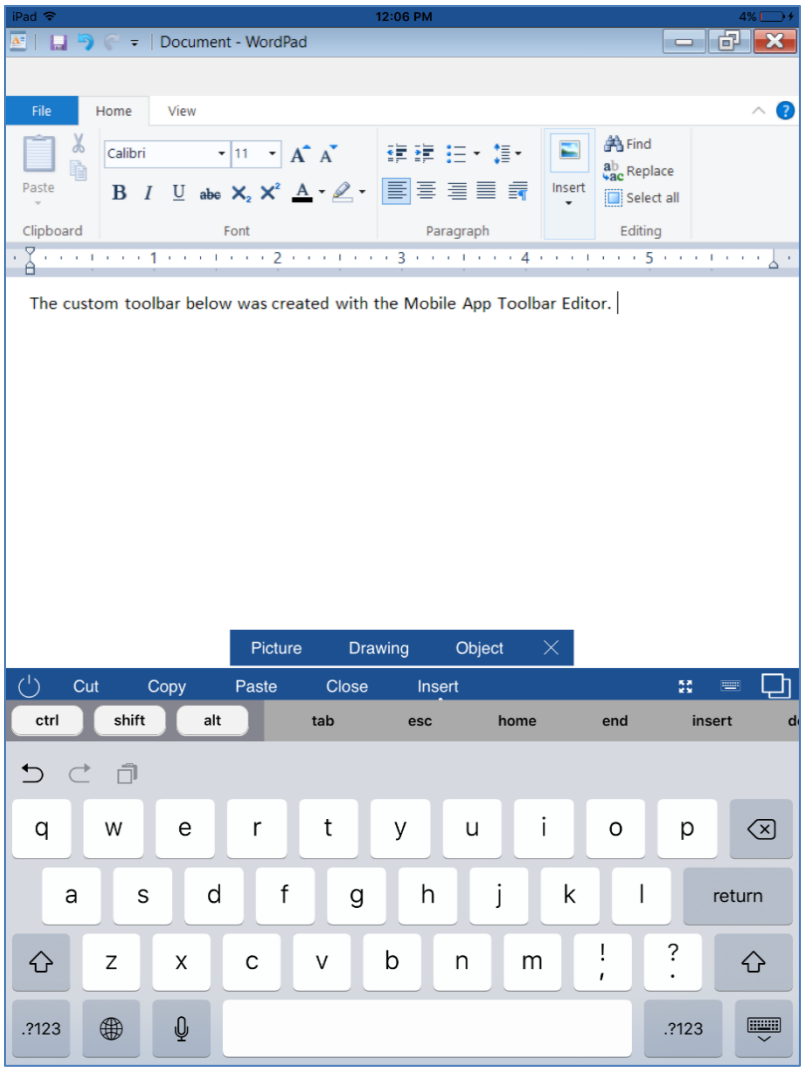
1. In the Toolbar Editor, click **Add**.
2. Browse to the child program's executable file.
3. Select the file and click **Open**.
4. Add buttons and menus as described above.

To copy a toolbar

1. To copy an existing toolbar to use with a child program, select the application's toolbar you want to copy from the list.
2. Click the **Duplicate** button.
3. Browse to the child program's executable file.
4. Select the file and click **Open**.

Viewing the Custom Toolbar

You can view the toolbar buttons you created by opening the GO-Global App on a mobile device. Launch WordPad, for example, to see the custom toolbar buttons at the bottom of the screen. Tap **Insert** to open the submenu. Tap the **X** to close the submenu.



Changing the Toolbar Directory

Toolbar files are stored in the **C:\ProgramData\GraphOn\GO-Global\MobileAppSettings** directory by default. If you have multiple GO-Global Hosts, you can store the toolbar in a shared network directory and use the same toolbar files on all hosts.

To change the directory where toolbars are stored

1. Browse to or type the path to the desired directory in the **Toolbar Directory** field.
2. Click **Apply**.
3. If you have already created toolbars, you will be asked if you want to copy the existing toolbars to the new directory.

Log Files

When logging is enabled, the Mobile App Console records messages in log files that are stored in the **%PROGRAMDATA%\GraphOn\GO-Global\MobileAppLogs** directory. Logging can be enabled and disabled in the Log Files panel of the Mobile App Console. Logging is disabled by default.

To enable logging

1. Click the checkbox next to **Enable Logging**.
2. Click **Apply**.

When logging is enabled, you can change the directory in which log files are stored by entering the path to the desired directory in the **Log Directory** field and clicking **Apply**.

CHAPTER XIII

Advanced Topics

13

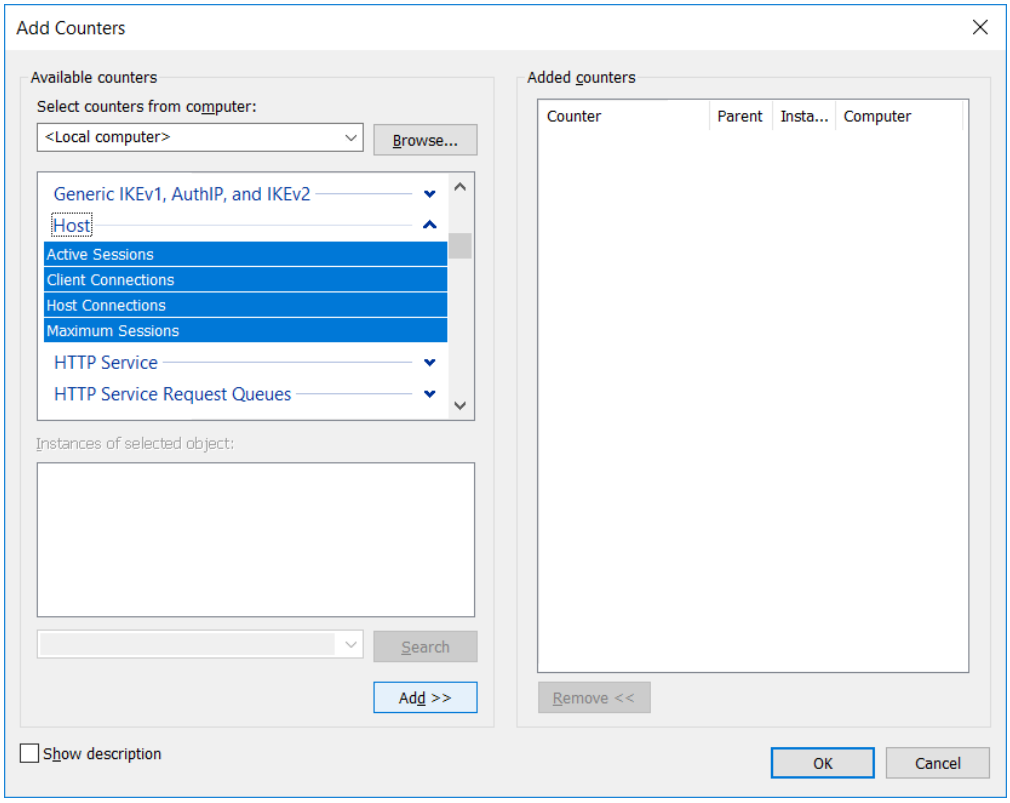
GO-Global Host Performance Counters

GO-Global Host performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a host. Performance counters can also be added to track the number of Application Hosts connected to an Application Host Manager (i.e., Relay Load Balancer or Farm Manager) and to identify the maximum number of sessions allowed on a host

GO-Global Host performance counters allow administrators to monitor host activity from any machine with network access to a GO-Global Host. The Remote Registry Service (Regsvc.exe) must be enabled for remote performance monitoring to work.

To add GO-Global Host Performance Counters to the Performance Monitor

1. Click Start | Programs | Administrative Tools | Performance Monitor.
2. Click **Performance Monitor**, then click the **+** button to add counter(s).
3. From the **Available counters** list, locate and click **GO-Global Host.**
4. Click the **Add >>** button to add the four counters (Active Sessions, Client Connections, Host Connections, Maximum Sessions).
5. Click **OK**.



GO-Global Host Performance Counters include:

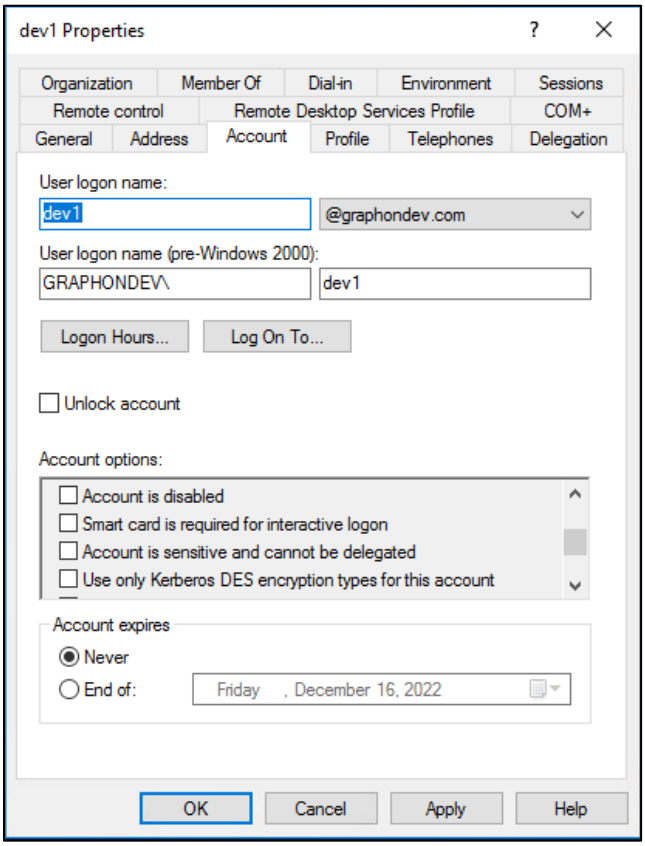
- **Client Connections**. The total number of client connections on Independent Hosts, Farm Hosts, or Relay Load Balancers. This value is always zero for Dependent Hosts and Farm Managers.
- **Host Connections**. The total number of Dependent Hosts connected to an Application Host Manager. This value is always zero for Application Hosts.
- **Active Sessions**. For Application Hosts, this is the number of client sessions running on the host. For Application Host Managers, this is the total number of sessions hosted on all connected Application Hosts.
- **Maximum Sessions**. This displays the **Maximum Session Count** set in the Admin Console's **Host Options** dialog.

Configuration Requirements for Delegation Support

When **OpenID Connect authentication** is used with the **Automatically sign users in to their domain accounts** option, or when **Integrated Windows authentication** is used, applications running in GO-Global sessions may not be able to access services running on other computers on the network unless either a) Delegation is enabled and configured to allow applications running on the GO-Global Host to access services running on the network or b) the associated **Cache passwords on the host** option is enabled. For example, Group Policy may not be applied if neither Delegation nor **Cache passwords on the host** are enabled.

Since the purpose of the **OpenID Connect authentication** and **Integrated Windows authentication** options is generally to provide Single-Sign-On (SSO) support, it is usually undesirable from both security and user-experience standpoints to enable the **Cache passwords on the host** option. It takes more effort to configure Delegation support, but this is the more secure way to provide access to backend services.

To enable delegation, first ensure that your user accounts may be delegated. In the **Active Directory Users and Computers** Management Console, select a user and click **Action | Properties**. Click the **Account** tab. In the Account options list box, scroll down and ensure the **Account is sensitive and cannot be delegated** option is disabled.



Next, enable each GO-Global Host to delegate users' accounts to other computers:

1. In the **Active Directory Users and Computers** Management Console, select the computer.
2. Click Action | Properties.
3. Click the **Delegation** tab.
4. Click Trust this computer for delegation to specified services only.

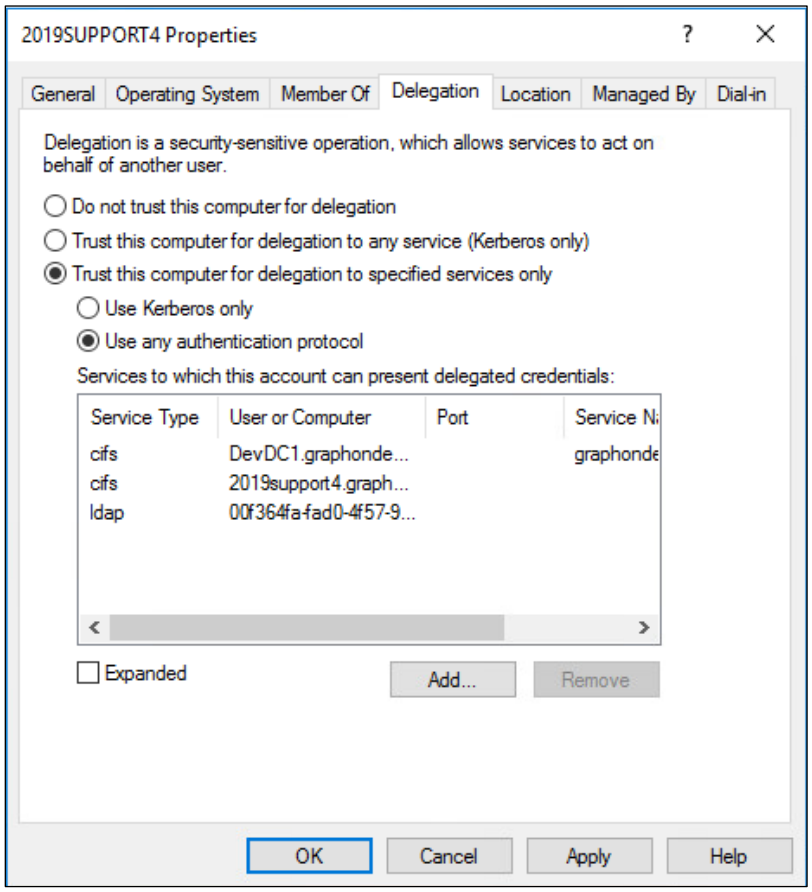
If you are using **Integrated Windows authentication**, you may alternatively select **Trust this computer for delegation to any service (Kerberos only)**. This option enables unconstrained delegation. Unconstrained delegation is easier to configure, but it is not secure because it allows processes running in GO-Global sessions to access any service running on the network. For this reason, GraphOn does not recommend using this option. Unconstrained delegation does not work with **OpenID Connect authentication**.

5. If using Integrated Windows authentication, click **Use Kerberos only**. Alternatively, if using OpenID Connect authentication, click **Use any authentication protocol**. (*Important*: Delegation will not work if **OpenID Connect authentication** is used and **Use Kerberos only** is selected.)
6. Click **Add**.
7. Click **Users or Computers**.
8. Select a computer that you want users to be able to access.
9. Click **OK**.
10. Select the services that you want users to be able to access.
    (For example, to enable users to apply Group Policy, select a domain controller at step 8 and then select the LDAP and CIFS services at step 10. Alternatively, to allow users to access a file share, select the file server at step 8 and select the CIFS service at step 10.)
11. Click **OK**.
12. Repeat steps 6-11 for each computer and service that you want users to be able to access. For example, repeat these steps for each domain controller.
13. Click **OK** to save the changes.
14. Restart the host computer to ensure the changes are applied to the computer.

CIFS stands for **Common Internet File System**. The CIFS service enables applications to access files on a server over the network. The GO-Global logon process needs to access this service on domain controllers to apply Group Policy.

LDAP stands for **Lightweight Directory Access Protocol**. The GO-Global logon process needs to access the LDAP service on domain controllers to retrieve Active Directory information and apply Group Policy.

After changing delegation options in the Active Directory, the GO-Global Host must be restarted for delegation to take effect.



To support Integrated Windows authentication and OpenID Connect authentication to domain accounts, the **GO-Global Application Publishing Service** must be able to register its Service Principal Name (SPN) with Active Directory. It attempts to do this every time the service starts. If the host computer is a member of a domain, the Application Publishing Service will register its SPN with the domain with the form {54094C05-F977-4987-BFC9-E8B90E088973}/[hostname.domain.com].

To verify that the SPN has been properly registered, run the setspn command from an elevated CMD process as follows: setspn [hostname.domain.com]

Mapped Drives

Drive mappings are private within each GO-Global session. For example, if there are two sessions running on a GO-Global Host, a drive letter (H, for example) can be mapped to one network share in session 1 (e.g., \\servername\session1), and the same drive letter can be mapped to a different network share in session 2 (e.g., \\servername\session2).

