



GO-GLOBAL

Gateway Administrator Guide

July 30, 2012

4.5.0

COPYRIGHT AND TRADEMARK NOTICE

Copyright © 1997-2012 GraphOn Corporation. All Rights Reserved.

This document, as well as the software described in it, is a proprietary product of GraphOn, protected by the copyright laws of the United States and international copyright treaties. Any reproduction of this publication in whole or in part is strictly prohibited without the written consent of GraphOn. Except as otherwise expressly provided, GraphOn grants no express or implied right under any GraphOn patents, copyrights, trademarks or other intellectual property rights. Information in this document is subject to change without notice.

GraphOn, the GraphOn logo, and GO-Global and the GO logo are trademarks or registered trademarks of GraphOn Corporation in the US and other countries. Microsoft, Windows, Windows NT, Internet Explorer, and Terminal Server are trademarks of Microsoft Corporation in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds. UNIX is a registered trademark of The Open Group. Red Hat is a trademark or registered trademark of Red Hat, Inc. in the United States and other countries. Adobe, Acrobat, AIR, Flash, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Firefox is a registered trademark of the Mozilla Foundation. Mac, Mac OS, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries.

Portions copyright © 1998-2000 The OpenSSL Project. All rights reserved. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (www.openssl.org). Portions copyright © 1995-1998 Eric Young (eyay@cryptsoft.com). All rights reserved. This product includes software written by Eric Young (eyay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

MacBinary Toolkit for Java, Copyright 1998, 1999, 2001 by Gregory L. Guerin.
Available at <http://www.amug.org/~glguerin/sw/#macbinary>. All rights reserved.

All other brand and product names are trademarks of their respective companies or organizations.

Printed in the United States of America.

CONTACT INFORMATION

GraphOn Corporation
1901 S. Bascom Avenue
Suite 660
Campbell, CA 95008

Toll Free: 1.800.GRAPHON
Phone: 603.225.3525
Fax: 408.626.9722

GraphOn
Building A, Trinity Court
Wokingham Road
Bracknell, Berkshire
RG42 1PL
United Kingdom

Phone: +44 1344.206549
Fax: +44 1344.206855

CHAPTER 1: INTRODUCTION

Introduction to GO-Global Gateway	5
Features.....	6
Requirements	8

CHAPTER 2: GETTING STARTED

Installing the Gateway	11
Granting Organizational Units Access to the Gateway	15
Installing the Host.....	16
Connecting the Host to the Gateway	19
Publishing Applications.....	21
Publishing Hosts to Users.....	23
Application-Based Load Balancing	23
Client Installation.....	24
Running Applications	26
Creating and Seeding the Microsoft SQL Server 2008R2 Database	26
Uninstalling the Gateway.....	30

CHAPTER 3: GATEWAY

Introduction.....	32
Gateway Navigation.....	32
Gateway Toolbar	34
Workspaces	37
Session Management.....	41
Default Host Properties	44
Access Logs	45

CHAPTER 4: HOST CONFIGURATION

Administering a Host	47
Client Updates	49
Security.....	50
Connections.....	51
Logging	61
Access Logs	65
Host Load Balancing.....	66
Support Request Wizard	67

CHAPTER 5: OPTIONS CONFIGURATION

Options Configuration.....	68
Viewing Options Details.....	71
Client Access	72
Client Printing	76
Display	82
Time Limits	82
User Sandbox.....	85

CHAPTER 6: ADVANCED TOPICS

Proxy Hosts	88
How Do Proxy Hosts Work?	89
Gateway Database Schema ID	91
Licensing	92
Configuring the Gateway for SAML Authentication.....	97
Preventing Users from Bypassing the Gateway.....	100
Performance Auto-Tuning.....	100
Advanced Session Process Configuration	102
Browser-Specific Limitations.....	106
Uninstalling Clients	107

CHAPTER 1: INTRODUCTION

INTRODUCTION TO GO-GLOBAL GATEWAY

GO-Global Gateway is the easy and cost-effective way to create a secure, private cloud environment. As a standard GO-Global for Windows feature provided at no additional cost, GO-Global Gateway provides a high-availability interface to GO-Global Hosts. Your Windows applications and documents remain in a secure, central location easily accessed by authorized users running Windows, Linux, UNIX, Apple OS X and iOS, Android, or simply a Web browser.

With GO-Global Gateway, administrators have extensive control over user rights and privileges, allowing them to monitor and manage clusters of GO-Global Hosts. Users can access and share applications, files, and documents via simple hyperlinks. And developers can integrate Windows applications into their Web-based enterprise and workflow applications.

GO-Global Gateway extends access to users who might be prevented from connecting directly to a GO-Global for Windows Host due to a firewall or proxy server.

GO-Global Gateway is a robust, yet easy-to-deploy Web service featuring a modern, intuitive user interface. GO-Global Gateway runs under Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Red Hat Enterprise Linux 5 and 6, or SUSE Linux Enterprise Server 11. It can be installed on a standalone Windows or Linux server, or together with a GO-Global Host on a Windows Server.

FEATURES

GO-Global Gateway includes the following features:

ANYWHERE ACCESS

GO-Global requires only an Adobe Flash-enabled browser to run applications and open documents and uses standard ports (e.g., 80) and standard protocols (e.g., HTTP) to communicate with gateways and hosts.

CENTRALIZED ADMINISTRATION

GO-Global allows administrators to centrally manage hosts from virtually any computer that has a Flash-enabled browser or a GO-Global client.

HIGH-AVAILABILITY LOAD BALANCING CLUSTERS

Administrators can create high-availability, load-balancing clusters of hosts. These clusters have no single point of failure, and balance the load between hosts taking into account factors such as CPU usage, memory usage and the number of running sessions.

ENHANCED SECURITY

GO-Global provides an additional level of authentication and access control to hosts. This enables corporations to safely provide their employees with access to hosts, as well as their partners and customers.

AUTOMATIC CLIENT UPDATES

Administrators can configure GO-Global to automatically update clients when users connect to a Windows host that is running a newer version.

GROUP-BASED PUBLISHING AND CONFIGURATION

Administrators can publish applications to groups and configure settings based on a user's group membership.

SESSION SHADOWING

Administrators are able to shadow users' sessions.

HTTP TUNNELING

The GO-Global Client tunnels GraphOn's RapidX protocol over HTTP. This enables users who connect to the Internet via Web proxy servers to run applications on GO-Global Hosts.

WEB API

With GO-Global's Web API, Windows applications can be easily integrated with existing Web applications. Almost all gateway and host features can be accessed and controlled programmatically from Web-based applications using the GO-Global Web API. For example, developers can start and monitor sessions, authenticate users, create user-private workspaces, move files to and from a workspace, start and stop applications, and monitor server usage.

HYPERLINK ACCESS

With GO-Global, every resource on a host can be accessed via a hyperlink. This makes it possible for users and administrators to share applications, documents, folders, files, sessions, etc. with authorized users by simply sending them a hyperlink in an email or instant message.

SECURE DOCUMENT SHARING

GO-Global's document sharing feature extends many of the benefits of application and desktop virtualization to documents. Using this feature, users can securely share documents and files centrally, from hosts. Depending on their access rights, recipients can view and edit documents regardless of whether or not they have the correct application installed on their computers. In addition, documents shared via GO-Global never have to leave the host, thereby protecting the sender's intellectual property.

HIGH PERFORMANCE, PATENTED RXP PROTOCOL OVER LOW-BANDWIDTH CONNECTIONS

GraphOn's RapidX protocol provides improved interactivity with graphics-intensive applications. RapidX is many times more efficient than the standard X protocol.

USER SANDBOX

The User Sandbox provides an easy and secure way to limit the files and programs that users can access.

APPLICATION-BASED LOAD BALANCING

Applications do not need to be installed on every host in a cluster. If an application exists on multiple hosts in a cluster, GO-Global starts the application on the host with the lightest load.

REQUIREMENTS

GATEWAY PLATFORMS

The gateway is supported on the following operating systems:

Windows Server 2008 R2 with Service Pack 1

- Standard Edition (64-bit)
- Enterprise Edition (64-bit)

Windows Server 2008 with Service Pack 2

- Standard Edition (32-bit and 64-bit)
- Enterprise Edition (32-bit and 64-bit)

Windows Server 2003 R2 with Service Pack 2

- Standard Edition (32-bit)
- Enterprise Edition (32-bit)

Windows Server 2003 with Service Pack 2

- Standard Edition (32-bit)
- Enterprise Edition (32-bit)

Red Hat Enterprise Linux 5 (64-bit)

Red Hat Enterprise Linux 6 (64-bit)

SUSE Linux Enterprise Server 11 (64-bit)

The gateway requires 1 CPU and 1 GB of memory for every 200 users.