Define drive letter mappings using logon scripts. You can also allow users to define their own drive letter mappings by publishing applications that provide this functionality.

Drive mappings defined within the interactive session on the GO-Global Host are not available to remote users. If all users require access to the same network share through a drive mapping, the drive mapping will generally need to be defined in a logon script.

Multi-Monitor Support

GO-Global supports multiple monitors on Windows and macOS. Multi-monitor support is enabled by default but can be disabled manually.

To disable multi-monitor support via a shortcut
Add the argument -mm 0 to the AppController shortcut.
For example, AppController.exe -h server1 -mm 0

To enable multi-monitor support via a shortcut
Append the argument -mm 1 to the AppController shortcut.
For example, AppController.exe -h server1 -mm 1

To disable multi-monitor support via the logon page
Set the multimonitor parameter to false.
For example, **http://hostname/goglobal/?multimonitor=false**

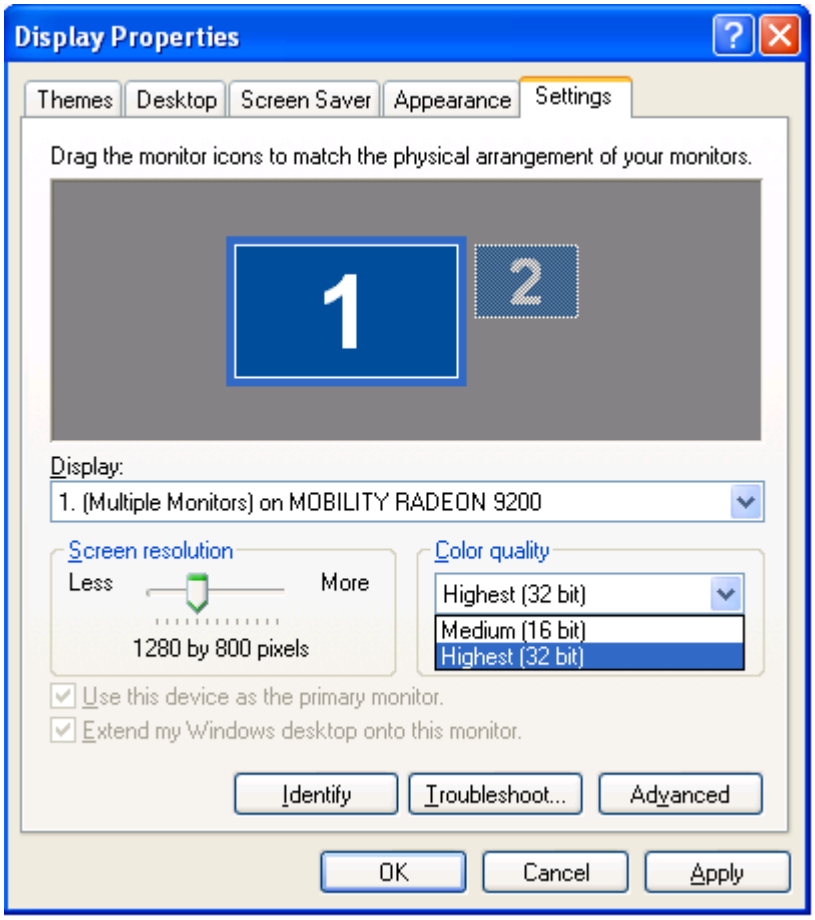
To enable multi-monitor support via the logon page
Set the multimonitor parameter to true.
For example, **http://hostname/goglobal/?multimonitor=true**

Specifying the Maximum Color Depth for GO-Global Sessions

The color depth (or color quality) of a GO-Global session can affect the quality of images in some applications. GO-Global sessions will run at the color depth of the client system up to a maximum value. By default, the maximum depth is set to 32-bits per pixel.

To increase or decrease the maximum color depth of a GO-Global session, use the -mx option when running GO-Global from a shortcut. The maximum color depth can be specified as follows: -mx 32, -mx 24, -mx 16, or -mx 8. A GO-Global session will use the minimum value of the -mx option and the color depth of the client system. For example, in order for a GO-Global session to run at 16-bits per pixel, -mx 16 must be added to the command-line and the client system must be running at 16-bits per pixel.

For example, "C:\Program Files\GraphOn\AppController\AppController.exe" -mx 16



When running GO-Global from the logon page, use the maxbpp parameter with the values 8, 16, 24 or 32.

For example, to set the maximum color depth to 24-bits per pixel, append maxbpp=24, as follows: http://hostname/goglobal/?maxbpp=24

Enabling Image Compression

GO-Global has the ability to compress all images to a maximum of 256 colors per image. If users are seeing slow performance due to low bandwidth on the host or client network, administrators can enable image compression to significantly decrease the bandwidth sent from the GO-Global Host. When image compression is enabled, complex images may lose some sharpness.

To enable image compression on GO-Global clients, append **-qt 1** to the target of the AppController shortcut, as follows:
"C:\Program Files\GraphOn\AppController\AppController.exe" -qt 1

To enable image compression via the logon URL, set the **quantize** parameter to true. For example, **http://hostname/goglobal/?quantize=true**

To enable image compression for *all clients* connecting to a GO-Global Host, set the value of the **QuantizeSwitch** parameter to 1 in C:\ProgramData\GraphOn\GO-Global\HostProperties.xml on the GO-Global Host.

Modifying the fontContrast Property

Font and text clarity can be adjusted by modifying the value of the **fontContrast** property in the **DefaultWorkspaceProperties.xml** file. The maximum value for **fontContrast** is 2200 and the minimum value is 1000. The property is set to 1400 by default.

To modify the fontContrast Property

1. Stop the Application Publishing Service.
2. Locate the **DefaultWorkspaceProperties.xml** file in the C:\ProgramData\GraphOn\GO-Global directory.
3. Open **DefaultWorkspaceProperties.xml** in WordPad and locate the following section:
   </property>
   <property type="UINT32" group="Miscellaneous" id="fontContrast">
   <value>1400</value>
   </property>
4. Replace 1400 with the desired value.
5. Save the edited .xml file.
6. Start the **Application Publishing Service**.

Setting a Printer Configuration Wait Time

Administrators can set a wait time for GO-Global to configure client printers *before* performing user session initialization tasks and starting applications. Administrators can do this by changing the value of the **PrinterConfigWaitTime** property in DefaultWorkspaceProperties.xml from 0 to the maximum number of seconds GO-Global should wait for printers to be configured.

The **PrinterConfigWaitTime** property is set to 0 by default. The maximum number of seconds PrinterConfigWaitTime can be set to is 300 (i.e., 5 minutes).

To set the Printer Configuration Wait Time

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\DefaultWorkspaceProperties.xml in a text editor.
3. Find the **PrinterConfigWaitTime** property and change its associated value to a positive integer between 1 and 300.
4. Save DefaultWorkspaceProperties.xml
5. Start the **Application Publishing Service**.

By setting a printer configuration wait time, users will likely wait longer before being able to start applications in their sessions. During the delay, GO-Global will display a message to users that client printers are being configured.

Disabling the Password Expiration Warning

By default, users are presented with a password expiration warning and new password prompt whenever they log on within 14 days of the password's scheduled date of expiration. Administrators can disable the warning by modifying the **PasswordExpirationWarning** value in the HostProperties.xml file.

Setting **PasswordExpirationWarning** to 0 will disable the password expiration warning in all cases.

Setting **PasswordExpirationWarning** to 1 will enable the password expiration warning in all cases.

The default value is 2, which enables the password expiration warning except when **OpenID Connect authentication** is enabled or when **Integrated Windows authentication** is enabled and **Cache password on the client** is disabled.

To disable the password expiration warning

1. Stop the **Application Publishing Service**.
2. Locate the **HostProperties.xml** file in the %PROGRAMDATA%\GraphOn\GO-Global directory.
3. Open HostProperties.xml in WordPad with administrator rights and locate the following section:

<property id="PasswordExpirationWarning" group="Miscellaneous" type="UINT32">
<value>2</value>
</property>

5. Change the value from 2 to 0 to disable the warning
6. Save the edited .xml file.
7. Start the **Application Publishing Service**.

Key Reporting Method

GO-Global clients can send key press information to hosts in one of two ways: as Unicode characters or as keycodes. Some applications require Unicode characters; others require keycodes. If an application is failing to process key information correctly, you can generally resolve the issue by changing GO-Global's key reporting method.

The **-krm** shortcut and **keyreportingmethod** startup parameter instruct the client to send either Unicode or keycode values to the host based on character type. This option may be used to resolve issues where an application fails to process certain keys correctly.

Valid values for the option are as follows:

0: a-z A-Z are Unicode, 0-9 are Unicode, other characters are Unicode

1: a-z A-Z are keycode, 0-9 are Unicode, other characters are Unicode

2: a-z A-Z are Unicode, 0-9 are keycode, other characters are Unicode

3: a-z A-Z are keycode, 0-9 are keycode, other characters are Unicode

8: a-z A-Z are Unicode, 0-9 are Unicode, other characters are keycode

9: a-z A-Z are keycode, 0-9 are Unicode, other characters are keycode

10: a-z A-Z are Unicode, 0-9 are keycode, other characters are keycode

11: a-z A-Z are keycode, 0-9 are keycode, other characters are keycode

For backward compatibility, the default value of this option depends on the type of client:

- Win32/macOS/HTML5 = 1 (a-z A-Z keycode, all others Unicode)
- iOS/Android = 0 (all characters Unicode)
- Linux = 11 (all characters keycode)

Administrators, however, can set the default value of the option for all clients by changing the value of the **KeyReportingMethod** property in the HostProperties.xml file from 4294967295 (-1) to one of the above values.

To set the KeyReportingMethod value

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\HostProperties.xml in a text editor.
3. Find the **KeyReportingMethod** property and change its associated value, as described above.
4. Save **HostProperties.xml**.
5. Start the **Application Publishing Service**.

The -krm option applies to all applications running in the session. If users are running applications that require different options, they must run the applications in separate sessions with the appropriate -krm options.

Administrators and users can override the default value of the option via the **-krm** and **keyreportingmethod** parameters.

For example, if an application is failing to process number keys correctly in some data fields, you can generally fix this as follows:

1. Determine how the affected keys are sent to the host. For example, if the client is AppController for Windows, the default key reporting method is 1. Referring to the above values for the key reporting method, we see that the number keys (0-9), which are being processed incorrectly in our example, are sent to the host as Unicode characters when the key reporting method is 1.

2. Find the key reporting method that will change the way the affected keys are sent to the host but continue to send the unaffected keys in the same way. In our example, when the key reporting method is 1, keys are sent to the host as follows:

   a-z A-Z: keycode
   0-9: Unicode
   other characters: Unicode

   This needs to be changed so that the client sends number keys (0-9) as keycodes but continues to send a-z and A-Z as keycodes and other (non-numeric) keys as Unicode:

   a-z A-Z: keycode
   0-9: keycode
   other characters: Unicode

The key reporting method that sends keys in this way is method 3.

3. Change the key reporting method via one of the above methods. For example, to set it for all users, change the value of the **KeyReportingMethod** property in HostProperties.xml to 3.

When key events are sent as keycodes, the character that is produced is determined by the selected Keyboard Layout on the host. If key events that are sent as keycodes produce unexpected or incorrect characters, disable Automatic Client Keyboard support, as follows:

1. Locate the file HostProperties.xml (e.g., C:\ProgramData\GraphOn\GO-Global)
2. Open HostProperties.xml in WordPad and locate the **ClientSideIME** property.
3. Set the **ClientSideIME** property to 0.
4. Save the file.

Obtaining the Name of the Client Computer

For applications that require the client's computer name rather than the GO-Global Host's, administrators can add the name of that executable under the Registry key **HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\Compatibility\GetComputerName** as a DWORD with a data value of **0x00000001.** Any time an executable matching any of the names listed under this Registry key with a data value of **0x00000001** calls the Windows **GetComputerName** API, the given buffer will be filled in with the client's computer name rather than the host's.

The standard Windows environment variable **COMPUTERNAME** remains unchanged; its value is the host's computer name.

To obtain the name of the client computer

1. Run the Registry Editor (regedit.exe).
2. From the Registry Editor, expand the **HKEY_LOCAL_MACHINE** key.
3. Locate the **GetComputerName** key: [SOFTWARE\GraphOn\GO-Global\Compatibility\GetComputerName]
4. Create a **DWORD** entry for the executable. (For example, pw.exe).
5. Set the value of the new entry to **0x00000001**.
6. Close the Registry Editor.

Additionally, there is an environment variable named **CLIENTCOMPUTERNAME** that exists as part of the running environment of a published application. This environment variable contains the client's computer name.

The **CLIENTCOMPUTERIPADDRESS** and the **CLIENTNETWORKADDRESS** environment variables perform a similar function; the former contains the local IP address of the client computer, the latter contains the public IP address of the client computer.

When a client reconnects to a session, the **CLIENTCOMPUTERNAME**, **CLIENTCOMPUTERIPADDRESS**, and **CLIENTNETWORKADDRESS** environment variables will be updated in each existing process once they have made an API call to acquire any environment variable. If another process attempts to acquire the environment variables of a session process prior to the session process calling one of these APIs, the value of these environment variables will not appear updated.

The exact API calls that will trigger the update are:

UserEnv!CreateEnvironmentBlock()

Kernel32!ExpandEnvironmentStringsA/W()

Kernel32!GetEnvironmentStringsA/W()

Kernel32!GetEnvironmentVariableA/W()

GO-Global shares the license seat when the username and CLIENTCOMPUTERNAME of the session are the same. The CLIENTCOMPUTERNAME is the COMPUTERNAME of the client computer. GO-Global stores this value in the CLIENTCOMPUTERNAME environment variable in the GO-Global session.

When the GO-Global Web App is used, however, browser security restrictions prevent GO-Global from obtaining the name of the client computer. In this case, GO-Global sets the CLIENTCOMPUTERNAME environment variable to “html5 client” and does not share license seats.

Application Script Support

Many Win32 applications were designed for installation on a client PC and run by only one user. When an application is deployed from a GO-Global Host, multiple users need to be able to run the application simultaneously, and a number of problems may be encountered if the application is not "multi-user ready."

The best way to solve multi-user deployment problems with an application is to modify the application so it properly supports multiple users. When it is not possible to modify the application, an application script may be used to perform the pre-launch configuration and post-shutdown cleanup that is required to allow the application to run in a multi-user environment.

The process for creating and deploying an application script is as follows:

1. Write a batch file that:
   - Performs the tasks necessary to prepare the application environment for a user.
   - Launches the application.
   - Performs any cleanup tasks required after the application shuts down. The batch file should end with an EXIT command. Otherwise, the CMD.EXE process will not shut down.

2. Publish the application script
   a. Open the Admin Console.
   b. Click Tools | Applications | Add.
   c. Type the path to CMD.EXE in the **Application Path** field.
   d. In the **Command Line Options** field, specify "/K filename", where filename is the full path of the batch file to be run.
   e. Type the application display name and specify an icon.
   f. Click **OK**.

3. Test the application script
   a. Launch one of the GO-Global clients and connect to the GO-Global Host.
   b. Double-click the icon for the application script. The user interface of the application should appear on the client display, and the application should be running in the environment configured by the application script.

When an application script is launched using GO-Global, the CMD.EXE window is displayed only briefly. As such, the application script cannot contain any prompts for user input.

Mix Windows Support

Mix Windows support allows the windows of applications running locally on the client computer to be interleaved with the windows of applications running in a GO-Global session. When users activate the window of an application running in a GO-Global session, *only the activated window will come to the foreground*. The z-order of windows belonging to other applications running locally and in the GO-Global session will be unaffected.

This feature is supported only on Windows clients running in loose windows mode. It is enabled by default, but can be disabled by changing the **MixWindows** property in the HostProperties.xml file to false.

To disable Mix Windows Support

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\HostProperties.xml in a text editor.
3. Find the **MixWindows** property and change its associated value to **false**.
4. Save HostProperties.xml.
5. Start the **Application Publishing Service**.

Mix Windows support can also be disabled by adding **-mixwindows 0** to the command line.

For example:
./ AppController -h 196.125.101.222 -hp 443 **-mixwindows 0**

Publishing Applications to Users and Groups

Applications published using the GO-Global Admin Console are published to all users. The Admin Console does not support publishing applications to specific users or groups, but administrators can publish applications to users and groups by adding and modifying GO-Global-specific registry keys.

GO-Global stores the details of published applications in the registry. Applications that are listed under the HKEY_LOCAL_MACHINE\Software\GraphOn\GO-Global\AppServer\InstalledApps registry key are published to all users. Conversely, applications that are listed under the HKEY_CURRENT_USER\Software\GraphOn\GO-Global\AppServer\InstalledApps registry key are published to only the signed-in user. Administrators can set the values under the HKEY_CURRENT_USER\...\InstalledApps registry key and thereby publish and unpublish applications to specific users and groups.

This can be done in many different ways, including via:

- Logon scripts based on user or group or other condition
- Registry-based Group Policies
- Third-party RMM management tools
- Microsoft tools such as SCCM or Intune

The general procedure to publish an application is:

1. Create a script or policy to create the registry values that define a published application in GO-Global.
2. Configure the script or policy to be applied for specific users and/or groups.

Similarly, the general procedure to unpublish an application is:

1. Create a script or policy to delete the registry key and values of a previously-published application.
2. Configure the script or policy to be applied to the users and/or groups to which the application was originally published.

Published Application Registry Values

To publish an application in GO-Global, create the following registry values for the application, where **APPNAME** is the name of the application as it will appear in the Program Window.

Name = "ExePath"
Type = "REG_SZ"
Data = Path to the executable
Hive = HKEY_CURRENT_USER
Path ="SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps**APPNAME**"

Name = "StartDirectory"
Type = "REG_SZ"
Data = Path to the start directory of executable
Hive = HKEY_CURRENT_USER
Path ="SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps**APPNAME**"

Name = "CmdLineOptions"
Type = "REG_SZ"
Data = Any command-line options (This can be empty.)
Hive = HKEY_CURRENT_USER
Path ="SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps**APPNAME**"

Optional Values

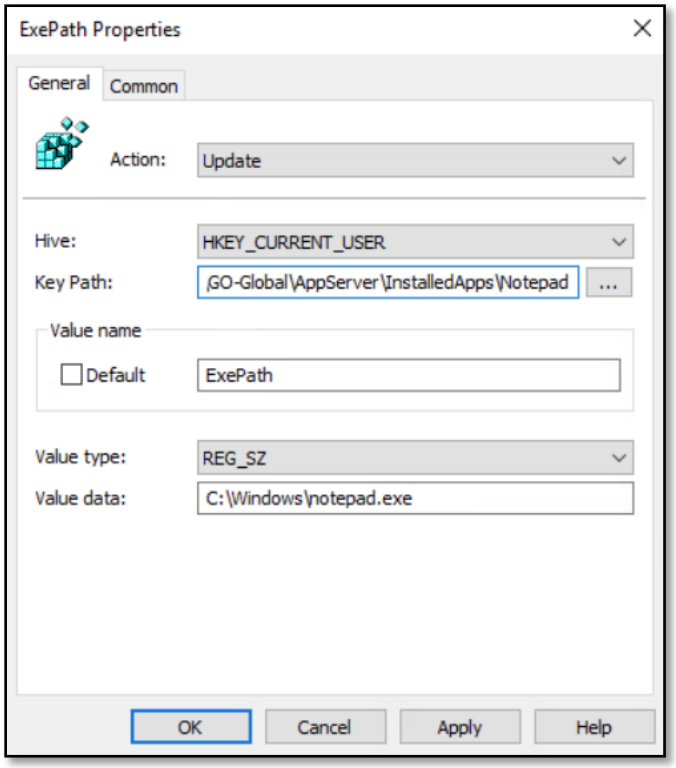
Name = "IconPath"
Type = "REG_SZ"
Data = The path to an alternate icon for the application.
Hive = HKEY_CURRENT_USER
Path ="SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps**APPNAME**"

Name = "StartState"
Type = "REG_DWORD"
Data = An integer specifying the application’s window start state (0=normal, 1=minimized, 2=maximized)
Hive = HKEY_CURRENT_USER
Path ="SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps**APPNAME**"

Publishing an Application Using Registry-Based Group Policy

In the example below, the steps describe how to publish Notepad using registry-based group policy, using **example.com** as the name of the domain.

1. Run the Group Policy Management app (type **gpmc.msc** in the Run box) on a domain controller.
2. Under Group Policy Management | Forest: **example.com** | Domains | **example.com**, right-click **Group Policy Objects** and select **New**. Type a name and click **OK**.
3. Right-click the new Group Policy Object and select **Edit**. (The Group Policy Management Editor window will open.)
4. Under User Configuration | Preferences | Windows Settings, right-click **Registry** and select New | Registry Item.
5. Set the Action to **Update**. Set Hive to **HKEY_CURRENT_USER**. Set the Key Path to SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps\Notepad. Replace *Notepad* with the name of the application being published. Set **Value name** to **ExePath** and uncheck the **Default** box. Set **Value type** to **REG_SZ** and set **Value data** to the application path. E.g., C:\Windows\notepad.exe. Click **OK**.



6. Repeat step 5 with the same settings except change Value Name to **StartDirectory** and Value Data to the application directory. E.g., C:\Windows\
7. Repeat step 5 with the same settings except change Value Name to **CmdLineOptions** and Value Data to any command-line options you choose. This can be left blank.
8. The three registry items from steps 5, 6, and 7 should be listed in the Registry box on the right. Close the Group Policy Management Editor window to return to the Group Policy Management window.
9. By default, **Authenticated Users** will be listed in the **Security Filtering** box within the new GPO under **Group Policy Objects**. Click **Authenticated Users** and select **Remove**. Then click **OK** to both dialogs.
10. **Add** any Active Directory users or security groups that require this policy.
11. Click Delegation | **Add** | Domain Computers | OK. Click **Advanced** and confirm *Domain Computers* only has the Read permissions.
12. To activate the new Group Policy Object, right-click the domain name under Group Policy Management | Forest: **example.com** | Domains and select **Link an Existing GPO...** Select the Group Policy Object you created and click **OK**.
13. To turn off the Group Policy Object, right-click the GPO from under **example.com** and select **Delete**. Then click **OK**. This unlinks the GPO; it can be linked again as described in step 10.
14. When a user or group specified in the **Security Filtering** box signs in to a computer in the **example.com** domain, the registry keys and values will be created under their user hive. These applications will be accessible via the Program Window.

Unpublishing an Application Using Registry-Based Group Policy

To unpublish an application, create a script or policy to delete the registry key and values of a previously-published application. Then configure the script or policy to be applied to the users and/or groups to which the application was originally published. The steps below use Notepad as the example application and **example.com** as the name of the domain.

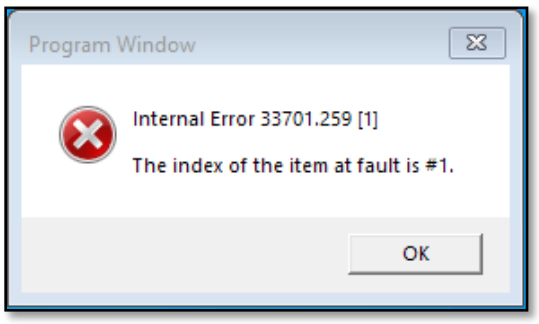
1. Run the Group Policy Management app (type **gpmc.msc** in the Run box) on a domain controller.
2. Disable the original GPO used to publish the application. Right-click the GPO (link) from under **example.com** and select **Delete**. Then click **OK**. This unlinks the GPO but does not delete it.
3. Under Group Policy Management | Forest: example.com | Domains | example.com, right-click **Group Policy Objects** and select **New**. Type a name and click **OK**.
4. Right-click the new Group Policy Object and select **Edit**. (The Group Policy Management Editor window will open.)

5. Under User Configuration | Preferences | Windows Settings, right-click **Registry** and select New | Registry Item.
6. Set the Action to **Delete**. Set Hive to **HKEY_CURRENT_USER**. Set the Key Path to SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps\Notepad. Replace *Notepad* with the name of the published application to be deleted. Leave the Value name and Value data fields blank. Click **OK**. Close the Group Policy Management Editor window to return to the Group Policy Management window.
7. By default, Authenticated Users will be listed in the Security Filtering box within the new GPO under Group Policy Objects. Click **Authenticated users** and select **Remove**. Then click **OK** to both dialogs.
8. **Add** any Active Directory users or security groups you want this policy to apply to.
9. Click Delegation | **Add** | Domain Computers | OK. Click **Advanced** and confirm *Domain Computers* has only the Read permission.
10. To activate the new Group Policy Object, right-click the domain name under Group Policy Management | Forest: example.com | Domains and select **Link an Existing GPO...** Select the Group Policy Object you just created and click **OK**.
11. To turn off the Group Policy Object, right-click the GPO from under example.com and select **Delete**. Then click **OK**. This unlinks the GPO; it can be linked again as described in step 7.
12. When a user or group specified in the Security Filtering box signs in to a computer in the example.com domain, the registry keys and values will be removed under their user hive.

Testing and Troubleshooting

After publishing an application, test the changes by signing in to the GO-Global Host using an affected user account. Verify that the applications appear in the Program Window as expected.

If there is an error in the specification of a published application, an error message such as the following may be displayed and prevent you from running any applications:



To resolve an issue such as this, do one of the following:

1. Review the changes you made and identify the incorrect setting.
2. Correct the setting in your policy or script.
3. Delete the incorrect registry values under HKCU\SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps\. Optionally, delete all subkeys and values under HKCU\SOFTWARE\GraphOn\GO-Global\AppServer\InstalledApps\. If roaming profiles are used, delete the values from both the local session host copy and the central copy of the user's registry.
4. Sign in to the GO-Global Host again and verify that the issue is resolved.

Advanced Session Process Configuration

This section covers some of the advanced configuration options that can be set for processes running within GO-Global sessions. These settings can be applied to specific executable (.exe) applications or as default settings applied to applications without specific configurations. Care should be taken when making any changes discussed in this section. An incorrect configuration can affect the startup of a process, make a process incompatible with GO-Global, or have fatal consequences during suspend/resume operations.

Most applications that run within a GO-Global session will have GO-Global libraries loaded within them to perform redirection in order to obtain desired behavior. There are two levels of redirection that these libraries can initialize.

The first level configures application and system modules to behave in a particular way. Most applications will need one or more level one settings enabled. Level one settings include Client Time Zone, Client Printing, and altered Windows API behavior.
The second level creates a communications channel between the application and client for duplex transmission of session related information. For the highest level of application compatibility with GO-Global, level two settings should be enabled in as few applications as possible. Level two settings include Client Sound and Client Serial and Parallel Ports.

The different configuration settings employed by the GO-Global libraries that redirect session processes are controlled by hexadecimal bit values within the registry. The desired bit values are logically ORed together to create a QWORD registry value. Here is the documented list of process redirector bits and a description of what they configure.

0x0000000000000001* - Prohibit a process from running within a session.

0x0000000000000002 - Disable the loading of GO-Global libraries. All redirection will be disabled. The time required to perform the redirection operations is generally a small percentage of the time required to launch typical Windows applications, but it can be a large percentage of the time required to launch and run simple console applications. Some console applications do not require redirection and performing these tasks can significantly extend the time required to execute logon scripts. Including this bit allows administrators to bypass redirection of a process. Applications execute faster since the

GO-Global libraries are not loaded and initialized. This bit can also be used for applications that, for one reason or another, are incompatible with some or all of the GO-Global redirection settings.

0x0000000000000004 - Disable Client Time Zone. This bit can be used for applications that, for one reason or another, are incompatible with the GO-Global Client Time Zone redirection settings.

0x0000000000000008 - Disable Client Printing. This bit can be used for applications that, for one reason or another, are incompatible with the GO-Global Client Printing redirection settings.

0x0000000000000040* - Enable the Windows ProcessIdToSessionId() API to return the GO-Global session ID.

0x0000000000000200 - Disable Client Sound. This bit can be used for applications that, for one reason or another, are incompatible with the GO-Global Client Sound redirection settings.

0x0000000000000400 - Disable client Serial and Parallel Ports. This bit can be used for applications that, for one reason or another, are incompatible with the GO-Global Client Serial and Parallel Ports redirection settings.

0x0000000000000800* - Enable the Windows GetComputerName() API to return the client computer name. See also: **Obtaining the Name of the Client Computer**. Disable the updating of the client environment variables (CLIENTCOMPUTERNAME and CLIENTCOMPUTERIPADDRESS) when a client reconnects to a suspended session.

0x0000000000001000* - Disable, for optimization purposes, some of the normal processing performed when Explorer.exe is launched. This bit prevents Explorer.exe from launching processes listed under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, RunOnce and RunOnceEx registry keys. This reduces the system resources needed to run Explorer in a session.

0x0000000080000000* - Enable application produced with Delphi to use the Client Serial and Parallel Ports feature. Applications built with Delphi do not properly process all return values from the Windows GetOverlappedResult() API. This bit prevents the returning of WAIT_TIMEOUT and instead returns WAIT_OBJECT_0.

0x0000000800000000* - Enable the NtQuerySystemInformation function to return the GO-Global session ID. This option may be required for .NET applications that make use of the Windows Session ID.

0x0000040000000000 - Make specific named pipes that the process creates or accesses session-private.

* Indicates advanced options that should only be used if instructed to by your support contact.

All the unlisted bits are purposely undocumented and reserved for internal GraphOn use only. Do not alter any registry values that contain any unlisted bits and do not apply any unlisted bits to any Registry values you add. GO-Global Host operation will be compromised if this is done.

These bits can be combined to customize the redirector settings of specific applications or to change the default settings used by applications that do not have a Registry entry. In either case, always include the default value bits set by the initial install of GO-Global, unless instructed otherwise by a support engineer.

To add custom redirector settings for a specific application

1. Click Start | Run.
2. Type Regedit.
3. Browse to the registry key: HKEY_LOCAL_MACHINE\GraphOn\GO-Global\Loader\Processes.
4. Click Edit | New | QWORD value.
5. Type the name of the application's executable file. (For example, Beeps.exe.) The application's name can be specified as either a fully qualified path or as the file's base name and extension.
6. Select the new registry value.
7. Click Edit | Modify.
8. Verify that the Base selection is **Hexadecimal**.
9. Type the combined bits in the **Value data** edit box.
10. Click **OK**.

To make a named pipe session-private

1. Add a custom redirector setting for each process that uses the named pipe that includes the **0x0000040000000000** bit.
2. Create a **DWORD** registry value under the KEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\System\Namedpipes registry key that identifies the named pipes that should be made session-private.
3. Set the name of the registry value equal to the string that will be compared to the name of the named pipes, and set the registry value to one of the following:
   - 1 - Make a named pipe session-private when the name of the named pipe matches the name of the registry value.
   - 2 - Make a named pipe session-private when the beginning of the name of the named pipe matches the name of the registry value.
   - 4 - Make a named pipe session-private when any part of the name of the named pipe matches the name of the registry value.

Comparison types 1 and 2 must be in the form of \\.\pipe\pipename and are made with a case-insensitive test. Comparison type 4 is case-sensitive.

To change the default redirection settings

1. Click Start | Run
2. Type Regedit.
3. Browse to the registry key: HKEY_LOCAL_MACHINE\GraphOn\GO-Global\Loader\Processes.
4. Select the existing **DefaultLoaderOptions** registry value.
5. Click Edit | Modify.
6. Verify that the Base selection is **Hexadecimal**.
7. Type the new setting in the **Value data** edit box.
8. Click **OK**.

Example Configuration

A GO-Global host has the following applications installed and registered in the Admin Console.

- DataDownloader.exe
- DataProcessor.exe
- DataViewer.exe

The **DataDownloader.exe** executable is a Windows application that reads data from a serial device and saves it to a file. Client Sound is needed for error conditions alerts that can be signaled while data is being downloaded. Client Files Access will be used to store the data file on the client system. The Windows GetComputerName() API must be redirected so that the client computer name can be used to indicate the source of the data within the data file.

Because the serial device that contains the data is connected to the client computer, Client Serial and Parallel Ports will need to be enabled. Because this is the only process that will access Client Serial and Parallel Ports on this system, a registry entry specifically for DataDownloader.exe has been added. This minimizes the risks and overhead associated with this level two redirector setting by disabling Client Serial and Parallel Ports in all other applications.