HOST PLATFORMS

The host is supported on the following operating systems:

Windows Server 2008 R2 with Service Pack 1

- Standard Edition (64-bit)
- Enterprise Edition (64-bit)

Windows Server 2008 with Service Pack 2

- Standard Edition (32-bit and 64-bit)
- Enterprise Edition (32-bit and 64-bit)

Windows Server 2003 R2 with Service Pack 2

- Standard Edition (32-bit)
- Enterprise Edition (32-bit)

Windows Server 2003 with Service Pack 2

- Standard Edition (32-bit)
- Enterprise Edition (32-bit)

Windows 7 with Service Pack 1 (64-bit)*

Windows Vista with Service Pack 2 (64-bit)*

Windows XP Professional with Service Pack 3 (32-bit)*

**GraphOn recommends Windows Server for multi-user environments.*

GO-Global is supported running in virtualized environments including VMware vSphere, Microsoft Hyper-V, and Citrix XenServer.

CLIENT PLATFORMS

GO-Global Gateway clients are supported on the following platforms:

- Windows 7 with Service Pack 1 (32-bit/ 64-bit)
- Windows Vista with Service Pack 2 (32-bit/64-bit)
- Windows XP with Service Pack 3 (32-bit)
- Mac OS X 10.5 and later
- Red Hat Enterprise Linux 5 and 6 (32-bit/64-bit)
- CentOS 5 and 6 (32-bit/64-bit)
- SUSE Linux Enterprise Desktop 11 (32-bit/64-bit)

The following browsers are supported with Adobe Flash Player 9:

- Internet Explorer 7.0 or later
- Mozilla Firefox 10 (ESR)
- Apple Safari 5.0.6 or later on Mac OS X

CHAPTER 2: GETTING STARTED

INSTALLING THE GATEWAY

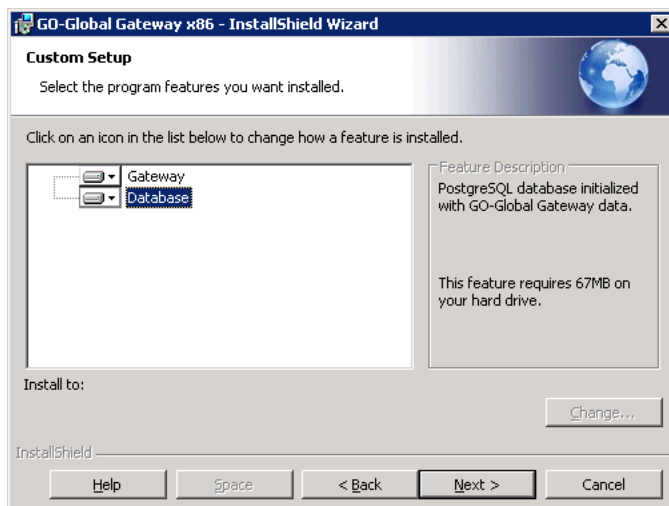


The gateway is supported on the x86 and x64 versions of Windows Server 2003 (Standard Edition and Enterprise Edition) and Windows Server 2008 (Standard Edition and Enterprise Edition) and the 64-bit versions of Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, and SUSE Linux Enterprise Server 11.

The gateway setup program installs the Java Runtime Environment (JRE) from Sun Microsystems, Apache Tomcat, PostgreSQL, and the GO-Global Gateway.

To install the gateway on Windows

1. Log on to the computer on which you plan to install the gateway as an administrator (i.e., log on using an account that is a member of the Administrators group)
2. Run the gateway setup program. On 32-bit systems, run **go-global.windows_x86.exe**; on 64-bit systems, run **go-global.windows_x64.exe**.
3. If the **User Account Control** dialog is displayed, click **Continue**.
4. If prompted to install **Microsoft Visual C++ Redistributable Package (x64)**, click **Install**.
5. On the **InstallShield Wizard** dialog, click **Next**.
6. Accept the terms in the license agreement and click **Next**.
7. By default, the setup installs the Gateway and Database. Click **Next**.



Type a password that will be used for Apache Tomcat and PostgreSQL. (If a PostgreSQL user already exists on the host, enter the existing PostgreSQL password.) Depending on the password complexity requirements of the computer, a complicated password may be required.

Note: The setup program creates administrator accounts for Apache Tomcat and PostgreSQL. The user name for the Apache Tomcat administrator account is `admin`. The PostgreSQL administrator account is a Windows account, and the user name is `postgres`. The password for both of these accounts is the password entered above.

8. Click **Next**.
9. Click **Install** to run the installation program.
10. In the **Active Directory Configuration** dialog, type an active directory user's login credentials, then click **OK**. Enter the user name and password of a normal user (i.e., a non-administrator) account that has rights to query the Active Directory. GO-Global uses this account to query the Active Directory for user and group information. This user name and password is stored in plain text on the gateway (in a directory that only members of the computer's Administrators group can access) to allow the gateway to query Active Directory. *Therefore, do not enter your own credentials or the credentials of the domain admin.* GraphOn recommends creating a special domain user with limited rights that is used *only* to search the domain.
11. Select the Organization Unit that contains the users and groups who will sign in to the gateway, then click **OK**. You can grant additional organizational units access to the gateway after installation. For more information, see [Granting Organizational Units Access to the Gateway](#).
12. Click **Finish** to exit the wizard.

To install the gateway on Linux

1. Import GraphOn's public key into your RPM database:
`rpm --import ftp://ftp.graphon.com/RPM-GPG-KEY-graphon`
2. Install the package as root:
 On Red Hat systems, type `yum install go-global_gateway-4.5.x-xxxx-linux-x86_64.rpm`
 On SUSE systems, type `zypper install go-global_gateway-4.5.x-xxxx-linux-x86_64.rpm`

On Linux, the installer does not automatically configure the gateway to use Active Directory. Configuring the gateway for Active Directory must be performed immediately following the installation of the gateway software.

To configure the gateway for Active Directory

1. Stop the Tomcat server hosting GO-Global.
2. Edit `web.xml` (`/webapps/go-global/WEB-INF/web.xml`) and change the line:
`/WEB-INF/spring/security/form-authentication.xml`
 to
`/WEB-INF/spring/security/iwa-ldap-authentication.xml`

3. Update the service configuration file by locating `<tomcat_home>/webapps/go-global/WEB-INF/classes/service-beans.xml`. Rename the file to `service-beans.xml`.
4. Edit LDAP configuration as follows:

- a. Open the following file for editing:

```
<tomcat_home>/webapps/go-global/WEB-INF/spring/security/iwa-ldap-
authentication.xml
```

- b. Locate `<bean id="ldapContextSource">` and modify the following to match your LDAP server location and login credentials. The user account name specified below can be the name of any user account that has rights to search the directory. Generally, it should be a normal user account, i.e., not an administrator account.

```
<constructor-arg value="ldap://[domain server address]:[domain server
port (e.g., 389)]/dc=[domain name],dc=[domain suffix (e.g., com)]"/>
  <property name="managerDn">
    <value>domain\username</value>
  </property>
  <property name="managerPassword">
    <value>password for above user account</value>
  </property>
```

- c. Determine the number of organizational units (OU) that the user search should query. By default, the LDAP configuration file is configured with two OU search beans, `ldapOUSearch1` and `ldapOUSearch2`. Copy or cut the OU search bean definitions to add or remove OU search definitions. Modify the first constructor argument of each search bean to specify the OU to search:

```
<constructor-arg index="0">
  <value>ou=HomeOffice</value>
</constructor-arg>
```

- d. Edit the `multiOUUserSearch` bean list to match the number of OU search beans configured in the previous step. By default, the `searchFilterList` list contains references to `ldapOUSearch1` and `ldapOUSearch2`.

```
<bean id="multiOUUserSearch"
class="com.graphon.goglobal.security.spring.MultipleOUUserSearch">
  <property name="searchFilterList">
    <list>
      <ref bean="ldapOUSearch1"/>
      <ref bean="ldapOUSearch2"/>
    </list>
  </property>
</bean>
```

- e. Find bean `<bean id="ldapAuthoritiesPopulator">` and modify the value to contain the LDAP user or group designated as the gateway administrator.

```
<list>
  <value>CN=Universal,CN=Users,DC=goglob4,DC=com</value>
</list>
```

- f. If a user's gateway password will include one or more characters from a foreign character set, locate and uncomment the following line:

```
<!-- <property name="passwordCharset" value="ISO-8859-1"/> -->
```

Set the value to the desired character set, for example:

```
ISO-8859-6 (Arabic)
ISO-8859-7 (Greek)
ISO-8859-8 (Hebrew)
ISO-8859-9 (Turkish)
```

5. Restart the gateway.

If you are using Active Directory, the **ADSI Edit** utility can help administrators determine the proper strings to enter above. ADSI Edit (`Adsiedit.msc`) is an MMC snap-in. You can add the snap-in to any `.msc` file through the **Add/Remove Snap-in** menu option in MMC, or just open the `Adsiedit.msc` file from Windows Explorer.

If you are running ADSI Edit on a computer that is not logged on to a domain or if you want to create a customized MMC, you may want to add the ADSI Edit snap-in to the console.