The settings for this application are calculated as follows:

0x0000000000000100 - These are the bits originally set in DefaultLoaderOptions.
0x0000000000000800 - This is the bit that enables the Windows GetComputerName() API redirection.
0x0000000000000900 – This is the hexadecimal QWORD to be set in the DataDownloader.exe registry value.

The DataProcessor.exe executable is a console application that needs Client File Access to read in the serial data file from the client and write out the processed data file to the client. It will also use Client Time Zone to properly process the times recorded in the serial data file. All other settings will be disabled to minimize the risks and overhead associated with redirector settings.

The settings for this application are calculated as follows:
0x0000000000000100 - These are the bits originally set in DefaultLoaderOptions.
0x0000000000000008 - This is the bit that disables Client Printing.
0x0000000000000200 - This is the bit that disables Client Sound.
0x0000000000000400 - This is the bit that disables Client Serial and Parallel Ports.
0x0000000000000708 – This is the hexadecimal QWORD to be set in the DataProcessor.exe registry value.

The **DataViewer.exe** executable is a Windows application that displays the data so that it can be analyzed. It needs Client File Access to read in the processed data file from the client. It needs Client Sound so that application sounds can be heard. It needs Client Printing so that the analyzed data can be printed on paper. These are some of the settings needed by most applications, so the **DefaultLoaderOptions** registry value is used for the calculation below.

The default setting will be changed to disable the Client Serial and Parallel Ports. This can be done because the only application that uses Client Serial and Parallel Ports, DataDownloader.exe, has its own registry setting that specifically enables it.
0x0000000000000100 - These are the bits originally set in DefaultLoaderOptions.
0x0000000000000400 - This is the bit that disables Client Serial and Parallel Ports.
0x0000000000000500 – This is the hexadecimal QWORD to be set in the DefaultLoaderOptions registry value.

This example demonstrates how a combination of application specific and the default settings can be used to minimize the risk of application incompatibilities and allow an optimal environment to run in.

Reducing Session Start Time by Disabling User Profile Initialization

The first time a user connects to a system, GO-Global runs **explorer.exe** (Windows File Explorer) in the session to initialize the user's user profile. This takes time and delays the startup of the user's application. This initialization only occurs the first time a user connects to a GO-Global Host, but in environments with a large number of load-balanced hosts, users can experience these delays nearly every time they connect.

If this initialization is not required, administrators can disable it by setting the value of the **InitializeProfileWithExplorer** property in HostProperties.xml to 0 on Application Hosts, as follows:

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\HostProperties.xml in a text editor, such as WordPad.
3. Locate the **InitializeProfileWithExplorer** property.
4. Set the value of **InitializeProfileWithExplorer** to 0.
5. Save the file.
6. Start the **Application Publishing Service**.

Running the Windows Desktop in Background of GO-Global Sessions

Some Windows applications use features and services that are provided by the Windows desktop (explorer.exe). Most applications run without the desktop, but some fail to start or run properly when the desktop is not running in the same session as the application. By default, the desktop does not run in GO-Global sessions. If an application fails to start or work properly in a GO-Global session, it may have a dependency on the desktop.

To register the Windows desktop (explorer.exe) to run in GO-Global sessions

1. From the Registry Editor, expand the HKEY_LOCAL_MACHINE key.
2. Expand \SOFTWARE\GraphOn\GO-Global\System\Run\LocalMachine.
3. Create a DWORD value and name it explorer.exe.
4. Set the value to 0.

With this configuration, the desktop will run in GO-Global sessions but will not be visible.

Registering the Windows desktop to run in the background of a GO-Global session adds significant overhead. Sessions will take longer to start and will consume more memory. Additional overhead can also result from other processes that are registered to run when the desktop starts up. Care should be taken to ensure that unnecessary processes are not registered in users' Startup folders or under the various Run commands in the Registry (e.g., HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run).

Explorer.exe will run in the session the first time that a user signs on to a host. This is done to fully initialize the user profile. Explorer.exe will not run in subsequent sessions started by the same user on the same host, unless configured to do so as described above.

Registering System Processes

The GO-Global architecture allows multiple processes to run within a single session. A minimum of one process must be running at all times. If all processes terminate, the GO-Global session is closed, all resources are de-allocated, and the client connection is broken.

During the course of normal program execution, most applications will create child processes to perform external operations. Some of these applications, Windows Help for example, provide their own user interface and are closed by the user when no longer needed. Others are helper processes that present no user interface but perform a fixed operation before exiting on their own. Applications also have the option of controlling the child processes they create and terminating them before they exit.

A problem arises in rare cases when a process has no user interface, does not exit on its own, and its parent process does not terminate it directly. Under a default configuration, these processes will create a hung GO-Global session when all other processes exit. The remaining process keeps the session active but the client has no user interface to close the session completely.

To resolve this issue, the GO-Global Host supports the registration of certain executables to run as system processes. The GO-Global session will close if the only processes remaining in the session are system processes.

For most applications, the default configuration is sufficient. For special cases where a process is created without the means to be terminated, registering the executable of the lingering process will allow GO-Global sessions to close properly.

WARNING: The following information involves opening and manipulating the Windows Registry. Carrying out operations other than those described here may cause configuration errors, possibly rendering your system unusable. Please use extreme caution any time you work in the Registry.

To register an executable file as one that Creates System Processes

1. Run the Registry Editor (regedit.exe).
2. Browse to HKEY_LOCAL_MACHINE\Software\GraphOn\GO-Global\System\Processes.
3. Create a **DWORD** entry with the name of the executable to be registered (e.g., AGENTSVR.EXE).
4. Set the value of the new entry to 1 if the full path to the executable is specified, or 2 if only the base name is specified. (Including the full path allows different versions of the same executable image to be run differently.)
5. Close the Registry Editor.

This setting affects all current GO-Global sessions in addition to any future sessions. This does not include any sessions already in the “hung” state. Such sessions should be terminated from the Admin Console.

Proxy Tunneling

Proxy tunneling via the **HTTP CONNECT** method allows a user who accesses the internet via a proxy server to connect to GO-Global Hosts on the internet when the following conditions are met:

- The user runs the GO-Global Client on a Windows computer;
- The address and port of the proxy server are stored under the client computer’s Internet Options; and
- The proxy server is configured to allow HTTP CONNECT method tunnels to the port on which the GO-Global Host is configured to accept RapidX Protocol (RXP) connections.

Proxy Tunneling via the HTTP CONNECT Method

When users on Windows computers are unable to establish a direct connection to a GO-Global Host, and when the client computer is configured through its Internet Options to use a proxy server, GO-Global attempts to establish an HTTP CONNECT method tunnel to the GO-Global Host.

Specifically, the client:

1. Connects to the proxy server using the address and port specified in the client computer's **Internet Options**.
2. Sends a CONNECT request to the proxy server: i.e., CONNECT *address:port* HTTP/1.0, where *address* and *port* are respectively the IP address of the GO-Global Host and the port on which the server accepts RXP connections (e.g., 491 by default).
3. Reads the reply from the proxy server.
4. Responds to the proxy server's reply as follows:
    a. If Basic authentication is required, GO-Global prompts users for their user name and password and then repeats Step 2, this time providing the user's credentials.
    b. If the request failed, GO-Global displays the following message: "Failed to connect to serverAddress via the proxy server at proxyAddress : [reason for failure].
    c. If the request succeeded, GO-Global initializes the RXP connection and starts the session.

To allow HTTP CONNECT method tunnels using port 443

1. Configure the GO-Global Host to accept connections on port 443.
2. Specify port 443 in the GO-Global hyperlink.
3. If necessary, configure the proxy server to allow connections to the GO-Global Host on ports 80 (HTTP) and 443 (HTTPS).

Once you have configured the GO-Global Host and the GO-Global hyperlinks, users that meet the three requirements above will be able to connect to the host. Users running GO-Global from a shortcut will need to append the -hp argument followed by 443 to the shortcut. For example, "...\gg-client.exe" -h server -hp 443. Otherwise these users will be unable to sign in to GO-Global.

GO-Global clients are unable to connect to GO-Global Hosts via proxy servers that are configured to verify that the traffic on port 443 is HTTPS.

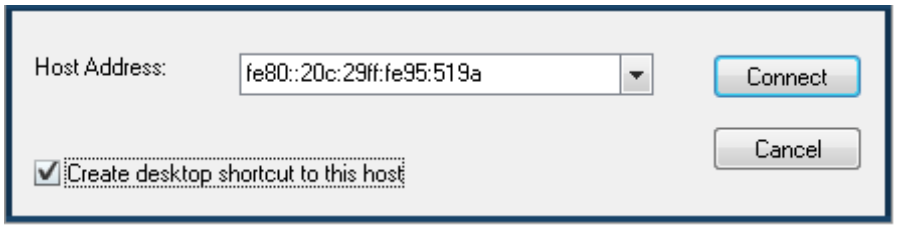
In a proxy server configuration, GO-Global only supports Basic authentication.

Support for Internet Protocol Version 6

GO-Global supports Internet Protocol version 6 (IPv6), the successor to IPv4, the dominant Internet layer protocol. IPv6 has a much larger address space than IPv4, and allows flexibility in allocating addresses and routing traffic.

GO-Global supports the following:

- GO-Global Hosts accepts connections from IPv4 and IPv6 clients.
- GO-Global Relay Load Balancers accept connections from IPv4 and IPv6 Dependent Hosts.
- Administrators can specify a Relay Load Balancer in the Admin Console using a hostname, an IPv4 address, or an IPv6 address.
- Users can connect to a GO-Global Host using its hostname, its IPv4 address, or its IPv6 address.



GO-Global healthCheck Request

Administrators can test the health of a GO-Global Host by sending a healthCheck request to the Application Publishing Service (APS).

To perform a healthCheck, use the following URL:

http[s]://server.domain.com[:port]/api/v1/healthCheck

For example,
http://winhost.example.com:491/api/v1/healthCheck

The healthCheck request can be used by third-party load balancers and monitoring tools to check the health of the Application Publishing Service. When the APS is running and responding to requests, the healthCheck request returns an HTTP 200 success status response code.

When the request is successful, the response includes a set of key-value pairs with information about the state of the GO-Global Host as follows:

```
{
  "time": 1715952273,
  "numSessions": 23,
  "cpuUsage": 57,
  "memoryLoad": 66,
  "totalPhys": 4293926912,
  "availPhys": 1418907648,
  "totalVirt": 140737488224256,
  "availVirt": 140732891750400
}
```

This information is generally not needed by load balancers and monitoring tools. It is provided in the response so that customers can use the request to programmatically retrieve information about the resource usage on a GO-Global Host.

The following table describes these key-value pairs:

healthCheck Key	Value Description
time	Current timestamp
numSessions	Number of sessions running on the host
cpuUsage	An (unreliable instant) measure of current CPU usage
memoryLoad	% of memory usage on the system
totalPhys	Amount of physical memory in the system
totalVirt	Amount of virtual memory in the system
availPhys	Amount of unused physical memory in the system
availVirt	Amount of unused virtual memory in the system

The healthCheck request also supports an optional **startSession** parameter to test the ability of the GO-Global Host to start a session.

To use this parameter, append **?startSession** to the healthCheck URL, as follows:

http[s]://server.domain.com[:port]/api/v1/healthCheck?startSession

For example,
http://winhost.example.com:491/api/v1/healthCheck?startSession

When this parameter is specified, the APS attempts to start a session. If it is successful, the request returns an HTTP 200 response status code. If it fails to start a session because of a resource limitation, the request returns a 503 status code. In this case, the status value contains a human-readable message indicating the resource that was not available. For example,

Resource PAGED_POOL_BYTES Not Available
Resource SYSTEM_PAGE_TABLES Not Available
Resource MEMORY_PHYSICAL Not Available
Resource MEMORY_VIRTUAL Not Available
Resource CPU Not Available

When the APS fails to start a session for some other reason, it returns a 500 response status code.

The APS limits the frequency of healthCheck session start attempts to prevent requests from overloading a GO-Global Host. When it receives a healthCheck request that includes the **startSession** parameter, it checks to see when it last attempted to start a session in response to a healthCheck request. If it was less than the number of seconds specified by the value of the **HealthCheckSessionStartInterval** property in HostProperties.xml, the APS does not attempt to start a session and returns the result of the last session start attempt as follows:


```
{
  "time": 1715952273,
  "lastHealthCheckSessionStartAttempt": 1715952258,
  "lastHealthCheckSessionStartStatusCode": 200,
  "lastHealthCheckSessionStartStatus": "OK",
  "numSessions": 23,
  "cpuUsage": 57,
  "memoryLoad": 66,
  "totalPhys": 4293926912,
  "availPhys": 1418907648,
  "totalVirt": 140737488224256,
  "availVirt": 140732891750400
}
```

The following table describes the key-value pairs that are returned in the response to the healthCheck request when the **startSession** parameter is included:

healthCheck startSession Key	Value Description
time	Current timestamp
lastHealthCheckSessionStartAttempt	Timestamp of the last session start
lastHealthCheckSessionStartStatusCode	Status of the last session start attempt (200 = OK, 500 = Unknown Error, 503 = Resource Unavailable)
lastHealthCheckSessionStartStatus	Human-readable status of the last session start ("OK", "Internal Server Error", "Resource PAGED_POOL_BYTES Not Available", "Resource SYSTEM_PAGE_TABLES Not Available", "Resource MEMORY_PHYSICAL Not Available", "Resource MEMORY_VIRTUAL Not Available", "Resource CPU Not Available")
numSessions	Number of sessions running on the host
cpuUsage	An (unreliable instant) measure of current CPU usage
memoryLoad	% of memory usage on the system
totalPhys	Amount of physical memory in the system
totalVirt	Amount of virtual memory in the system
availPhys	Amount of unused physical memory in the system
availVirt	Amount of unused virtual memory in the system

GO-Global's healthCheck feature is limited to IP addresses specified in the **ApiWhitelist** property in **HostProperties.xml**. These addresses are specified in Classless Inter-Domain Routing (CIDR) notation. For example, 192.168.0.0/24 specifies that IP addresses 192.168.0.1 to 192.168.0.255 would be allowed access.

If the connecting IP address does not match the specified **ApiWhitelist** value, access is denied with an HTTP 403 (Forbidden) error. The default whitelist is an empty string, which means no access is allowed.

The address that needs to be whitelisted is the source IP address of the system making the healthCheck API call. For monitoring and alerting purposes, this will be the IP address of your monitoring system that periodically checks the health status of GO-Global Hosts to ensure service availability.

In farm deployments, the third-party load balancer can use GO-Global's healthCheck feature to validate farm host availability. When configuring the ApiWhitelist, specify the IP address that the load balancer uses for its backend healthCheck probes. This IP address varies by load balancer. For example, an Azure Load Balancer uses a dedicated health probe IP address of 168.63.129.16.

To add IP Addresses to the ApiWhitelist property

1. Locate the file **HostProperties.xml** in the following directory: C:\ProgramData\GraphOn\GO-Global.
2. Open **HostProperties.xml** in a text editor, such as WordPad.
3. Locate the **ApiWhitelist** property ID. For example:

   <property id="ApiWhitelist" group="Connections" type="STRING">
   <value></value>
   </property>
4. Add a space-separated list of approved CIDR-form addresses to the value. For example, the following property setting allows the loopback IPs (127.x.x.x) and the local network (192.168.1.x) to access the healthCheck service:

   <property id="ApiWhitelist" group="Connections" type="STRING">
   <value>127.0.0.0/8 192.168.1.0/24</value>
   </property>
5. Stop and start the **Application Publishing Service**.

The whitelist can be configured to allow all accesses by specifying a CIDR value of "0.0.0.0/0".

For example:

<property id="ApiWhitelist" group="Connections" type="STRING">
<value>0.0.0.0/0</value>
</property>

Application Publishing Service log files only display healthChecks when the Log output level is set to 6.

Performance auto-tuning is used in situations when an application is generating a large amount of graphical data or when a client system has limited processing speed. When Performance auto-tuning is enabled, the client machine reports the rate at which it is processing the data the host is sending. The host uses this information to reduce the total amount of data it sends by eliminating any graphical information that the client system is unable to keep up with, such as animations with a high frame rate, or by choosing to send an image of an application's contents rather than primitive graphical operations.