To add the ADSI Edit Snap-in to MMC

1. Open your existing console or create a new console. To create a new console, click Start, click Run, type `mmc`, and click OK, or at a command line, type `mmc`, and then press ENTER.
2. Click **Add/Remove Snap-in**, and then click **Add**.
3. In the **Add Standalone Snap-in** dialog box, click **ADSI Edit** in the list.
4. Click **Add**, then click **Close**.
5. Click **OK**.

For more information, see the following article: <http://technet.microsoft.com/en-us/library/cc773354%28WS.10%29.aspx>

When using this utility, administrators must take care to not make any modifications to the directory.

GRANTING ORGANIZATIONAL UNITS ACCESS TO THE GATEWAY

The GO-Global Gateway installer grants one organizational unit access to the gateway. Administrators can grant additional organizational units access to the gateway by editing the `iwa-ldap-authentication.xml` file.

1. Stop the **GO-Global Gateway** service.
2. Click Start | All Programs | Accessories | WordPad | Run as administrator.
3. Open
`\Program Files\GraphOn\GO-Global\Tomcat\webapps\go-global\WEB-INF\spring\security\iwa-ldap-authentication.xml`
4. Search for "ldapOUsearch1".
5. Add a value to the list for the OU you are adding. This value does not need to be the name of the OU. For example, you can name it "ldapOUsearch2".

After this step, the list should appear as follows:

```
<property name="searchFilterList">
  <list>
    <ref bean="ldapOUsearch1"/>
    <ref bean="ldapOUsearch2"/>
  </list>
</property>
```

6. Copy the specification for `ldapOUsearch1` (everything between `<bean id="ldapOUsearch1" ...` and `/bean>`).
7. Paste a copy of this structure below the specification for `ldapOUsearch1`.
8. Change the bean id to "ldapOUsearch2".
9. Change the value following `constructor-arg index="0"` to the distinguished name (without the base DN) of the OU that you are granting access to the gateway. When you are done with this step, the new entry should appear as follows:

```
<bean id="ldapOUsearch2"
class="org.springframework.security.ldap.search.FilterBasedLdapUserSearch">
  <!-- The base query below (first arg) must omit the parts
  specified in the connection string (ie. dc=goglob4.com,dc=com) -->
  <constructor-arg index="0">
    <value>>[distinguished name of your OU without that base DN,
e.g., OU=Gateway]</value>
  </constructor-arg>
  <constructor-arg index="1">
    <value>(sAMAccountName={0})</value>
  </constructor-arg>
  <constructor-arg index="2">
    <ref local="ldapContextSource"/>
  </constructor-arg>
  <property name="searchSubtree">
    <value>>true</value>
  </property>
</bean>
```


10. Search for “ouSearchList”.
11. Add a value to the list with the distinguished name of your OU without the base DN. For example, if the OU is named Gateway, the new entry should appear as follows:

```
<property name="ouSearchList">
  <list>
    <value>OU=OU1</value>
    <value>OU=Gateway</value>
  </list>
</property>
```

12. Optionally repeat steps 4-11 to add additional OUs.
13. Save the file.
14. Restart the Gateway service.

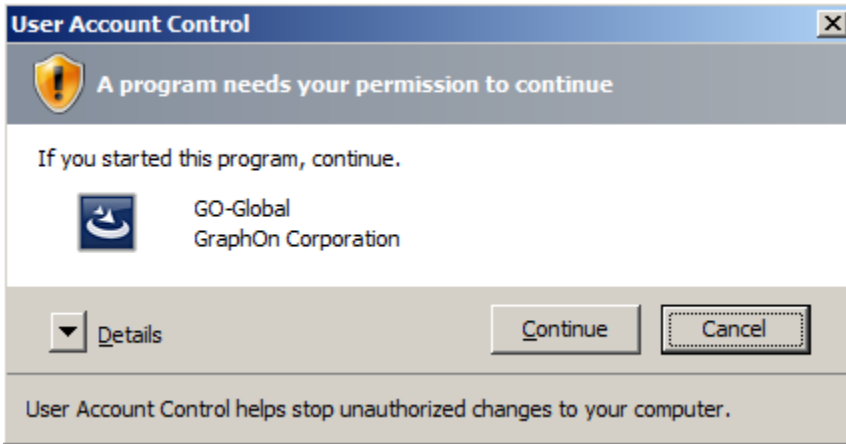
INSTALLING THE HOST

The host can be installed on the same computer as the gateway, or on a separate computer. The host setup program installs the GO-Global Host, ActiveX Control, and Firefox Plug-in, and optionally installs the GO-Global Gateway Connector, the Gateway Client, and Adobe AIR.

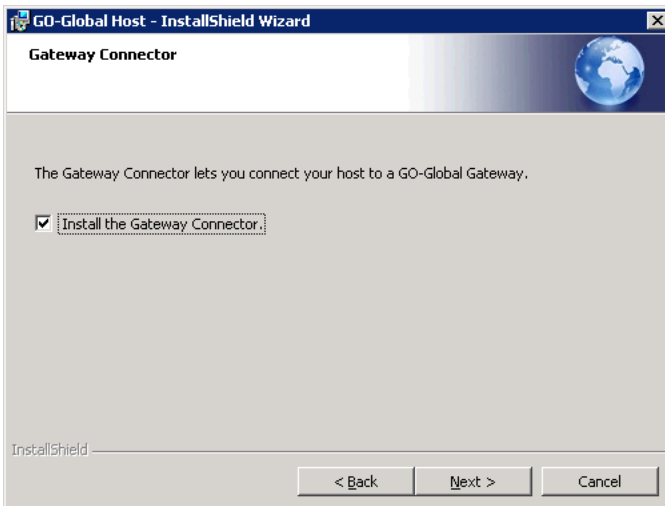
IMPORTANT: When running the host setup program, you must be logged in to the computer as “administrator” (i.e., under the computer’s local administrator account). It is not sufficient to be logged in to an account that is a member of the computer’s **Administrators** group; you must be logged in as the local administrator (**[computer name]\administrator**).

To install the host

1. Run the host setup program. On 32-bit systems, run **gg-host.windows_x86.exe**; on 64-bit systems, run **gg-host.windows_x64.exe**.
2. If the following **User Account Control** dialog is displayed, you are not logged in to the computer as the local administrator. Click **Cancel**, log out of the computer, and log back in as the local administrator.

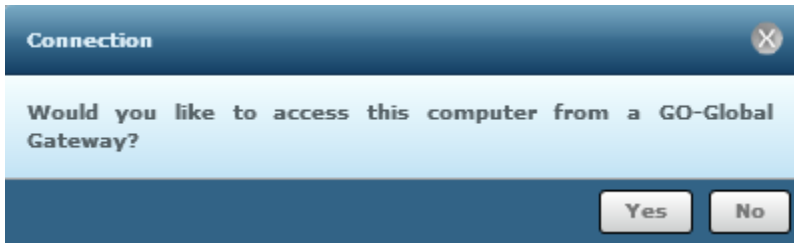


3. In the **InstallShield Wizard** dialog, click **Next**.
4. Accept the terms in the license agreement and click **Next**.
5. Click **Install the Gateway Connector** and click **Next**.



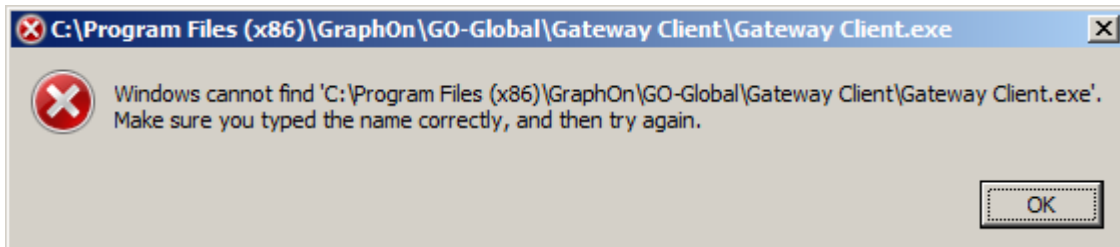
6. Note the destination folder and click **Next**.
7. Click **Install** to begin the installation.
8. If a message appears cautioning that the GO-Global Display Driver has not passed Windows Logo testing, it is safe to ignore. Click **Continue Anyway**.
9. The setup includes a **License Retrieval Wizard** which will automatically retrieve and install a license for GO-Global if there is no existing license. If you already have a valid license, the License Retrieval Wizard will not launch. You will need the Product Code supplied by your GraphOn sales representative in order to complete the License Setup. The License Retrieval Wizard will copy the license to the Programs directory. After typing the Product code, click **Next**.
10. Review the license agreement and click **I accept**.

11. Complete the User Information and click **Next**.
12. Click **Next** to install the license.
13. Click **Close** to exit the license setup.
14. Click **Finish**.
15. Click **Yes** to restart the computer.
16. When the computer restarts, the GO-Global Gateway Connector will start automatically and display the following message:



17. Click **Yes** and follow the steps described below to connect the host to the gateway.

If at step 16, the following message is displayed, it is likely that you are not logged in to the computer as the local administrator. If this occurs, you can work around the issue by manually starting the Gateway Connector.



To manually start the Gateway Connector

1. Click **OK** to the above message.
2. Click Start | All Programs | GraphOn GO-Global 4 | Tools | Gateway Connector | Run as administrator.
3. Run the host setup program. On 32-bit systems, run **gg-host.windows_x86.exe**; on 64-bit systems, run **gg-host.windows_x64.exe**.
4. In the **User Account Control** dialog, click **Continue**.

If you do not have a Product Code and wish to obtain a temporary demo license, please go to the following web page: <http://marketing.graphon.com/what-to-try.html>.

CONNECTING THE HOST TO THE GATEWAY

When you run the host setup program as described in the previous section and check the **Install the Gateway Connector** option, the setup program installs the Gateway Connector and starts it automatically when the computer restarts at the end of the setup process.

If you did not opt to install the Gateway Connector when you ran the host setup program, you can install the Gateway Connector at a later time via the host setup program's **Modify** option:

To add the Gateway Connector to a computer that already has the host installed

1. Run the host setup program. On 32-bit systems run, **gg-host.windows_x86.exe**; on 64-bit systems, run **gg-host.windows_x64.exe**.
2. In the **InstallShield Wizard** dialog, click **Next**.
3. Click **Modify**. Click **Next**.
4. Click **Install the Gateway Connector**. Click **Next**.
5. Click **Install**.
6. Click **Finish**.
7. Click **Yes** to restart the computer.

The gateway setup program automatically grants members of the **Domain Admins** group the right to administer the gateway. If you are not a member of the Domain Admins group, but you are a member of the **Administrators** group on the computer on which the gateway is installed, you can manually grant yourself the right to administer the gateway.

To add gateway administrators

1. Click Start | All Programs | Accessories | WordPad | Run as administrator.
2. If the **User Account Control** dialog is displayed, click **Continue**.
3. Browse to \Program Files\GraphOn\GO-Global\Tomcat\webapps\go-global\WEB_INF\spring\security.
4. In the **File name** text box, type *.*. Press the **Enter** key.
5. Open **iwa-ldap-authentication.xml**.
6. Search for "Domain Admins."
7. Insert a new value after the Domain Admins value with the distinguished name of your user account. When you are done, there should be two values. For example,

```
<value>CN=Domain Admins,CN=Users,DC=[yourdomainname],DC=[com]</value>
<value>CN=[yourusername],CN=Users,DC=[yourdomainname],DC=[com]</value>
```

Note that the distinguished name of your user account may have a different structure than the distinguished name in the example. You can obtain the distinguished name of user and group accounts in your domain using a tool such as ADSI Edit. (<http://technet.microsoft.com/en-us/library/cc773354%28ws.10%29.aspx>).

8. Click **File | Save**.
9. Restart the **GO-Global Gateway** service.

To connect a host to the gateway

1. At the end of the host setup process, when the Gateway Connector opens after restarting the computer, click **Yes** to connect the host to a gateway. Alternatively, if you are connecting a host to a gateway at a later time, run the Gateway Connector from the **Start** menu:
 - On Windows Server 2003, click Start | All Programs | GraphOn GO-Global 4 | Tools | Gateway Connector.
 - On Windows Server 2008, click Start | All Programs | GraphOn GO-Global 4 | Tools | Gateway Connector | Run as administrator.
2. If the **User Account Control** dialog is displayed, click **Continue**.
3. In the **Connection** dialog, type the network address (e.g., wilson.graphon.com) of the gateway you are connecting to in the **Address** box. Click **Connect**.
4. In the **Sign in** dialog, type the user name and password of a gateway administrator. This may be an account that is a member of the Domain Admins group, or an account that you added to the iwa-ldap-authentication.xml file described above. Click **Sign In**.
5. In the **Name Your Computer** dialog, type a name for the computer in the **Name** box. This name is displayed in the gateway. Type the computer's hostname (e.g., wilson.graphon.com) in the **Address** box. The full domain address is required when the gateway and host are on different domains.
6. Click **Ok**. An icon for the host will appear in the window. Initially, the icon is gray, indicating that the host is offline. Within about 30 seconds, the icon will turn blue, indicating that it is now online and can be accessed from GO-Global Gateway.

In addition to the icon for the host, an icon for the domain should also be displayed. If there is no icon for the domain, you are either not signed in to the gateway as a gateway administrator or there is a problem with the specification of gateway administrators in the iwa-ldap-authentication.xml file. Review the section above that describes how to add gateway administrators, then verify the configuration in the iwa-ldap-authentication.xml file.

PUBLISHING APPLICATIONS

Applications can be published to specific users and groups.

To publish applications to users and groups

1. If you are not already signed in to GO-Global Gateway, click Start | All Programs | GraphOn GO-Global 4 | GO-Global Gateway and sign in using the same account you used to connect the host to the gateway. Alternatively, start a web browser, browse to [http://\[gateway address\]:8080/go-global](http://[gateway address]:8080/go-global), and sign in.
2. Double-click the host computer.
3. If the application you want to publish is not displayed, create a new shortcut:
 - a. Click the **Add** button.
 - b. Click **Browse**. The programs available on the host's Start menu will be displayed.
 - c. Select a program.
 - d. Click **Select**.
 - e. Type the name of the program into the **Name** edit box.
 - f. Click **Create**.
4. Click the **Toggle navigation pane** on the toolbar to display the **Navigation Pane** on the left side of the window.
5. Drag the application shortcut you created from the main window and drop it on **Home** in the **Navigation Pane**.
6. Click **Home**.
7. Select the application's icon.
8. Click **Edit Properties**.
9. Click the **Security** tab.
10. From the list on the left, select the user(s) and/or group(s) you would like to grant access to. Search for users or groups by typing all or part of the group or user's name in the Search box, then clicking the **Search** button.
11. Select the users/groups, and click **Add**.
12. Optionally, repeat steps 10 and 11 to add additional users/groups.
13. Click **Save**.

Alternatively, you can publish applications to groups via simple drag-and-drop.

To publish applications to groups via drag-and-drop

1. Click the **Toggle navigation pane** button on the toolbar.
2. Expand the domain node in the Navigation Pane to view groups.
3. Drag an application shortcut from the main window and drop it onto a group in the Navigation Pane. You can only publish applications to groups; you cannot publish them to organizational units. If you try to drop an application on an organizational unit, a red X will be displayed.

With the above methods, the published applications are displayed to users when they sign in to the gateway. These methods provide a good way to publish multiple applications to a user. If, however, you simply want to share a single application or document with a user, you can do this using the **Share** feature.

To share a specific application or document

1. Sign in to the gateway.
2. Select an application or document. You can select a link to an application or document on the home page, a shortcut to an application or document under a host, or a document under a host's Files folder.
3. Click the **Share** button on the toolbar.
4. From the **Share** dialog, click the **Email** button to email the link or click the **Copy** button to copy it. Paste the link into an email message or instant message.
5. Send the email or instant message.

PUBLISHING HOSTS TO USERS

In addition to publishing applications and documents to users, you can publish hosts to users. You can do this, for example, when you want users to have access to all of the applications on a host.

To publish a host to users or groups

1. Sign in to the gateway as a gateway administrator.
2. Double-click the host to start a session.
3. Click the **Toggle navigation pane** button on the toolbar.
4. Select the host from the Content Pane or the Navigation Pane.
5. Click the **Edit Properties** button on the toolbar.
6. Click the **Security** tab.
7. From the list on the left, select the user(s) and/or group(s) you would like to grant access to. Search for users or groups by typing all or part of the group or user's name in the Search box, then clicking the **Search** button.
8. Select the users/groups, and click **Add**.
9. Click **Save**.

When an authorized user signs in to the gateway, the host will be displayed and the user can connect to the host by double-clicking it.

APPLICATION-BASED LOAD BALANCING

When an application is available on multiple hosts, administrators can create shortcuts to the application that will automatically start the application on the host with the lightest load. To do this administrators first publish the application to the home page from each host, as described above, and then group the shortcuts from each host into a single shortcut group. For example, to create a shortcut group that launches Notepad from one of two hosts:

1. Drag a Notepad shortcut from each host to the home page.
2. On the home page, select one of the Notepad shortcuts.

3. Click the **Edit Properties** button on the toolbar. The following dialog will be displayed.

The screenshot shows the 'Edit Published Item Group' dialog box. The 'Group Details' tab is selected. The 'Name' field contains 'Notepad'. The 'Available Items' table has one row with 'Notepad' and 'win2003r2-dev2'. The 'Grouped Items' table has one row with 'Notepad' and 'BILLT-THINKPAD'. There are 'Add' and 'Remove' buttons between the tables, and 'Save' and 'Cancel' buttons at the bottom right.

4. Select the Notepad item in the **Available Items** list.
5. Click **Add**.
6. If desired edit the **Name**.
7. Click the **Security** tab specify the users and groups that will have access to the item.
8. Click **Save**.