Performance auto-tuning allows any client to run even the most graphically intense applications. Performance auto-tuning is disabled by default.

To enable Performance Auto-Tuning for all clients connecting to a host

1. Locate the file **HostProperties.xml** in the following directory: C:\ProgramData\GraphOn\GO-Global.
2. Open **HostProperties.xml** in WordPad.
3. Change the value of **ClientProcessingBatch** from 0 to 1.
4. Change the value or **ClientProcessingThrottleV2** from 0 to 1.
5. Open Regedit and create a DWORD registry value \HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\AppServer\ClientOffscreenSurfaces and set its value to 0.
6. Stop and start the **Application Publishing** Service.

Make sure to create a backup of **HostProperties.xml** before making any changes.

How Performance Auto-Tuning Works

When performance auto-tuning is disabled, the host updates the client's display by sending primitive drawing commands such as "draw rectangle," "draw line," and "draw text" to the client.

The alternative is for the host to wait and send an image with the final result of the drawing operations to the client. This approach is referred to as "screen scraping." In most cases, it is much more efficient to update the client display using primitive drawing commands, but there are times when it is more efficient to "screen scrape."

When performance auto-tuning is enabled, the host attempts to determine the most efficient means of updating the client display each time display data is sent from the host to the client. For example, if the host estimates that the bandwidth required to send an image of the modified area of the screen will be less than the bandwidth required to send all of the drawing commands that were used to modify the screen, the host will send the image instead of the drawing commands. In other words, it will "screen scrape."

Enabling performance auto-tuning is recommended for applications that display animations or video because it allows the host to skip frames and remain responsive to user input even when the application on the host is drawing a large number of

images. However, when this option is enabled, minor display anomalies can occur when parts of the screen are updated from the host's frame buffer (screen) and other parts are updated using drawing commands. Because of these anomalies, performance auto-tuning is disabled by default.

Silent Installation

GO-Global can be installed silently. In other words, installation is performed without user interaction except for the initial launch of the process.

To run a silent client install

1. Run cmd.exe as local administrator (Run as administrator).
2. Run the following command:
   AppController.exe /q

This adds the AppController shortcut to the Start menu:
Start | Programs | AppController.

To install AppController silently without a shortcut, run the following command:
AppController.exe /q CLIENT_SHORTCUT="No"

Extracting AppController MSIs

The **AppController.msi** or **AppController.AllUsers.msi** can be extracted from the respective AppController installer with the following steps:

1. Download the desired AppController.exe installer to a system that does not already have the client installed.
2. Run the AppController.exe to start the installation process.
3. At the beginning of the installation process, the MSI is extracted. The extracted MSI can be found in one of the following locations. (The {hex number} in the path will vary.)

   Single User:
   C:\Users\[username]\AppData\Local\Package Cache\{F3076184-F457-4700-98D9-319715546406}\client-user.msi

   All Users:
   C:\ProgramData\Package Cache\{4ef15330-a5b6-402f-a89b-0300c65bb2d1}\client-admin.msi

There may be more than one new {hex} folder created in the **Program Cache** directory, but only one will contain the MSI file.

To silently install the All Users AppController in a specific folder, run the following command: appcontroller.AllUsers.exe /q InstallFolder="X:\temp"

The GO-Global Host can also be installed silently. These instructions are the same when upgrading the GO-Global Host. A valid GO-Global license that is compatible with the version being installed must be copied to the Licensing directory before running the silent host upgrade.

To run a silent host install

1. Run cmd.exe as local administrator (Run as administrator).
2. Run the following command:
   gg-host.exe /q
3. The host will reboot automatically.
4. Copy the license file into the **Licensing** directory.
5. Restart the **GO-Global License Manager** service.

To run a silent host install without automatically restarting the system, run the following command:
gg-host.exe /q /norestart

To silently install the host in a specific folder, run the following command:
gg-host.exe /q InstallFolder="X:\Program Files\GraphOn"

Running a Silent Targeted Installation
The instructions above install the Host (MSI_HOST), Web (MSI_WEB), and Licensing (MSI_LICENSE), components of the GO-Global Host silently.

These components can be installed selectively on the command line by setting the property to 1 to install the component, and setting the property to 0 to prevent it from being installed.

In the following examples, the Host (MSI_HOST=1) and License (MSI_LICENSE=1) components will be installed silently. The Web (MSI_WEB=0) component will not be installed. In the second example, the components will install to a specific folder.

gg-host.exe /q MSI_HOST=1 MSI_LICENSE=1 MSI_WEB=0

gg-host.exe /q InstallFolder="E:\Program Files\GraphOn" MSI_HOST=1 MSI_LICENSE=1 MSI_WEB=0

This feature is only available for new installations for the GO-Global Host. It is not available when upgrading.

Automating the Configuration of GO-Global

GO-Global offers several ways to automate its configuration.

The GO-Global Host can be installed silently on Farm Managers and Application Hosts by running the installer with the following command line:

gg-host.exe /q

Applications can be published from the command line using the Admin Console's command-line interface. For more information, see the document, *Admin Console Command-Line Interface*, accessible via the Customer Portal.

GO-Global's settings can be configured by updating the values in its properties files, stored in the following locations:

- \ProgramData\GraphOn\GO-Global*HostProperties.xml*
- \ProgramData\GraphOn\GO-Global*DefaultWorkspaceProperties.xml*

The properties files can be replaced with files that are pre-configured with the desired settings as described in the Manually Copying Configuration Setting from one Host to Another section.

The address of the Farm Manager is stored in the following registry value:
HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\AppServer\RelayServer

On Farm Hosts, this value is set to the address of the Farm Manager. On Farm Managers, this value is set to the name or IP address of the Farm Manager itself.

The Support Request Wizard cannot be executed from the command line.

Log Files

The GO-Global Host creates log files in which it records information about its own performance and that of certain GO-Global processes. GraphOn Technical Support uses the data to diagnose and correct problems that may arise. This can be especially helpful for errors that are only reproducible on specific machines or with a specific application.

All log files, whether they pertain to the client or host machine, are located in the **Log** folder on the GO-Global Host. For example, C:\Program Files\GraphOn\GO-Global\Log. In the Log folder are four subfolders: **Backup**, **Codes**, **Clients**, and **Templates**. Be careful not to delete these folders. GO-Global messages are recorded within log files prefixed with *aps* and followed by the date and time the Application Publishing Service was started (Year-Month-Day-Hour-Minute-Second-Millisecond) and the process ID of the Application Publishing Service. (For example, *aps_2024-09-04_09-55-47-033_p9999.log*). The first log in a series will not include the milliseconds as part of the timestamp.

A new log file is created each time the Application Publishing Service is started. The log file with the latest date and time stamp contains messages for the current, or most recent instance of the Application Publishing Service.

Problems detected in the execution of GO-Global are described by entries in the log file. Each entry is uniquely identified by an item number along with a date and time stamp, and a description of the event or program error. GraphOn Support uses this information to locate a problem's source and to determine its resolution.

Entries in the log file may also include prefixes for locating messages associated with an individual user's session and applications. If the event occurred within the context of a given session, the name of the session will appear at the beginning of the message, for example, *SuzyG on Server1*. If the event occurred within the context of a connection to the Application Publishing Service—a connection either from a client or from an application, the name of the connected process will be included in the message prefix, for example, *pw (1244).* In this example, a problem occurred during the connection between the Program Window process and the Application Publishing Service*.* 1244 is the ID of the process in which the event took place. If the message prefix contains the connection name *aps*, the event occurred within the Application Publishing Service, but was not associated with a connection to another process.

Selecting a New Location for the Log Files

By default, log files are created and stored at %PROGRAMFILES%\GraphOn\GO-Global\Log. You can select a new location for the log files through the Admin Console's **Host Options** dialog.

To select a new location for the Log files

1. From the Admin Console, click Tools | Host Options.
2. Click **Log**.
3. Type the path to the new directory in the **Folder** edit box or browse to its location.

You cannot specify a path to a remote system for the log file location. For example, if you type a UNC path or a mapped network drive in the **Folder** edit box, the following message is displayed:

Please specify a usable Windows folder where log files may be written.

Move the **Log** folder and all its contents to the new location. Be sure to copy the *entire* Log folder, including all subfolders and files.

The Log Folder *must* be the same on *all* systems in a GO-Global cluster. For example, when a Farm Host connects to a Farm Manager, the path to the Log folder of the Farm Host will be set to the path to the Log folder on the Farm Manager (e.g., %PROGRAMFILES%\GraphOn\GO-Global\Log). If that path does not exist on the Farm Host, the Application Publishing Service will fail to start on the Farm Host.

Setting the Output Level

GO-Global offers six log output levels, as follows:

0: No output
1: Errors
2: Errors and Events
3: Errors, Events, and Warnings
4: Errors, Events, Warnings, and Diagnostic Messages
5, 6: Errors, Events, Warnings, Diagnostic Messages, and Trace Messages

To set the output level

1. From the Admin Console, click Tools | Host Options.
2. Click **Log**.
3. Type one of the above numeric values in the **Output level** box.
4. Click **OK**.

Setting the log output value to 5 or 6 will cause the host to generate very large log files and may adversely affect performance and scalability. These output levels should only be used in a controlled environment—preferably when no clients are accessing the GO-Global Host.

The default value for the Output level is 4.

Maintaining Log Files

GO-Global creates a new log file in the **Log** folder every time the Application Publishing Service starts. Over time these files can accumulate and consume a significant amount of disk space. To help manage these files, GO-Global lets you delete or backup log files and set file size or age limits.

To delete log files

1. From the Admin Console, click Tools | Host Options.
2. Click **Log**.
3. Under **Maintenance**, select **Delete**.
4. Specify how old (in days) log files can become before being deleted.
5. Specify at what size (in megabytes) log files are to be deleted.
6. Click **OK**.
7. Restart the **Application Publishing Service**.

To backup log files

1. From the Admin Console, click Tools | Host Options.
2. Click **Log**.
3. Under **Maintenance**, select Back up.
4. Specify how old (in days) log files can become before being moved to the Backup subdirectory of the Log folder.
5. Specify at what size (in megabytes) log files are to be moved to the Backup subdirectory of the Log folder.
6. Click **OK**.
7. Restart the **Application Publishing Service**.

Once every half hour, and each time it is started, the Application Publishing Service searches the **Log folder** for files that have reached the specified age or size limit. It then either deletes the files or moves them to the **Backup** subdirectory of the Log folder. If while sweeping the log files, the Application Publishing Service finds that the age or size limit has been met in the current log file, it closes the file and installs a newly created file in its place.

By default, log files are backed up after 7 days or when the file size has reached 20 MB.

Changing Log Files to Text File Format

Log files are created as .html files by default. To change the file format to text file (.log) format, set the **LogTextFormat** host property to **true** in HostProperties.xml.

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\HostProperties.xml in a text editor, such as WordPad.
3. Locate the **LogTextFormat** property.
4. Set the value of **LogTextFormat** to **true**, as follows:

   ```
   <property id="LogTextFormat" group="Log" type="BOOL">
   <value>true</value>
   </property>
   ```
5. Save the file.
6. Restart the **Application Publishing Service**.

GO-Global messages are recorded within log files prefixed with *aps* and followed by the date and time the Application Publishing Service was started (Year-Month-Day-Hour-Minute-Second-Millisecond) and the process ID of the Application Publishing Service. (For example, aps_2024-09-04_09-55-47-033_p9999.log). The first log in a series will not include the milliseconds as part of the timestamp.

Client Log Files

The GO-Global client records messages in a log file on the client device when the client is not connected to a host. In addition, after a user signs in to a host, the client synchronizes its log files with the host. Specifically, GO-Global determines if there are any log files on the client from previous sessions with the host that have not already been copied to the host. If there are, GO-Global copies the missing client log files to the host.

These changes make it easier for system administrators to determine the cause of connection problems. For example, if a user reports that his or her connection to the host is frequently getting dropped, the system administrator can check the host and client log files to determine the cause. In this scenario, the client log files from the user's previous sessions will generally be available on the host, and the administrator will not need to manually retrieve the client log files from the client device. Generally, administrators will only need to retrieve log files from a user's computer in cases where the user is unable to connect to a host at all.

The names of client log files include the name of the user, the address of the host, and the date and time that the client was started. Client log files are stored on the host in the %PROGRAMFILES%\GraphOn\AppController\Log\Clients directory.

Client logs are stored on the client device in the following locations:

- Windows: %APPDATA%\GraphOn\Logs
- Linux: %HOME%/.AppController/Logs
- macOS: %HOME%/.AppController/Logs
- iOS/Android: Not accessible from the client

On Linux and macOS, the .AppController directory is hidden.
When a log file is copied from the client to the host, the client's copy of the log file is moved to the **%APPDATA%\GraphOn\Logs\Old** directory on the client computer.

Log files are stored on the client for the number of days specified in the HKEY_CURRENT_USER\Software\GraphOn\AppController\Client\LogFileAgeLimit registry value. The default is 10 days.

Messages that the client outputs while it is connected to a host are recorded in the host's (APS_...) log file. The GO-Global client only records messages in the client log file when the client is not connected to a host.

Connection Monitoring

GO-Global monitors the latency and the input and output rates of connections to the host. When a new client connects to a host, the host tests the client's connection and records initial values for each of the metrics in the host's log file. Thereafter, the host monitors the connection for quality changes. If the quality of any of the metrics changes while the session is running, the host records the change in its log file.

The frequency of quality checks and the quality threshold values are specified in the **HostProperties.xml** file.

Connection Verification

Users with poor quality connections may get disconnected from hosts because AppController's connection verification (ping) requests time out. To work around this, administrators can configure GO-Global's connection verification interval and timeouts to be more forgiving via the **ConnectionVerificationInterval** and **ConnectionVerificationTimeout** properties in the HostProperties.xml file.

The default value of both properties is 10000 milliseconds (10 seconds). The value of the **ConnectionVerificationTimeout** must be less than or equal to the value of the **ConnectionVerificationInterval**. If ConnectionVerificationTimeout is set to 0 (zero), connection verification requests are disabled (i.e., the client will not ping the host).

To edit Connection Verification Interval and Timeout

1. Stop the **Application Publishing Service**.
2. Locate the file HostProperties.xml in the C:\ProgramData\GraphOn\GO-Global directory.
3. Open HostProperties.xml in WordPad and locate the **ConnectionVerificationInterval** and **ConnectionVerificationTimeout** properties.
4. Increase the timeout and interval values to something larger than the default 10000 milliseconds. For example, set **ConnectionVerificationInterval** and **ConnectionVerificationTimeout** to 30000.
5. Save the file.
6. Restart the **Application Publishing Service**.

Support Request Wizard

The GO-Global Host includes a Support Request Wizard that gathers log files and information about the host that can be sent to technical support.

Run the Support Request Wizard from the Admin Console by clicking Help | Support Request Wizard or via the Start menu by clicking Programs | GraphOn GO-Global | Support Request Wizard. A third option is to launch the **srw.exe** directly from C:\Program Files\GraphOn\GO-Global\Support.

The wizard prompts the administrator for a description of the problem, a time frame for when the problem happened, and the user or users that were affected. If the issue is associated with an existing support case, administrators can enter the Case Number. By default, the zipped report is placed on the user profile's desktop, but administrators can select an alternative destination via the wizard.

Administrators can also reply to an existing support email (support@graphon.com) with the zipped file attached.

High Resolution Client Devices

When AppController is run on a high resolution client device that is configured to scale the display, AppController attempts to scale the GO-Global session's graphical output so the text and controls of applications running in the session are the same size as the text and controls of applications that are running locally on the client device. For example, if the client computer is configured to scale the display by 200%, AppController scales the graphics commands it receives from the host (e.g., text characters and images) by 200%.

When the client stretches graphic objects such as images and text, their quality is not as good as when the objects are drawn at 100%. The edges of text characters, for example, are not as smooth when they are stretched; characters may appear blocky or blurry. On high resolution screens (where display scaling is most often enabled) these effects are typically not very noticeable. On low resolution screens, however, the effects can be quite noticeable, especially when the display scale factor is set to a non-integral value such as 125%.