CLIENT INSTALLATION

Users can run GO-Global from any Adobe Flash-enabled browser without installing any GraphOn software, but in order to get the best performance and access to all of GO-Global's features, users should have the GO-Global Gateway Client installed on their computers. The client can be deployed in two ways: via the client setup program or via a Web browser's Add-on manager.

Administrators should deploy the client via the client setup program when users do not have sufficient rights to install browser Add-ons, or when users will be running GO-Global Gateway from a Windows desktop or Start Menu shortcut. Otherwise, if users have sufficient rights to install browser Add-ons or will be running GO-Global from Linux or Macintosh computers, administrators should deploy the client via the browser's Add-on manager.

To install via the client setup program

1. Sign on the computer as an administrator.
2. Run the client setup program, **gg-gateway-client.exe**. In addition to the Windows client, this setup program installs the ActiveX Control for Internet Explorer, the Plug-in for Mozilla Firefox,

- the GO-Global Update Client service, and Adobe AIR.
3. Accept the terms in the license agreement and click **Next**.
 4. Click **Install**.

By default, the client installs to C:\Program Files (x86)\GraphOn\GO-Global\. The ActiveX installs to Windows\Downloaded Program Files, and the Plug-in installs to Program Files\GraphOn\GO-Global.

The client can also be deployed using Group Policy Object. For more information, see the following article: <http://support.microsoft.com/kb/816102>.

To install via a Web browser's Add-on manager

1. If it is not already installed, install Adobe Flash Player.
2. In the Web browser's address field, type the address of the gateway.
(For example, <http://host.domain.com:8080/go-global>)
3. If **Install GO-Global Add-on** is displayed on the right-hand side of the title bar, optionally click it to boost performance, allow applications to run outside of the browser's windows, and for access to local printers and drives. (A browser restart is required.)
4. Follow the instructions to install the add-on for your browser and operating system.
5. Restart your browser.

With Internet Explorer, the ActiveX installs to Windows\Downloaded Program Files.

With Firefox on Windows, the Plug-in installs to %APPDATA%\Mozilla\Firefox\Profiles\profilename.default\extensions\support@graphon.com. On Linux, it installs to the user's plugins directory for whichever browser they used.

When users run GO-Global from a browser in which the GO-Global Add-on is not installed:

- Application performance will be slower.
- Applications will run embedded within a browser window.
- Users will not be able to access local devices (e.g., printers, drives, serial ports, etc.).

Sounds will not play on the client computer.

RUNNING APPLICATIONS

Users can run applications from browsers that have Adobe Flash installed, but users should install a GO-Global Add-on to get the best performance and to gain access to all of GO-Global's features.

Administrators can optionally distribute GO-Global Add-ons to Windows computers using group policy.

For more information, see the following article, <http://support.microsoft.com/kb/816102>.

To run GO-Global from a browser

1. Browse to [http://\[gateway address\]:8080/go-global](http://[gateway address]:8080/go-global).
2. Type the user name and password and click **Sign in**.
3. Click **Install GO-Global Add-on** on the right-hand side of the title bar to allow applications to run outside of the browser's windows, to access local printers and drives, and to maximize overall performance. (A browser restart is required after installing the Add-on.)
4. Double-click an application icon.

Users can also run GO-Global from the Windows Start menu.

To run GO-Global from the Windows Start menu

1. Install the client using the **gg-gateway-client.exe** setup program. This setup program installs the GO-Global client, ActiveX Control, Firefox Plug-in and Adobe AIR.
2. From the Start menu, click Start | Programs | GraphOn GO-Global 4 | GO-Global Gateway.
3. In the **Connection** dialog, type the name of the gateway into the **Address** box.
4. Click **Connect**.
5. Type the user name and password and click **Sign in**.
6. Double-click an application icon.

CREATING AND SEEDING THE MICROSOFT SQL SERVER 2008R2 DATABASE

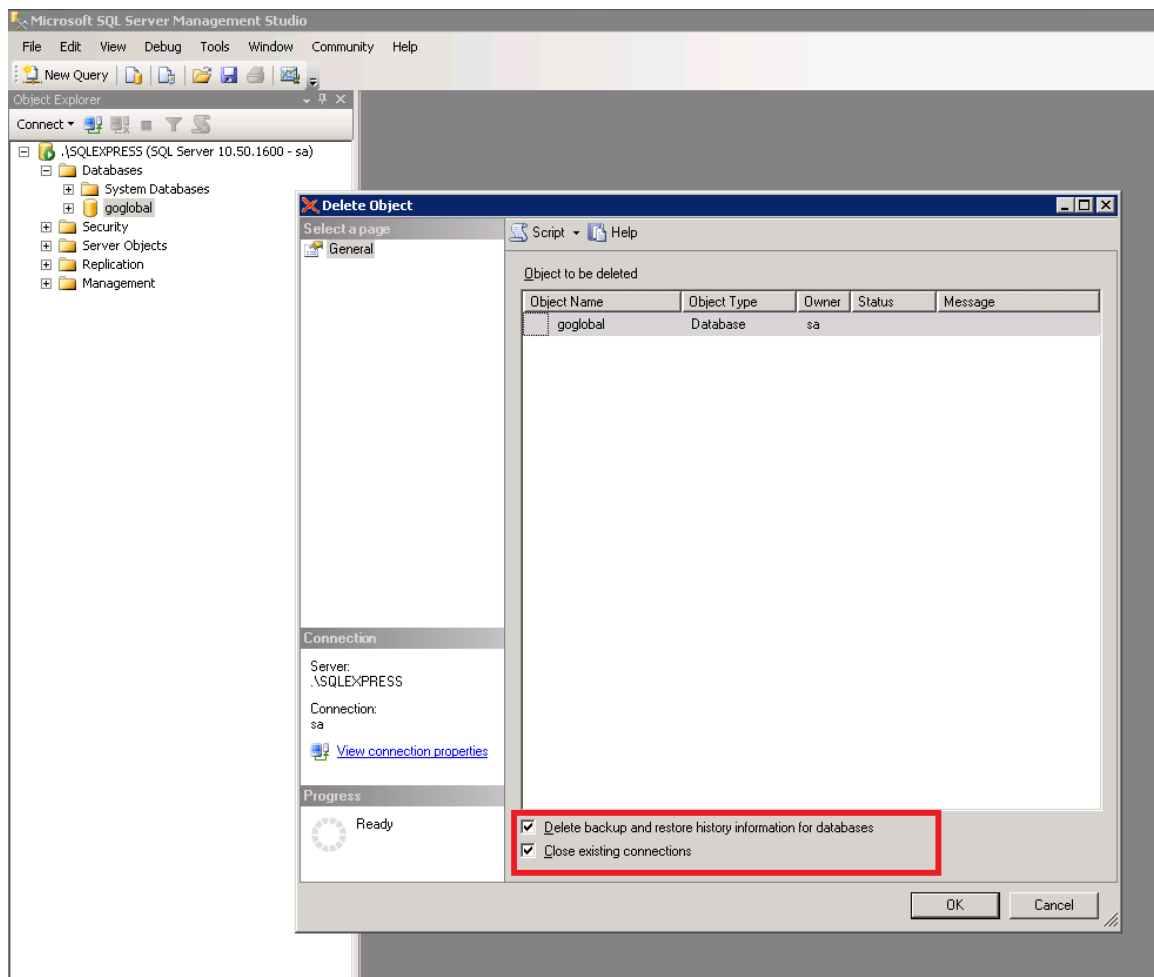
The following instructions are intended for organizations using Microsoft SQL Server 2008R2 as their gateway database.

Creating the database schema and subsequently seeding the database, requires the following:

- Microsoft SQL Server 2008R2
- Microsoft SQL Server Management Studio
- sqlserver-entities-schema.sql (as found in the gateway install directory)
- sql_server_seed_data.sql (as found in the gateway install directory)

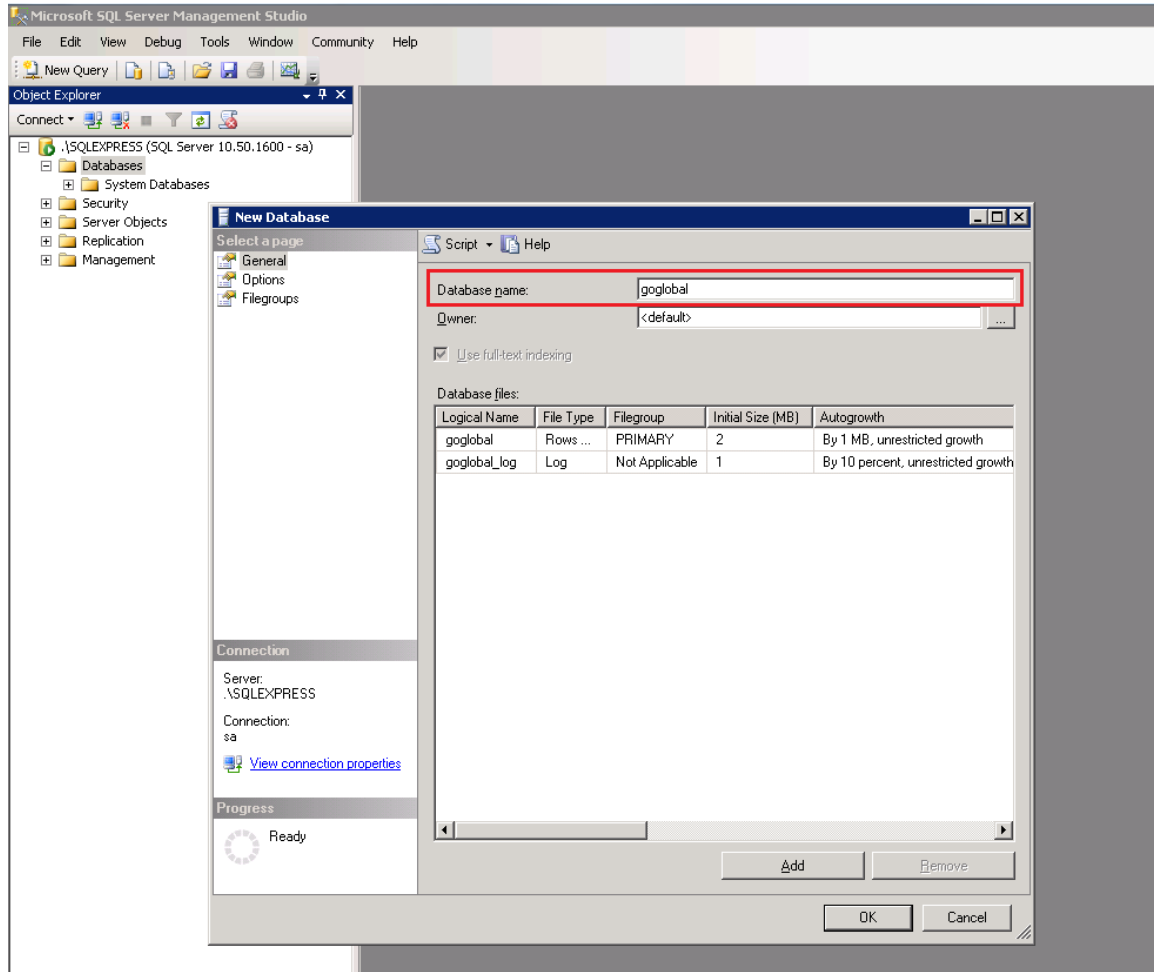
If a previous version of the GO-Global database already exists, the database must first be deleted, as follows:

1. Open Microsoft SQL Server Management Studio.
2. Selected the **goglobal** database.
3. Select **Delete** from the Edit menu.
4. Check both checkboxes at the bottom of the **Delete Object** dialog.
5. Click **Ok**.



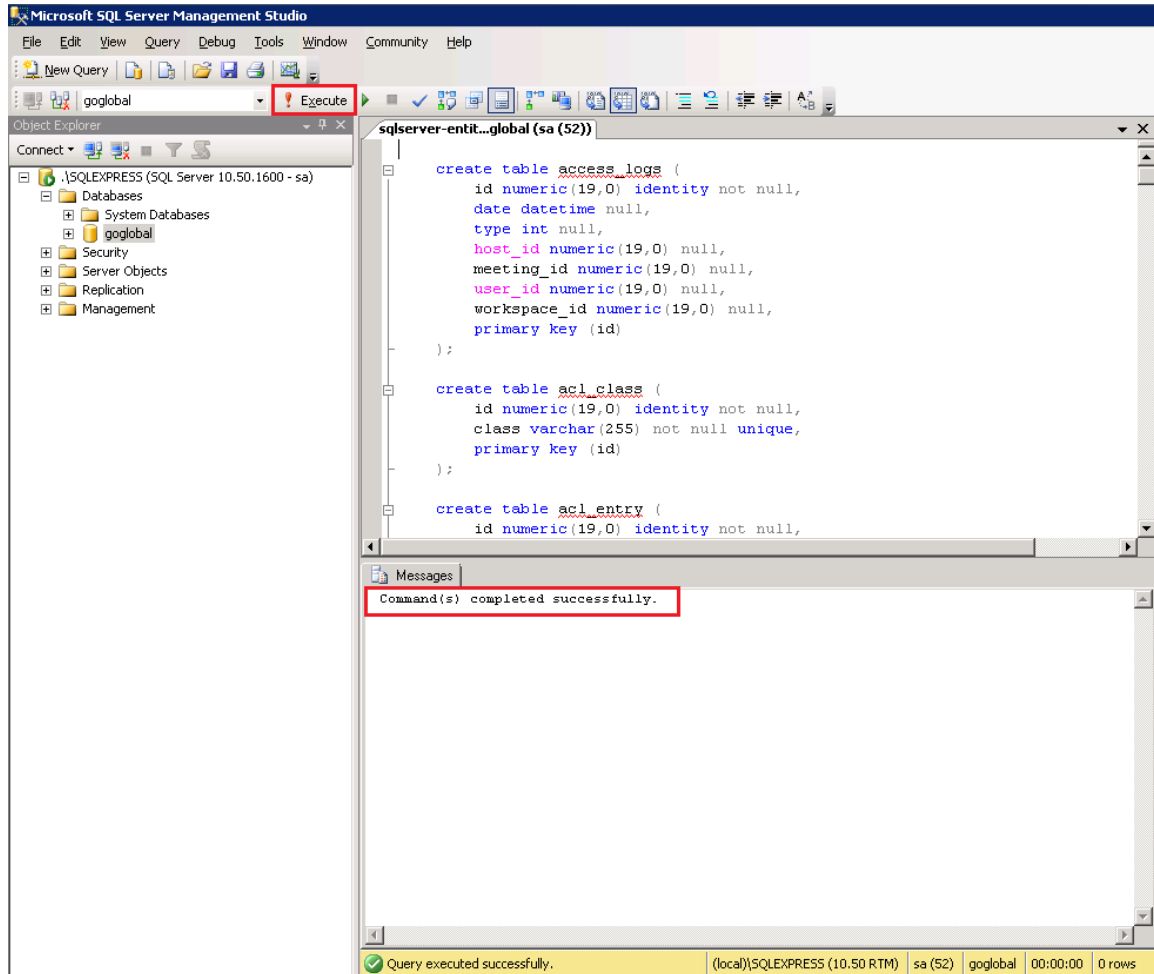
To create the database

1. Open Microsoft SQL Server Management Studio.
2. Right click the **Databases** node.
3. Select **New Database...** from the context menu.
4. Type **goglobal** as the Database Name.
5. Click **Ok**.