If these effects are noticeable, GO-Global's scaling feature can be disabled as follows:

- When the client is run from a shortcut, add **-clientdpi 0** to the client's command-line
- When the client is run from a browser, add **&clientdpi=false** to the URL
- To disable the feature on the host for all users, change the value of the **ClientDPIScalingEnabled** property in the **HostProperties.xml** file on the host from "true" to "false"

When GO-Global's scaling feature is disabled, GO-Global will render the session using the scale factor specified for the user under the Control Panel's Display applet on the host. In this configuration, administrators can allow users to modify the DPI setting by publishing the Display applet to users.

To publish the Display applet to users

1. Sign in to the console on the host as an administrator.
2. Create a shortcut to the Display applet:
   a. Click Start | Control Panel.
   b. Right-click **Display**. A shortcut will be added to the Desktop.
   c. Drag the shortcut to a directory that all users can access (e.g., C:\Users\Public\Desktop).
3. Publish the shortcut to users:
   a. Run the Admin Console and click Applications | Add.
   b. Type "Display Settings"(or some other descriptive name) in the **Display Name** field.
   c. Enter the path to explorer.exe (e.g., C:\Windows\explorer.exe) in the **Executable Path** field.

d. In the **Command-Line Options** field, type the path to the shortcut created in step 2 (e.g., C:\Users\Public\Desktop\Display.lnk).
e. Click **OK**.

Setting the Program Window Close Option

By editing the **ProgramWindowCloseOption** key, administrators can determine how the Program Window closes when the user clicks the X button in the upper-right corner. By default, **ProgramWindowCloseOption** is set to 1. When the user clicks the X button, the **Sign out** option is executed, and the user is prompted to confirm the sign out. Users can still disconnect by clicking File | Disconnect.

To edit the ProgramWindowCloseOption key

1. Run the Registry Editor (regedit.exe).
2. Locate the **ProgramWindowCloseOption** key: [HKEY_LOCAL_MACHINE\Software\GraphOn\GO-Global\AppServer\ProgramWindowsCloseOption]
3. Set the value of the entry to one of the following:

0: Disconnect
If the Admin Console's **Disconnected sessions terminate** option is set to **Never** or **After x minutes**, the Program Window executes the File | Disconnect option when the user clicks the X button in the upper-right corner of the Program Window.

The user is presented with the following message:
Your session and its applications will continue to run on the host until you reconnect.

Otherwise, if the **Disconnected sessions terminate** option is set to **Immediately**, the Program Window executes the File | Sign out option, and the user is presented with the following message:
Your session and its applications will be closed. Are you sure you want to sign out?

1: Sign out
When **ProgramWindowCloseOption** is set to 1, the Program Window executes the File | Sign out option when the user clicks the X button, and the user is presented with the following message:
Your session and its applications will be closed. Are you sure you want to sign out?

2: Close
When **ProgramWindowCloseOption** is set to 2, the Program Window executes the File | Close option when the user clicks the x button. This closes the Program Window, but the user's applications continue to run on the host.

4. Close the Registry Editor.

Reconnecting to Sessions when the Network Connection is Dropped

Administrators can configure the GO-Global Host to only allow users to reconnect to their sessions when the network connection is dropped. First, set the **Disconnected sessions terminate** option to **Immediately** on the **Sessions Shutdown** tab of the **Host Options** dialog. Then set the value of the **SessionTimeoutBrokenConnection** property in the HostProperties.xml file to the number of minutes sessions should remain running on the host after the connection to the client is dropped.

For example, in the instructions below, sessions would be suspended for 10 minutes after a network disconnection.

1. Stop the **Application Publishing Service**.
2. Locate the file **HostProperties.xml** in the C:\ProgramData\GraphOn\GO-Global directory.
3. Open **HostProperties.xml** in WordPad and locate the **SessionTimeoutBrokenConnection** property.
4. Set the **SessionTimeoutBrokenConnection** property to **10.**
5. Save the file.
6. Restart the **Application Publishing Service**.

Dragging Full Windows

Administrators can configure the GO-Global Host to show either the contents or outline of a window when users drag a window by editing the **DragFullWindows** property in the HostProperties.xml file. Users can set this via the **–dfw** command-line option described in the Startup Parameters section. By default, the contents are shown when the window is moved or resized.

To edit the DragFullWindows key

1. Stop the **Application Publishing Service**.
2. Locate the file **HostProperties.xml** in the C:\ProgramData\GraphOn\GO-Global directory.
3. Open **HostProperties.xml** in WordPad and locate the **DragFullWindows** property.
4. Set the **DragFullWindows** property to one of the following:

   0: The host will turn off dragging windows contents and ignore the -dfw client command-line option.
   1: the host will turn on dragging windows contents and ignore the -dfw client command-line option.
   2: The host will follow what is specified on the client command-line which is set to drag windows contents by default. (DragFullWindows is set to 2 by default.)
5. Save the file.
6. Restart the **Application Publishing Service**.

Automatic Client Keyboard Support

The automatic client keyboard feature lets administrators configure GO-Global Hosts to automatically work with any client keyboard. Users can switch between keyboards on the fly using the local keyboard switching features of their client device, and the Input Method Editor (IME) of the client. It is not necessary to install keyboard layouts on the GO-Global Host or keyboard mapping files on GO-Global clients.

Automatic client keyboard is enabled by default, but can be disabled by editing the HostProperties.xml file.

To disable automatic client keyboard

1. Locate the file **HostProperties.xml** (e.g., C:\ProgramData\GraphOn\GO-Global)
2. Open **HostProperties.xml** in WordPad and locate the **ClientSideIME** property.
3. Set the **ClientSideIME** property to 0.
4. Save the file.

Configuring Support for Client Keyboards and/or IMEs

Windows uses input languages, keyboard layouts, Input Method Editors, and code pages to map keys on a keyboard to the characters on the display. When a key is pressed on the client's keyboard, GO-Global sends a key code to the host, which translates the key code into a Windows input message using the session's active keyboard layout. The GO-Global setup configures the host to support clients that use the same operating system, keyboard, and/or IME as the host. GO-Global supports clients with different operating systems and keyboards with keyboard mapping files.

When GO-Global's Automatic Client Keyboard support does not meet a customer's needs, the host's IME functionality might be required. The following section describes mechanisms and procedures to manage keyboards and IMEs in sessions on client computers that do not match the host system.

Installing Additional Keyboards and IMEs

Before clients can use keyboards and/or IMEs that are different from the host's, the files used to support them must be installed on the GO-Global Host. In most cases the layouts are copied during the installation of the operating system, but East Asian and right-to-left input languages are not.

To add keyboard layouts on a host running Windows Server 2016

1. From the Start menu, click **Control Panel**.
2. Click **Language**.
3. Select the desired language (and Regional variant, if applicable) and click **Add**.

Additional files will be copied to your machine. You may need to provide the OS install CD or the network share name. Support for the new languages will become available after restarting.

The following is a list of keyboards that each GO-Global client supports.

Linux supports:

Linux Keyboard Layout Name(s)	Linux Keyboard Layout	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S. English	us	English (United States)	US	00000409	us.kbm
Japanese	jp	Japanese	Japanese (106/109 Key)	E0010411 (IME)	jp.kbm
French	fr	French (France)	French	0000040C	fr.kbm
Belgian (be-latin1)	be	French (Belgian)	Belgian French	0000080C	be.kbm
German, German (Latin1), German (Latin1 w/ no dead keys)	de	German (Germany)	German	00000407	de.kbm
Polish	pl	Polish	Polish (214)	00010415	pl.kbm
Brazilian (ABNT2)	br	Portuguese (Brazil)	Portuguese (Brazilian ABNT2)	00010416	br.kbm
***See the Client Keyboard Mapping Files section below for more information.**					

macOS supports:

MacOS Keyboard Layout Name	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S.	English (United States)	U.S. International	00020409	us.kbm
French	French (France)	U.S. International	00020409	fr.kbm
German	German (Germany)	U.S. International	00020409	de.kbm
***See the Client Keyboard Mapping Files section below for more information.**				

Due to physical differences between the macOS and Windows keyboards, the macOS keyboard mapping files use the **U.S. International** Windows keyboard layout to translate a majority of the keys to Windows applications.

Windows clients support any keyboard that the GO-Global Host has drivers for.

Client Keyboard Mapping Files

GO-Global uses keyboard mapping files on Linux and macOS to ensure that the proper keyboard layout is loaded on the host and that the correct key codes are sent for each key press and release. Keyboard mapping files allow support for new keyboards to be added by simply copying a new keyboard mapping file to the client. Keyboard mapping files are installed into the **/etc/AppController/kbd** directory on Linux and the **/etc/AppController/kbd** directory on Mac. An internal version of the **us.kbm** keyboard mapping file will be used if a keyboard mapping file is not found.

These clients can automatically load keyboard mapping files based on information obtained from the operating system.

The keyboard mapping file installation location (i.e., default root path) for Linux is **/etc/AppController/kbd**. The default layout is U.S. English, obtained by the environment variable or automatically from the operating system.

Keyboard/IME Identifiers Used by GO-Global

GO-Global uses two identifiers, collectively known as **GO-Global Input Identifiers** (GGII), to specify a keyboard/IME for a session. The first is a keyboard layout. These are 8-digit string identifiers that Windows operating systems use to load keyboard drivers and IME programs. They are similar to locale IDs in that the last four digits typically match the 4-digit locale ID of the language supported by the keyboard. Keyboard layouts that specify an IME typically start with an “E”. The list of available keyboard layouts can be viewed in the registry under the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts] key. The second identifier used by GO-Global is the layout text string, which is a registry value of each keyboard layout registry key. These strings are displayed in the dropdown box under Keyboard layout/IME when adding input languages.

In the following examples, the first has a keyboard layout GGII of 00000409 and a layout text GGII of US. The second example has a keyboard layout GGII of E0010411 and a layout text GGII of Japanese Input System (MS-IME2002).

For example:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\00000409
Layout File = KBDUS.DLL
Layout Text = US

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\E0010411
Ime File = imejp81.ime
Layout File = Kbdjpn.dll
Layout Text = Japanese Input System (MS-IME2002)

Environment Variable	Description
APPCONTROLLER_KBD_FILE	This environment variable is used to specify the fully qualified path name of the mapping file to use. If specified, this will override all other means of obtaining the filename path. For example: On Linux, **APPCONTROLLER _KBD_FILE= /home/someuser/KeyMappingFiles/MyCustomKeyMappingFile .kmf** will cause that exact file to be loaded. If that file is not found the internal version of the **us.kbm** keyboard mapping file will be used.
APPCONTROLLER_KBD_FILE_ROOT	This environment variable is used to specify the root path name to the keyboard mapping files. The **kbd** directory that contains the keyboard mapping files will be expected to be in this directory. For example: On Linux, **APPCONTROLLER _KBD_FILE_ROOT=/home/someuser**, will cause the file /home/someuser/kbd/*xxx*.kbm to be loaded, where '*xxx*' indicates the LAYOUT obtained from the following APPCONTROLLER _KBD_ LAYOUT environment variable or automatically from the OS.
APPCONTROLLER_KBD_LAYOUT	This environment variable is used to specify which LAYOUT (or file name prefix) to use. This LAYOUT name along with the appended .kbm extension will be used as the file name. For example: **APPCONTROLLER_KBD_LAYOUT= MyCustomKeyMappingFile** will load the file /etc/AppController/kbd/MyCustomKeyMappingFile.kbm. If the above example for APPCONTROLLER_KBD_FILE_ROOT is also used, the file /home/someuser/kbd/ MyCustomKeyMappingFile.kbm will be loaded. A subdirectory of the root path name to the mapping files can also be included here. For example: APPCONTROLLER_KBD_LAYOUT=thinclient/us will load /etc/AppController/kbd/thinclient/us.kbm provided a different root path is not specified. This will override the LAYOUT obtained automatically from the OS.

To use client-side IME on an Arabic OS, the **KeyReportingMethod** property in the HostProperties.xml file must be set to 0. For more information, see Key Reporting Method.

Configuring Client Keyboard Options

You can specify the keyboard/IME for a session using the -kb shortcut parameter or the "keyboard" hyperlink parameter. These take both types of GGIIs described above. On Windows computers, if the -kb shortcut parameter is not specified, GO-Global will use the layout text of the currently active keyboard layout. On Linux computers, GO-Global does not send a layout text to the server if one is not specified on the command-line.

For example:
Windows shortcut using a keyboard layout:
AppController.exe -h server1 -kb 00000409

Specifying Layout Text Substitutions

Layout text substitutions can be specified on the server to map between client and server keyboard layout names. They can be used to:

1. Overcome differences in layout text names on different versions of Windows. For example, the **Japanese Input System (MS-IME2000)** layout text from a Windows 2000 GO-Global client system can be substituted with the **Japanese Input System (MS-IME2002)** layout text from a GO-Global Host.

2. Substitute an ANSI name for a keyboard layout that has a UNICODE name. For example, when specifying a keyboard layout with a UNICODE name through the “keyboard” applet parameter in an ASCII HTML page, it is necessary to substitute an ASCII name for the UNICODE name.

Keyboard Layout Substitutions are specified under the [HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\AppController\System\Keyboard\Layout \Substitutes] registry key. Each REG_SZ value within this key has the name of a GGII, and the value is the name of a layout text from the server that should be used in place of the client name.

Setting the Fallback Layout Text

If there is no GGII specified from the client, or the one specified fails to load a valid keyboard layout, the GO-Global Host uses a fallback mechanism to determine which keyboard layout should be used for the session. The fallback layout text should be the layout text for the keyboard layout that will be used by all clients connecting to the server, exclusive of those passing a valid GGII. The fallback layout text is automatically set during installation if the keyboard layout that is active is an IME. It may be modified after installation by editing the **Fallback Layout Text** value under the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\AppController\System\Keyboard Layout

When connecting to a Chinese GO-Global Host, the **Sign In** dialog appears from the shortcut along with the IME bar specifying Chinese as the default language. Clicking CTRL+spacebar does not toggle the languages. Users must manually click the IME bar with the mouse pointer to select English. Without manually clicking the IME bar, users will be unable to type a user name and password.

Configuring Multiple Input Locales

The **Default User** account profile can be configured with different and/or multiple input locales. Account profiles for new users logging on to a GO-Global Host are automatically configured with the **Default User** account's input locales. Users can switch to any input locale that is defined in their account profile.

Users with roaming profiles or profiles that already exist on the GO-Global Host will not receive these new settings. These accounts must be configured manually.

As an example, the following instructions describe how to install and use the German input locale on an English Windows Server 2016.

1. Enable German on Windows Server 2016.

1.1 Sign in to the GO-Global Host interactively with a user account that you wish to set the Input Local for.
1.2 Click Start | Control Panel | Language.
1.3 Click **Add a language**.
1.4 Select Deutsch (German) and click **Open**.
1.5 Select Deutsch (Deutschland) as the Regional variant and click **Add**.

2. Verify that the input locale is correctly installed and configured.

2.1 Launch Notepad in this interactive session.
2.2 Type a few characters in English.
2.3 Type Left Alt + Shift.
2.4 Type a few characters (for example, [; and ‘) and verify that they display in German.

The German input locale is now enabled for the **Default User** profile and the user that was logged on to the system in step 1.1.

3. Switch between input locales during a GO-Global session.

3.1 Start a GO-Global client and connect to the server with the account used in step 1.1.
3.2 Launch Notepad.
3.3 Type a few characters in English.
3.4 Type Left ALT + Shift.
3.5 Type a few characters and verify that they display in German.

Users will not be able to switch input locales when the **Sign In** dialog is displayed. The input locale for the default language of the GO-Global Host will be used.

On Windows clients, the selected input locale of server-based applications is not displayed in the system tray of the client computer.

Localizing Messages

Text that GO-Global displays to end users can be displayed in users' native languages, irrespective of the language of the host computer. This includes text displayed by GO-Global's Logon and Program Window applications and messages displayed by GO-Global clients (i.e., AppController and the GO-Global Web App and its associated web pages).

Text that GO-Global displays to end users is read from language-specific resource files. By default, when a GO-Global client starts, it checks the default language of the client device and then checks for the existence of a resource file for that language. If a resource file exists for the language, it is loaded, and text strings are read from it. If no resource file exists for the language, the client loads the English resource file and reads text strings from it.