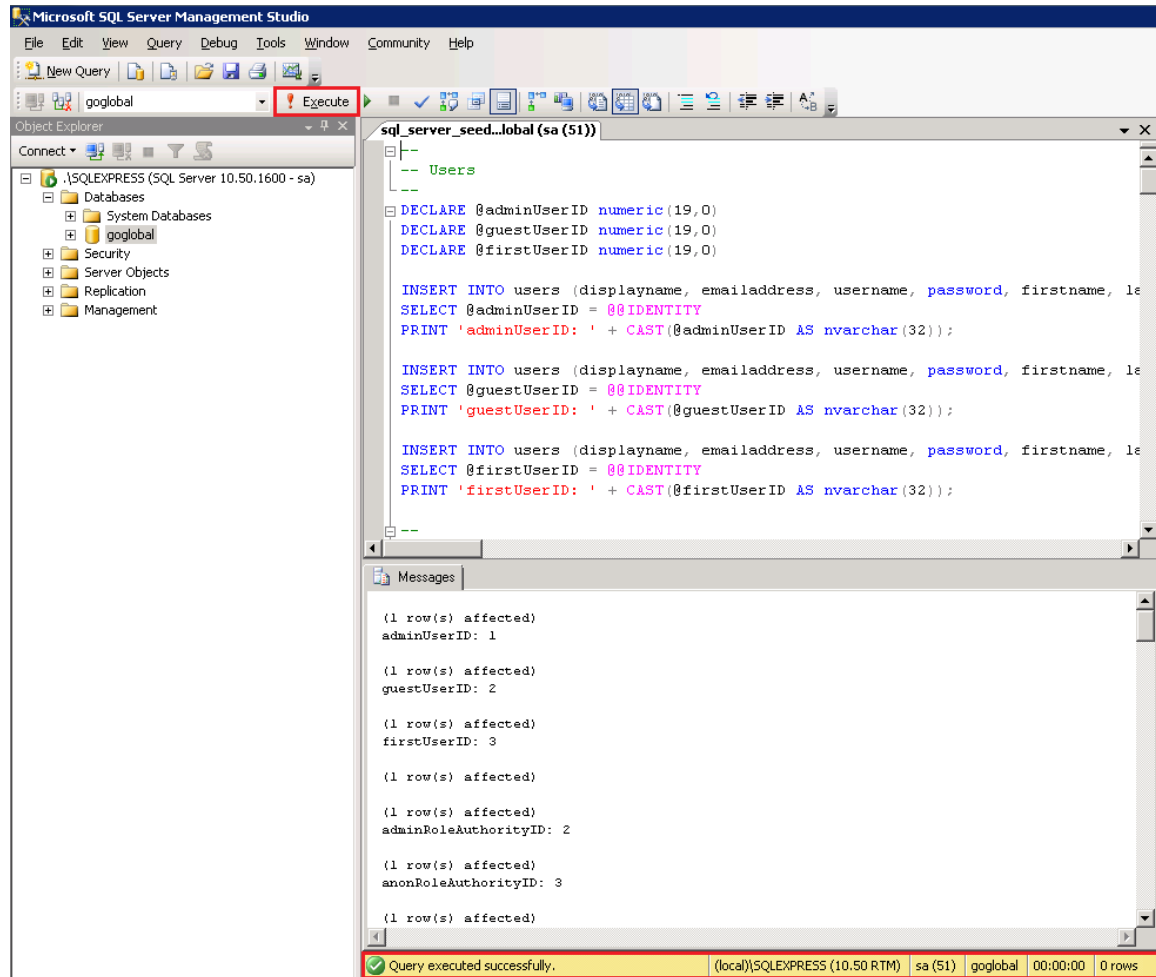
Create the database schema

1. Open Microsoft SQL Server Management Studio.
2. Selected the **goglobal** database.
3. Drag and drop the **sqlserver-entities-schema.sql** file onto the **goglobal** node.
4. Click the **Execute** button in the application toolbar.
5. Verify that the database schema was created, as shown in the **Messages** window.



Seed the database

1. Open Microsoft SQL Server Management Studio.
2. Selected the **goglobal** database node.
3. Drag and drop the **sql_server_seed_data.sql** file onto the **goglobal** node.
4. Click the **Execute** button in the application toolbar.
5. Verify that the database schema was created, as shown in the **Messages** window.



UNINSTALLING THE GATEWAY

To uninstall the gateway

1. Click Start | Control Panel | Programs and Features.
2. Select **GO-Global Gateway**.
3. Click **Uninstall**.
4. Restart the machine.

After restarting, delete the user "postgres" from **All Users** under **Documents and Settings**, and delete the user "postgres" from the **Users** folder under **Local Users and Groups** in **Computer Management**. Also, confirm that the contents of the GraphOn directory have been deleted.

On Windows Server 2003 this directory is located at: C:\Documents and Settings\All Users\Application Data\GraphOn. On Windows Server 2008, this directory is located at: C:\Users.

CHAPTER 3:

GATEWAY ADMINISTRATION

INTRODUCTION



The GO-Global Gateway is a Java-based Web application that provides a secure, programmable, high-availability gateway to Windows hosts. It can optionally authenticate users and ensure that only authorized users are allowed to connect to hosts.





GATEWAY NAVIGATION

When the **Toggle navigation pane** button is pressed on the toolbar, a tree view is displayed on the left. This is the **Navigation Pane**. It displays the computers, workspaces, and folders that the user is allowed to access. When a user selects an object in the Navigation Pane, the contents of the object are displayed in the Content Pane, which is the main area of the application.

The **Content Pane** displays the contents of whatever is selected in the Navigation Pane. To open an item in the Content Pane, double-click the item, or select the item and click **Open** on the toolbar.






Icons in the Navigation Pane are described in the table below:






	HOME	<i>The user's home page. Displays items that have been published to the user.</i>
	DOMAIN	<i>A domain is the collection of users, groups, and organizational units that are administered with a common set of rules and procedures. Each domain has a unique name. Click to display your designated Organizational Units and Groups.</i>

	ORGANIZATIONAL UNIT	<i>Active Directory objects which can contain users, groups, and other organizational units. An organizational unit cannot contain objects from other domains.</i>
	GROUP	<i>A group is a collection of user accounts that all have the same security rights.</i>
	COMPUTER ONLINE	<i>Online host computers registered on the gateway.</i>
	COMPUTER OFFLINE	<i>Host computer is registered on the gateway but is currently unavailable.</i>
	WORKSPACE RUNNING	<i>The user's workspace.</i>
	FILES FOLDER	<i>Contains files and folders. Click to view its contents in the Content Pane.</i>

GATEWAY TOOLBAR

Depending on what is selected in the Navigation Pane or Content Pane, the toolbar contains the following options:

	TOGGLE NAVIGATION PANE	<i>Opens and closes the Navigation Pane.</i>
	VIEWS	<i>Displays the following view options: Tiles and Details.</i>
	UP	<i>Moves the selection up one level in both the Navigation and Content Panes.</i>
	OPEN	<i>Opens whatever is highlighted in the Navigation or Content Pane.</i>
	ADD	<i>Allows users to add a shortcut.</i>
	EDIT PROPERTIES	<i>Opens the properties dialog box of the selected item.</i>
	DELETE	<i>Deletes the selected item (e.g., a folder.)</i>
	ADD FOLDER	<i>Creates a new folder.</i>
	COPY	<i>Copies a folder or file to the clipboard</i>

	PASTE	<i>Creates a copy of what is on the clipboard.</i>
	CUT	<i>Moves a file from one location to another.</i>
	SHARE	<i>Share a file, folder, or application with other users.</i>
	ALL PROGRAMS	<i>Provides a list of all the applications the user has access to (all the applications in the Windows All Programs menu.)</i>
	OPEN DESKTOP	<i>Opens the desktop environment of the computer in a separate window. On Windows computers, explorer.exe will start and display the Start menu, taskbar, desktop icons, etc.</i>
	CLOSE SESSION	<i>Signs the user out of the host and closes all of the applications running in the host session.</i>
	SUSPEND SESSION	<i>Suspends the user's session on the host. Applications continue running in the background for the time specified in the Time Limits tab of the Options dialog.</i>
	HELP	<i>Opens Help files for GO-Global.</i>

CHANGING VIEWS

You can change the view to display items in the Content Pane as **Tiles** or **Details**.

To change views

1. Click the **Views** button on the toolbar.
2. Select **Tiles** or **Details**.

The **Details** view displays information about each item in the window, such as file size, type, and the date the file was last modified. While viewing items in Details view, a column header is displayed below the toolbar. To adjust the width of the columns, point your mouse to the vertical separator and drag to the left or the right.

By clicking the column's title, you can change the order in which items appear in the Content Pane. For example, click the Size header to list either the smallest files or the largest files first. Click the column's title again to toggle back and forth.

DRAG AND DROP

GO-Global supports dragging and dropping items from one location to another. Items can be dragged from the Content Pane to a folder in the Navigation Pane. Holding the Control key down while dragging will copy the item to the new location. Workspaces and sessions can only be dropped in gateway folders; they cannot be dropped in host folders.

To drag and drop an item

1. Click the **Toggle navigation pane** button to view the Navigation Pane. Make sure the destination folder for the item you want to move is visible.
2. Select a file from the Content Pane.
3. To move the item, drag it to the destination folder. To copy the item instead of moving it, press and hold down CTRL while dragging.

To drag and drop multiple items

1. Click the **Toggle navigation pane** button to view the Navigation Pane. Make sure the destination folder for the item you want to move is visible.
2. Using the CTRL key, select two or more items from the Content Pane.
3. While pressing the CTRL key, drag the items to the destination folder.
4. Release the CTRL key, then release the mouse button.

To copy multiple items

1. Click the **Toggle navigation pane** button to view the Navigation Pane. Make sure the destination folder for the item you want to move is visible.
2. Using the CTRL key, select two or more items from the Content Pane.
3. While pressing the CTRL key, drag the items to the destination folder.
4. Release the CTRL key and the mouse button at the same time.

SHARING

Users can securely share document, files, and programs centrally, from hosts. Depending on their access rights, recipients can view and edit documents regardless of whether or not they have the correct application installed on their computers. Documents shared via GO-Global never have to leave the host, thereby protecting the sender's intellectual property.

Users can share a document or an application by sending a unique URL in an email or instant message.

To share a document

1. Select the document.
2. Click the **Share** button on the toolbar.
3. From the **Share** dialog, click the **Email** button to email the link or click the **Copy** button to copy it. Paste the link into an email message or instant message.
4. Send the email or instant message.

If a user shares a link to an item in the user's private workspace, the user will be able to access the item but other users will not.

WORKSPACES

A **workspace** is a directory on a host in which environmental settings, preferences, files, and links to applications are stored. On Windows computers, workspaces are user profiles. By default, the Workspace folder is the Desktop folder on Windows computers and the Home directory on UNIX and Linux.