Once the language is selected, all GO-Global processes that start within the user’s session attempt to load the application-specific (e.g., Logon, Program Window, etc.) resource files for the selected language and display the text strings stored in the file. If a resource file for the selected language does not exists for a given GO-Global application (e.g., the Program Window), the application will display its text in English.

GO-Global ships with English and Portuguese resource files. These files are located in the \Program Files\GraphOn\GO-Global\Programs\localization\strings directory. Administrators can modify the text strings contained within these files and can also create files for additional languages.

In environments using a third-party load balancer, changes to GO-Global's resource files must be replicated on all Farm Hosts. In environments using a GO-Global Relay Load Balancer, changes to GO-Global's resource files must be replicated on all Dependent Hosts, the Relay Load Balancer, and the backup Relay Load Balancer.

Administrators cannot modify the text strings that GO-Global clients display to users before the client connects to a host. For example, administrators cannot alter the text that is displayed by the AppController Connection dialog. Text that a GO-Global client displays before the user connects to a host is displayed using the resource files that ship with the GO-Global client.

Partners wishing to provide native language support for additional languages should contact sales@graphon.com.

Language Codes

The language files and options are defined with the ISO 639 two-letter code. For example, English is **en** and Portuguese is **pt**. A list of ISO 639 language codes can be found at https://en.wikipedia.org/wiki/List_of_ISO_639_language_codes.

Web Client Language

Client-side language is determined by the display language of the client system. For the GO-Global Web App, the display language of the browser is selected. The Web App language can be changed on a per user basis by a URL suffix of language=xx. For example, to use Portuguese, browse to: https://gg-host1.example.com/**?language=pt**.

Additionally, the logon.html file accepts the parameter controlArgs.set(["language","pt"]);.

AppController Language

GO-Global supports overriding the default language of the client device on a per user basis in AppController via a command-line option. The option **-language xx** can be used to override the client's system language.

In the following example, the default language for the client is set to Portuguese: AppController.exe -h gg-host1.example.com **-language pt**

GO-Global also supports overriding the host operating system's language with a language specified in the HostProperties.xml file.

Specifying a Language for Host-Side Generated Text

The session language on the GO-Global Host can be specified in the HostProperties.xml file by setting the **ClientLanguage** property to the appropriate ISO 639 two-letter code.

To specify a default language on a GO-Global Host

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\GraphOn\GO-Global\HostProperties.xml in a text editor.
3. Locate the **ClientLanguage** property and set its associated value to the two-letter code of the desired language. For example, to use Portuguese:

```
<property id="ClientLanguage" group="Branding" type="STRING">
        <value>pt</value>
</property>
```

4. Save HostProperties.xml.
5. Start the **Application Publishing Service**.

If a language is not supported, it defaults to English.

If the **ClientLanguage** property is set in the HostProperties.xml file, host-side generated text will be set to the specified language, regardless of the client's language or the client's **-language** command-line option.

Setting Resolution on Mobile Clients

When AppController connects to a GO-Global Host from an iOS device, the resolution of the session is set as follows:

1. If "-geometry WIDTHxHEIGHT" is specified in the **Options** field of the **Edit Connection** dialog, the session's width and height are set to the specified WIDTH and HEIGHT.

2. Otherwise, if the **Resolution Width** and **Resolution Height** values are specified under **AppController Settings**, the session's width and height are set to the specified values.

3. Otherwise, if **Scale Resolution** is disabled under **AppController Settings**, the session's width and height are set to the device's native resolution, as specified in the following table: https://developer.apple.com/library/archive/documentation/DeviceInformation/Reference/iOSDeviceCompatibility/Displays/Displays.html

4. Otherwise, the session's width and height are set to the device's scaled resolution (UIKit Size), as specified in the above table.

   Then, if **Pin Toolbar** is enabled under AppController Settings, the session's height is reduced by the height of the toolbar.

   And finally, if the above algorithm results in a width less than 800, or a height of less than 600, then the width and height are scaled up proportionally so they are both greater than or equal to those minimum values.

When AppController connects to a GO-Global Host from an Android device, the resolution of the session is set as follows:

1. If "-geometry WIDTHxHEIGHT" is specified in the Options field of the **Edit Connection** dialog, the session's width and height are set to the specified WIDTH and HEIGHT.

2. Otherwise, if the **Resolution Width** and **Resolution Height** values are specified under **Settings**, the session's width and height are set to the specified values.

3. Otherwise, if **Scale Resolution** is disabled under Settings, or if the device's logical density is less than 2, the session's width is set to the device's native width, and the session's height is set to the device's native height minus the height of any system toolbar.

4. Otherwise, if the session's width is set to half the device's native width, and the session's height is set to half the difference of the device's native height minus the height of any system toolbar.

Then, if **Pin Toolbar** is enabled under **Settings**, the session's height is reduced by the height of the AppController toolbar.

And finally, if the above algorithm results in a width or height less than 100, the width and/or height are set to 100 independently.

On Android, the logical density is defined as follows:

The logical density of the display is a scaling factor for the Density Independent Pixel unit, where one DIP is one pixel on an approximately 160 dpi screen (for example, a 240x320, 1.5"x 2" screen), providing the baseline of the system's display. On a 160 dpi screen, this density value will be 1; on a 120 dpi screen it would be .75; etc.

This value does not exactly follow the real screen size (as given by xdpi and ydpi), but rather is used to scale the size of the overall UI in steps based on gross changes in the display dpi. For example, a 240x320 screen will have a density of 1 even if its width is 1.8” or 1.3,” etc. However, if the screen resolution is increased to 320x480 but the screen size remained 1.5"x2" then the density would be increased (probably to 1.5).

APPENDIX

RapidX Protocol (RXP)

RXP is a proprietary protocol used for all GO-Global client-host data communications. By default, RXP runs over TCP port 491 but can be made to run over any compatible data port. RXP operates as part of the standard TCP/IP protocol stack. It is designed and optimized to handle low-bandwidth connectivity. The RXP display protocol is almost entirely asynchronous, which means the host and the client are rarely waiting for a response from its peer.

RXP is currently designed to handle encryption levels from 56-bit DES to 256-bit AES. When the TCP transport is selected, GO-Global uses GraphOn's implementation of the Data Encryption Standard (DES). When the Transport Layer Security (TLS) protocol is selected, GO-Global uses OpenSSL's implementation of TLS and OpenSSL's implementation of the selected cipher, for example, Advanced Encryption Standard (AES). When RXP is transported over a TLS connection, it is referred to as RXPS.

When a client opens a connection to the Application Publishing Service (APS), the APS first attempts to negotiate an RXP connection with the client. If the data that the APS receives from the client does not match the data that RXP clients send, the APS then attempts to negotiate a WebSocket (ws://) or WebSocket Secure (wss://) connection with the client.

During protocol negotiation, the APS closes the connection when any of the following occur:

- when the time required to negotiate the protocol exceeds the value of the **ProtocolNegotiationTimeout** property in the HostProperties.xml file
- when an error occurs while attempting to negotiate an RXP connection after the APS has determined that the client is trying to negotiate an RXP connection with the host
- when the client attempts to negotiate a WebSocket (ws://) connection with the host, and the host is configured to accept TLS connections (the TLS protocol is selected)
- when the client attempts to negotiate a Web Socket Secure (wss://) connection with the host, and the host is not configured to accept TLS connections (the TCP selected)

Encryption and Exportation Regulations

GO-Global incorporates open-source, publicly available software from the OpenSSL project. GO-Global's use of OpenSSL and other encryption technologies has been reviewed by the United States Department of Commerce and classified under the Export Commodity Control Number (ECCN) 5D002. The ECCN 5D002 classification allows GraphOn and its resellers to export and re-export GO-Global with support for up to 256-bit encryption, implemented by OpenSSL, to government and non-government entities, with the exception of USA embargoed countries, and except when GO-Global will be used in the design, development, production or use of nuclear, chemical or biological weapons or missiles.

Commodity Classification Automated Tracking System (CCATS) is an alphanumeric code assigned by the United States Bureau of Industry and Security (BIS) to products that it has classified under the Export Administration Regulations (EAR). GraphOn's CCATS number is G066799.

For further inquiries regarding GraphOn's CCATS number or ECCN classification, or for a copy of GraphOn's export license, please contact sales@graphon.com.

GO-Global Settings

Custom settings made in the Admin Console are saved in the **HostProperties.xml** and **DefaultWorkspaceProperties.xml** files, in the \ProgramData\GraphOn\GO-Global directory. The HostProperties.xml file stores general system-wide settings. The DefaultWorkspaceProperties.xml file stores user related settings.

The HostProperties.xml file is generated from the data in the HostPropertyDefinitions.xml file. On a clean install, GO-Global only installs the HostPropertyDefinitions.xml file. When the Application Publishing Service starts for the first time, it generates the HostProperties.xml file by copying the properties and their default values from the HostPropertyDefinitions.xml file into the HostProperies.xml file. Thereafter, the host uses the values in the HostProperties.xml file.

On an upgrade, the installer replaces the HostPropertyDefinitions.xml file with an updated version that includes all the newly supported properties. When the upgraded GO-Global Host attempts to access a new property and cannot locate it in the HostProperties.xml file, it copies the property and its default value from the new HostPropertyDefinitions.xml into the HostProperties.xml file.

Similarly, on a clean install, GO-Global only installs **WorkspacePropertyDefinitions.xml**. When the Application Publishing Service starts for the first time, it generates the DefaultWorkspaceProperties.xml file by copying the properties and their default values from the WorkspacePropertiesDefinitions.xml file into the DefaultWorkspaceProperties.xml file.

When upgrading, the installer replaces the DefaultWorkspaceProperties.xml file with an updated version that includes all the newly supported properties. When the upgraded host tries to access a property and cannot locate it in the DefaultWorkspaceProperties.xml, it copies the property and its default value from the new WorkspacePropertyDefinitions.xml into the DefaultWorkspaceProperties.xml file.

Third-Party Components

GO-Global uses code, including open source software, that is provided by the third parties. The third-party components that GO-Global uses, along with the associated licenses and supporting information, are identified below.

Third-Party Component	License Agreement
Codejock Software Xtreme Skinframework	http://www.codejock.com/products/licensefaq.asp
FFmpeg	https://github.com/BtbN/FFmpeg-Builds/releases
libpng	http://www.libpng.org/pub/png/src/libpng-LICENSE.txt
OpenSSL	https://github.com/openssl/openssl/#license
Qt	http://www.gnu.org/licenses/lgpl.txt
VeryPDF	http://www.verypdf.com/custom/license_agreement.htm
win-acme	https://github.com/PKISharp/win-acme/blob/master/LICENSE
XML Parser Library	https://www.applied-mathematics.net/tools/xmlparser_doc/html/index.html
Zlib	http://www.zlib.net/zlib_license.html

Known Limitations

The following are known limitations of GO-Global:

- GO-Global does not support Group Policy logon or logoff scripts.
- Microsoft's VBScripts are not supported as logon scripts unless they are run in a batch file.
- Copying a file on a GO-Global Host and pasting it to the client, while attempting to overwrite an existing file, may not work.
- GO-Global does not support Parallels Virtuozzo.
- GO-Global supports Adobe Acrobat 8.0 in a GO-Global session. Previous versions of Acrobat are not supported.
- Apple's Preview application is not supported when printing from a Mac. Adobe Reader is required in order to print when running on macOS.
- When any software on the GO-Global Host uses port 9010, users are unable to print with the Universal Printer Driver and ps2pdf.exe processes remain running on the host. Ps2pdf.exe uses port 9010 and this port cannot be changed. To work around this limitation, the software that is listening on port 9010 must be configured to use a different port. To check if another program is listening on port 9010, run CMD.exe as Administrator. Type **netstat -a** and click Enter. This will list all active TCP connections. The port numbers will be displayed after the IP address, separated by a colon.
- The GO-Global License Manager Service must be restarted whenever license files are added or removed.
- Japanese keyboards are only supported on macOS with the -kb ClientSideIME option.
- Painting problems may occur if a client's Task Manager is set to "Always On Top".
- Colors may display incorrectly when the client's display is set to 256 colors.
- Journal record hooks are not supported. As such, macros may fail to record in some applications.
- OLE objects embedded in a client-side file cannot be edited. If the application required to edit the OLE object is available on the host, copy the file to a drive on the host, edit it, and then, if desired, copy it back to the client.
- On non-Windows clients, only text and images can be copied and pasted between applications running on the client and applications running on the host.
- When a GO-Global Host is connected to a Relay Load Balancer, no warning is displayed that the host's settings (published applications, etc.) will be replaced by those of the Relay Load Balancer.
- Users are unable to reconnect to a disconnected session while the session is being shadowed.
- GO-Global does not support running the Application Publishing Service in any account other than the System account.
- The keyboard mapping command-line argument -kb is case sensitive on Linux and macOS. -KB will not work.

- GO-Global does not support the /3GB switch.
- Microsoft's XPS Document Writer is supported as a client printer when using the Universal Printer Driver, but the XPS Printer Driver is not.
- GO-Global does not support applications that integrate with the system tray.
- Sessions take longer to start when Apply Group Policy is enabled in the Admin Console.
- The host's Theme is not applied when users authenticate with Integrated Windows Authentication and server-side password caching is disabled.
- If Internet Explorer Enhanced Security Settings are enabled for users, *.microsoftonline.com must be added to the user's Trusted Sites in order to login to Office 365 from a GO-Global session.
- When the GO-Global Web App is run in Chrome 77 and later with useApp=true (default setting), the user is prompted to approve AppController every time it runs. Chrome no longer gives users the option to bypass the approval dialog and always run an application.
- Users cannot access client-side smart cards from Chrome running in a GO-Global session.
- The GO-Global Host fails to check out licenses if the LM_LICENSE_FILE environment variable:
  does not exist, is set to nothing, or does not match the value of the HKLM\SOFTWARE\FLEXlm License Manager\GGLicenseManager\License registry value.
- In some license configurations (e.g., when a central license server is used), the APS logs messages stating: “Failed to obtain a [application_process_name] license for the following reason: License server system does not support this feature...” These messages are benign.
- GO-Global sessions fail to start on Windows Server 2016 and Windows Server 2019 when the Hyper-V role is enabled.
- When ClientSideIME is set to true in the HostProperties.xml file (the default value), Ctrl-Z and Ctrl-Y can produce abnormal behavior in some applications. To work around these issues, set ClientSideIME to false.
- When users connect from iOS or Android to a GO-Global Host that has the TLS protocol enabled, a TLS warning dialog is displayed. To work around this issue, administrators must concatenate both the intermediate and root certificates to the server certificate, and users must inspect the certificate when they first connect to the host and, if it is correct, click Install to install the certificate on their device.
- When Adobe Reader is run in a GO-Global session on Windows Server 2012 R2, it reports that there is an “AppContainer System Incompatibility." To work around this issue and prevent the message from appearing, users can uncheck the option to "Enable Protected Mode at startup" in Adobe preferences.
- If the Web MSI is installed via the Updates tab of the Host Options dialog box and the corresponding Host MSI is not installed, the contents of the GO-Global\Web directory are updated, but the Updates tab does not include the Web MSI in the list of installed updates.

- The host computer crashes when Adobe Acrobat Pro is run in a GO-Global session. To work around this issue, disable the Adobe Genuine Monitor Service and Adobe Genuine Software Integrity Service.
- Files that have not changed are not replaced when an earlier release of the version 6 GO-Global Host is upgraded to the latest release. This is by design.
- The GO-Global Host fails to install on some systems that are not up-to-date with Windows Updates. This occurs when the prerequisites for Microsoft's Visual Studio Redistributables are not installed. To work around this issue, apply Windows Updates.
- When a user runs the GO-Global Web App in Google Chrome or Mozilla Firefox and types CTRL+N or CTRL+T, the browser opens a new window or a new tab, respectively. Similarly, when a user runs the GO-Global Web App in Microsoft Edge and types CTRL+O or CTRL+P, Microsoft Edge opens its File Open or Print dialog, respectively. In these, and other cases, browsers do not allow the GO-Global Web App to suppress their default behavior.
- When the GO-Global Web App is moved to a background tab on Safari on macOS, the client is disconnected from the session.
- DPI Scaling may not work in the GO-Global Web App.
- When the version 6 GO-Global Host is installed silently, the GO-Global Audio Driver will not be installed or upgraded. To work around this issue, install the GO-Global Audio Driver from Device Manager after running the GO-Global Host installer.
- AppController may not start automatically after it is installed. If this happens, click the Reload link.
- Mapping drives and printers via Group Policy is not supported. To work around this limitation, perform the mapping in a logon script.
- Numeric keys do not produce the correct characters in some applications. To work around this issue, modify the **keyreportingmethod** parameter. See the GO-Global Startup Parameters section for more information.
- The Client Drives feature is not supported from applications that are "run as administrator." Windows provides a variety of ways to run applications as administrator. For example, users can right-click an application in Explorer and choose **Run as Administrator**. Client Drives are not accessible to applications that are run as administrator, regardless of how the application is "run as administrator."
- If User A has a Print dialog box open while User B signs in to a GO-Global Host, User B's client printers may appear in User A's Print dialog. User A will not, however, be able to print to User B's printers.
- PDF, JPG, PNG, BMP, and JPEG files fail to open in their default viewer applications on Windows 10.
- The GO-Global Web App is compatible with Web Application Firewalls (WAFs) that support WebSocket connections. AppController is not compatible with WAFs, as they do not support TCP/IP connections.
- GO-Global does not map client drives A or B.
- There is a 20 character limit in Windows for local usernames. When creating longer usernames in Active Directory, the first 20 characters of the username will be

stored by default in the **User logon name (pre-Windows 2000)** field on the user's Account tab. The username in this field can be used to sign in to GO-Global.

- The Automatic Client Update feature does not work when GO-Global's Web component is not installed on the Application Hosts. To resolve this issue, re-run the GO-Global Host installer on the computer, click **Customize**, check **Web**, click **OK**, then **Install**.
- On-premises licenses will not work when NIC teaming is enabled on a GO-Global License Server and the hostid of the on-premises GO-Global license is a MAC Address that may be changed by NIC teaming. To work around this limitation, add a separate network adapter to the GO-Global License Server that is not affected by NIC teaming and request an on-premises license with a hostid equal to the MAC Address of the "un-teamed" network adapter.
- The following PDF converters are not supported:
  - PDFCreator from pdfforge
  - pdfFactory from FinePrint
  - CutePDF from Acro Software
- Windows 10 N and Windows 11 N are not supported platforms for the GO-Global Host. In addition, when AppController for Windows is run on Windows 10 N or Windows 11 N without the Media Feature Pack, sessions will fail to start, the AppController.exe process will exit soon after it starts, and the APS log on the host will contain the following error message:

  Failed to lookup the version of the GraphOn::RXP::DisplayClient class in the remote process. The class may not be registered in that process.

  Users can work around this issue by installing the Windows 10 or Windows 11 Media Feature Pack.

INDEX

4

443, 45
491, 45

8

80, 45

A

About dialog, 205
About menu, 205
-ac, 213, 217
Activation Wizard, 40
Active Directory, 136, 165, 178, 256
Active Directory Domain Controller, 165
Active Sessions, 239
addLink, 66
ADFS, 177
Adjusting the Printable Area, 228
Admin Console, 51, 59, 60, 88, 95, 132, 146, 198
  accessing from a client machine, 128
Adobe Acrobat Pro, 303
Affinity, 142
All Hosts, 88, 100, 105, 107, 108, 113, 146, 215
Always in front, 115
Apache HTTP Server, 47
AppController, 62, 139, 209
AppController.AllUsers.MSI, 273
AppController.MSI, 273
Apple Safari, 8
Application Host Manager, 145
Application Link, 52, 55
Application Publishing Service, 85, 88, 133, 136, 149, 187, 276, 278
Application Script Support, 251
Application Users/Groups, 60
Applications, 110
  adding, 51
  duplicating, 57
  editing properties, 58
  installing, 51
  renaming, 58
Apply Group Policy, 302
Arrange Items, 209
Audio Driver, 303
Audit data, 33, 35
Authenticator app, 173
Automatic client keyboard, 285, 286
Automating, 275
autoreconnect, 70, 151
AWS Application Load Balancers, 141
AWS Network Load Balancers, 141

B

Background Image, 206
Backup, 278
Backward Compatibility, 2
Basic authentication, 266
Branding, 199
Broadcast Interval, 113

C

Cache password on the client, 167, 168
Cache passwords on the host, 172
Case Number, 281
Central license server, 14
Certificate, 190, 191
Certificate Authority, 191
Change Icon, 52, 58
Change Password, 171, 172
Client clipboard, 100
Client Connections, 239
Client drive letters, 103
Client drives, 102, 103, 104
Client file access, 1, 102, 262
Client keyboards, 286
Client printer name, 227

Client Printer Naming, 227
Client printers, 70, 247
Client printing, 213
Client Printing, 258
Client Serial and Parallel Ports, 3, 101
Client Sound, 3, 101, 262
Client Time Zone, 100, 258
CLIENTCOMPUTERNAME, 251
clientdpi, 71, 282
ClientDPIScalingEnabled, 71, 282
ClientSideIMEEnabled, 302
Clipboard support, 100
Cloud environments, 22
Cloud License, 26, 41
Cloud License Administration, 26
Cloud License Service, 31, 33, 34, 35, 145
Cloud licenses, 131
cloud licensing, 145
Cloud Licensing Service, 13
cm.exe, 128
Color depth, 7, 244
Column Header, 208
COM Security, 166, 183
Command-line options, 52, 58, 61
Components, 300
computerName, 72
Concurrent usage, 13
Configuration Settings, 153
Configuration Tab, 49
Connected Clients, 91, 110
Connection dialog, 132, 188
Connection Verification, 280
ConnectionVerificationInterval, 280
ConnectionVerificationTimeout, 280
Consecutive letters, 103
Copy and paste, 100
CPU, 113
CPU requirements, 8
CPU utilization, 113
Critical, 125
Cross-platform Compatibility, 1
Custom toolbars, 231
CutePDF, 304

D

Data Encryption Standard, 297
DataDownloader.exe, 261, 262
DataProcessor.exe, 261
DataViewer.exe, 261
dcomcnfg, 166, 183
Default printer, 217, 218
Default Printer, 223
DefaultLoaderOptions, 261, 262
Defer Windows Updates, 124
DelayWindowsUpdates, 123
Delegation, 165
Demilitarized zone, 136
Dependent Host, 146, 148
Dependent Hosts, 135, 147
DES encryption, 188
DesktopColor, 66
dfw option, 285
Diagnostic Messages, 277
Disconnect, 95, 97, 120, 198
Disconnecting a session, 97
Display applet, 282
Display name, 52
Display scaling, 282
DMZ, 57, 147
Domain, 63
Domain Controller Security Policy, 86
Domain name, 85
Domain Security Policy, 86
DPI Scaling, 303
DragFullWindows, 285
Drive letters, 103
Drive mappings, 243
DWORD, 260
Dynamic Display Resize, 3

E

Elastic IP address, 22
Elastic Network Interface, 22
Emergency licenses, 38
Encrypted WebSocket, 79
Encryption, 188, 189
Errors, 277
Events, 277
Expiration Date, 93
Expired, 95
explorer.exe, 263
Explorer.exe, 259

F

Failover Farm Manager, 154
Failover server, 151, 152
Failure recovery, 149
Fallback Layout Text, 291
Farm Host, 139
Farm Manager, 130, 137, 152
File Open Redirection, 5, 106
File Permissions, 86
Firewall, 136, 147, 187
Full Windows, 285

G

geometry, 81
Get Link, 52
GetComputerName, 250
GGII, 288
Global logon script, 118
Global scripts, 116
GO-Global Application Publishing Service, 42, 188
GO-Global Host, 7, 86, 89, 95, 198, 251, 277
GO-Global Host Performance Counters, 239
GO-Global Input Identifiers, 288

GO-Global licenses, 4
GO-Global Licenses, 93
Grace, 95
Grace period, 122
Gridlines, 208
Group Policy, 114, 301, 303
Group Policy Management, 255, 256
Group Policy Object, 255
Group Policy Objects, 256
Group Policy Support, 2

H

H.264 video format, 105
healthCheck request, 6
Help Topics, 206
Hex number, 273
Hiding client drives, 104
High Availability, 31
High resolution, 282
High Resolution Displays, 3
Host, 40, 41
Host activity, 110
Host address, 55
Host Installer, 43
Host Monitoring, 2
Host Options dialog, 96
Host Port, 187
Host Updates, Pending and Installed, 126
hostid, 18
HostProperties.xml, 169, 228, 253, 282
HTML5, 4
HTTP, 56, 266
HTTP CONNECT method, 265
HTTPS, 56, 266
Hyper-V, 302

I

ID token, 181
Idle limit, 120
Idle time, 120
IIS, 80
IIS Web Server, 46
Image compression, 246
Increment, 103
Independent Hosts, 132
InitializeProfileWithExplorer, 263
Input Method Editor, 285
Input Method Editors, 286
Installing the GO-Global Host, 40, 41
Integrated Web Server, 45
Integrated Windows authentication, 95, 136, 146, 164, 198
Integrated Windows Authentication, 172
INTERACTIVE group, 163
Internet Options, 265
Invalid logons, 64
IP address, 110
IPv4, 267
IPv6, 188, 267
isembeddedwin, 71

J

Journal record hooks, 301

K

Kerberos authentication, 184
Keyboard layout, 288
Keyboard Mapping Files, 288
keyreportingmethod, 72

L

Large deployments, 130
Launch and Activate, 166, 183
Launch Parameters, 60
Layout text, 290
Layout text substitutions, 290
License Administration, 26
License Change Request, 16
License Change Requests, 14
License Consumption, 13
License ID, 16, 93
License Management, 26, 38
License Manager Service, 301
License Master ID, 14, 15, 93
License seats, 13, 251
License Server, 144
License-file list redundancy, 19
Live collaboration, 90
LM_LICENSE_FILE, 19, 21
lmtools, 19
Load Balancing, 2, 130
Local computer, 63
Local logon rights, 86
Local Security Policy, 86
Localization, 6
Log Directory, 237
Log Files, 276, 278
Log folder, 134, 278
Logon Manager, 116
Logon scripts, 116, 243

M

MAC Address, 13
Maintenance, 278
ManageLicensesFrom, 49
Mapped drives, 59, 243
MappedPrinterDrivers.xml, 216, 221, 222
Master, 18
Maximum number of sessions, 119
Maximum Sessions, 239
Maximum sessions count, 119
Media Feature Pack, 304
MEM, 113
Mem usage, 113

Memory requirements, 8
Messages, 276
Microsoft Hyper-V, 7
Mix Windows, 6
Mobile App Console, 237
Mobile App Toolbar Editor, 3
MobileAppLogs, 237
MobileAppSettings, 237
Modifying the Host Port Setting, 187
Mozilla Firefox, 303
Multi-Factor Authentication, 4, 173
Multiple Input Locales, 291
Multi-user deployment, 51, 251

N

Named pipe, 260
Network adapter, 304
Network Printer, 87
Network share, 243
New Password, 170, 171
NIC teaming, 304
noscale, 71
NTFS, 60
Numeric keys, 303

O

ODBC data sources, 59
Offline, 136
Ogg Vorbis, 101
OIDC, 178
OIDC identity provider, 179
Okta, 177
On-Premises License, 44
OpenID Connect, 178
OpenID Connect Authentication, 177
Optional, 125
Options dialog, 129
Organizational units, 6
OTP, 142
Output Level, 277

P

Password, 70
Password Caching, 166
Password Change, 170, 172
Password expiration, 247
Password Locations, 168
Password manager, 173
PasswordExpirationWarning, 247
PDFCreator, 304
pdfFactory, 304
Performance Auto-Tuning, 271
Performance counters, 2, 238
Performance problems, 119
Perpetual, 15
Physical memory, 120
Ping, 280
Port, 70, 187
Port Forwarding, 57
PowerShell, 27
Preview PDF, 214
Print Spooler Service, 214
Printer Configuration, 216
Printer drivers, 213, 221, 223
printerconfig, 213, 217
PrinterConfigWaitTime, 247
PrinterNameFormat, 227
Printers Applet, 216, 217, 220
Printing, 213
Process
  ending, 89
Process ID, 111, 276
Process information, 111
Processes, 113
Procs, 113
Product Code, 12, 14, 93
Product Logo, 210
Program Cache, 273
Program Window, 59, 60, 95, 198, 199, 205, 217, 283
ProgramWindowCloseOption, 283
Progress message, 114
Protocol, 56
ProtocolNegotiationTimeout, 298
Proxy printer names, 227
Proxy printers, 216, 222
Proxy server, 266
Proxy tunneling, 2
Proxy Tunneling, 265
Publishing Applications, 51

Q

quantize, 246
QuantizeSwitch, 246
Quick, 51
QWORD, 186, 262

R

RapidX Protocol, 105, 265, 297
Recommended, 125
Redirection settings, 261
Redirector settings, 260
Redundant license lervers, 18
Refresh rate, 112
Relay Load Balancer, 50, 133
Relay server, 147
RelayConnectionAddress, 142
Remapping client drives, 103
Remote users, 57
Reserved seats, 30, 94
Reset Printers, 220
Resource limits, 114, 119
Reverse proxy, 78
Revoked,, 94
Roaming user profiles, 86, 131

Router, 57
RSA algorithm, 168
RXP, 297

S

S4U login, 179
Scaling, 282
Screen scrape, 272
Search, 111
Search button, 6
Seat reservations, 32, 34
Seats, 93
Seats in use, 94
Security, 86, 188
Security Alert, 190
Serial and Parallel Ports, 101, 258, 262
Server Connections, 239
Server Performance Counters, 239
Service Principal Name, 184, 243
Session
  encrypting, 188
  terminating, 89, 90
Session information, 110
Session limit, 120
Session Name, 110
Session Process Configuration, 258
Session reconnect, 2, 95, 131, 198
Session shadowing, 2, 90
Session Startup, 117
Session termination, 96
Session timeout, 95, 198
Sessions, 113
Sessions tab, 96
SessionTimeoutBrokenConnection, 132
Shadowing a session, 90
Shared account, 99
Shortcut, 273
showlogon, 169
showLogonCachedPassword, 169
Sign In dialog, 169, 199
Silent installation, 273
Single sign-on, 177
Smart Card, 108
Sound, 101
SQL Server, 184
srw.exe, 281
Standard authentication, 163, 165
Start Directory, 52, 58, 59, 61
Start menu, 63, 64, 273
Startup State, 52, 58, 61
Startup Time, 110
Status bar, 113, 129
Stickiness, 142
Support Request Wizard, 281
System Extensions Driver, 34
System requirements, 7
System tray, 302

T

Target endpoint, 76
TCP/IP, 130
Test Page, 219
Theme, 302
Third-Party Components, 300
Third-Party Load Balancers, 130, 139
Three-server redundancy, 18
Time Zone Redirection, 2
Title bar icon, 206
TLS certificate, 154
TLS Configuration, 153
tls option, 154
TLS protocol, 65, 154, 302
Toolbar Directory, 237
Total seats, 94
Trace Messages, 277
Trial license, 44, 94
Trusted domains, 63
Two-Factor Authentication, 173, 201

U

UNC, 59
Unencrypted WebSocket, 79
Universal Driver, 214
Universal Printer Driver, 220, 221, 228
UniversalRemotePrinter.ppd, 228
Updates, 125, 126
Upgrading, 42
USB drives, 102
useApp, 66, 71, 142
User, 110
User Accounts, 40, 85
User name field, 64
User Principal Name, 176
User Profiles, 86
User Verification Codes, 176
Users and Groups, 253
User-specific scripts, 116

V

VBScripts, 301
Version number, 127
Video Replay, 105
Virtual directory, 56
Virtual memory, 120
VMware ESXi, 7
VPN, 57

W

WAF, 78, 303
Warning period, 121
Warnings, 277
Web access, 82
Web App, 4, 13, 65, 66, 131, 303
Web Application Firewalls, 303

Web MSI, 302
Web proxy server, 265
Web server address, 54, 55
WebSocket, 78, 297
WebSocket Secure, 297
WebSocket URL, 75
Wildcard certificate, 154
Windows 10 N, 304
Windows 11 N, 304
Windows Compatibility Assurance, 3, 123
Windows Explorer, 86
Windows folder, 214
Windows Updates, 123
ws, 76
wss, 76
wsurl parameter, 76

X

XPS Document Writer, 302

Y

Yellow, 136