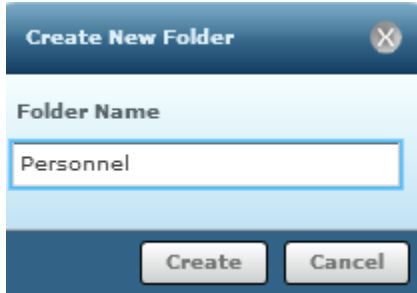
Each workspace has one user account that is granted full control over the workspace's files and directories. Users signed in to a workspace on a host are subject to the access restrictions of the workspace's user account. The operating system enforces access restrictions on files, programs, etc.

ADDING A FOLDER

The **Add Folder** button allows users to create new folders.

To add a folder

1. Select the workspace from the Navigation Pane.
2. Click the **Add Folder** button on the toolbar.
3. Type a name in the **Folder Name** box.
4. Click **Create**.



COPY, CUT, AND PASTE

The **Copy** button on the toolbar copies a folder or file to the clipboard. The **Cut** button moves the selected file to the clipboard. The **Paste** button creates a copy of what is on the clipboard.

To copy and paste a file

1. Select a file or folder from the Content Pane.
2. Click the **Copy** button.
3. Browse to the destination folder.
4. Click the **Paste** button.

To cut and paste a file

1. Select a file or folder from the Content Pane.
2. Click the **Cut** button.
3. Browse to the destination folder.
4. Click the **Paste** button.

OPENING ALL AVAILABLE PROGRAMS

By clicking the **Open Programs** button on the toolbar, users can view and open all the programs available in the selected workspace.

To open all programs

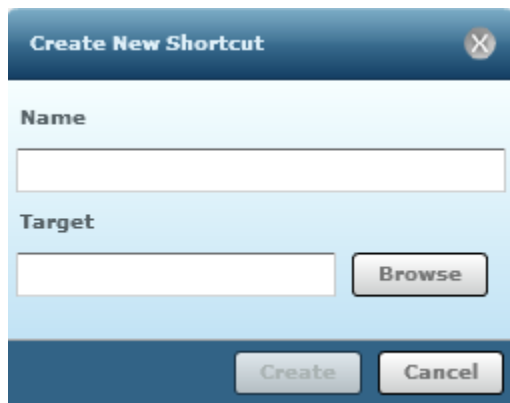
1. Select the workspace.
2. Click the **Open Programs** button on the toolbar.
3. Click the desired program to open it.

ADDING A SHORTCUT

Users can add a shortcut to a file or program to their workspace.

To add a shortcut

1. Select the workspace or a folder within the workspace.
2. Click the **Add** button on the toolbar.
3. In the **Create New Shortcut** dialog, type a name for the shortcut.
4. Click the **Browse** button to browse for the desired file or program.
5. Click **Select**.
6. Click **Create**.



OPENING THE DESKTOP OF A USER ACCOUNT

The toolbar's **Open desktop** button launches the desktop environment of the computer in a separate window. For example, on Windows computers, explorer.exe will launch and display the Start menu, taskbar, desktop icons, etc.

To open a desktop

1. Select the user account from the navigation pane.
2. Click the **Open desktop** button on the toolbar.

CLOSING A SESSION

After signing in to a host, users remain signed in until they either close the session or the session times out. When users navigate away from a workspace, they remain signed in to the workspace, and are able to navigate back to it without having to sign back in.

To close a session

1. Select a workspace or any folder under a workspace.
2. Click the **Close Session** button on the toolbar.

When a user clicks the **Close Session** button, each application running in the workspace session will be notified that it is going to be closed and will be given the opportunity to prompt the user to save modified files, etc. Thereafter, all applications will be closed, the connection to the client will be closed, and the user will be signed out.

SUSPENDING A HOST SESSION

Suspending a host session disconnects the user from the applications running within the session, but the applications continue running in the background for the time specified in the **Time Limits** tab of the **Options** dialog. If the session termination is set to **Immediately**, applications will not continue running in the background.

To take advantage of the suspend workspace feature, be sure the session termination option is set to Never or to a specified number of minutes. See [Setting the Session Termination Option](#) for more information.

To suspend a host session

1. Select the workspace or a folder under the workspace..
2. Click the **Suspend Session** button on the toolbar.
3. Click **Yes** in the confirmation dialog.

Note: A workspace or a folder within a workspace must be selected in order to suspend a session. If a host is selected, the **Suspend Session** button is not enabled.

SENDING MESSAGES

Host administrators can send messages to other users who are connected to the host.

To send a message to all users connected to a host

1. Select one or more hosts.
2. Click the **Send Message** button on the toolbar.
3. Type a message in the **Send Message** box.
4. Click the **Send** button.

Gateway administrators can send messages to all users who are signed in to a gateway.

To send a message to all users who are signed in to a gateway

1. Select **Home**.
2. Click the **Send Message** button on the toolbar.
3. Type a message in the **Send Message** box.
4. Click the **Send** button.

SESSION MANAGEMENT

When a user clicks **Manage sessions** in the lower-right corner, the Content Pane displays the sessions



running on the computer that the user is allowed to manage. The Sessions page allows administrators to shadow a session, terminate processes running in a session, and to terminate a session.

The Sessions page allows users and administrators to view the following information about a session:

- Session name
- Host name
- Workspace name
- User name of the session's owner
- Session ID



To return to the Content Page, click the **Show items** button in the lower-right corner.

SESSION PROPERTIES

Through the Session Properties dialog, administrators can view the following information about each **connection** to a session:

- Name of the user that established the connection
- Time established.
- IP address (machine name)
- Bytes sent
- Bytes received
- Client version number

Administrators can view the following information about **processes** running in a session:

- Process name
- Time the process was started
- Process ID (PID)
- CPU usage
- Memory usage

To view session properties

1. Click the **Manage sessions** button in the lower right corner of the Content pane.
2. Select a session.
3. Click the **Edit Properties** button on the toolbar.

ENDING PROCESSES

A process is any action taking place on a 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.

To end a process

1. Click the **Manage sessions** button in the lower right of the Content Pane.
2. Select a session.
3. Click the **Edit properties** button on the toolbar.
4. Select the process or processes you would like to end.
5. Click the X button on the right side of the process listing.

SHADOWING A SESSION

When a host administrator clicks **Manage sessions**, the Content Pane lists all sessions running on the host. With permission from the session's owner, the host administrator can access these sessions.

To shadow a session

1. Click the **Manage Sessions** button located in the bottom right of the Content Pane.
2. Select the session you would like to shadow.
3. Click the **Open** button on the toolbar.

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 communication failure.

DEFAULT HOST PROPERTIES

The gateway administrator can set default security properties for hosts through the **Gateway Properties** dialog. The default security properties are applied to new hosts that are registered with the gateway. Once a user edits the security properties of a host and saves the changes, the default properties no longer apply.

To edit the default host properties

1. Sign in to the gateway as admin.
2. Click the **Home** icon in the Navigation Pane.
3. Click the **Edit Properties** button on the toolbar.
4. Click the **Edit Default Host Properties** button, which opens the **Security** tab of the **Host Properties** dialog.
5. Set the defaults, as desired, and click **Save**.

ACCESS LOGS

Access to the gateway is recorded in the gateway's database. Access logs record when a user signs in and out of the gateway and when a host connects and disconnects from the gateway.

Access logs also record when a user signs in and out of the gateway, when a user starts and stops a process, and when a user opens and closes a file.

Access logs contain the following information:

- Date and time an item was accessed
- The name of the item that was accessed
- The name of the user or host that accessed the item
- A description of the access (e.g., sign in/sign out, connect/disconnect, etc.)

Administrators can use the information in Access logs to track when users access the gateway and its hosts. Access logs can be viewed and searched through the **Gateway Properties** dialog.

To filter the Access Logs

1. Sign in to the gateway as admin.
2. Click the **Home** icon in the Navigation Pane.
3. Click the **Edit Properties** icon on the toolbar.
4. Click the **Access Logs** tab.
5. Select a date range by clicking the calendar icons next to the **From** and **To** boxes.
6. Click **Search**.

Administrators can save the Access Logs in XML format. The XML file exports all the data displayed in the table.

To export Access Logs

1. Sign in to the gateway as admin.
2. Click the **Home** icon in the Navigation Pane.
3. Click the **Edit Properties** icon on the toolbar.
4. Click the **Access Logs** tab.
5. If desired, select a date range.
6. Click **Search**.
7. Click **Export Logs**.
8. Open or save the .xml file.

GATEWAY LOG OUTPUT

GO-Global offers six gateway log output levels, from greatest to least log output, as follows:

TRACE
DEBUG
INFO
WARN
ERROR
FATAL

By default, the gateway only outputs WARN and ERROR level messages. Please note that using INFO, DEBUG, or TRACE levels will significantly increase the size of the log file and potentially impact gateway performance.

To increase or decrease the log output on Windows

1. Stop the **GO-Global Gateway** service.
2. Locate C:\Program Files\GraphOn\GO-Global\Tomcat\webapps\go-global\WEB-INF\classes\log4j.properties.
3. Change the log level value for the root logger in this line:
log4j.rootCategory=WARN, CONSOLE, LOGFILE
from WARN to one of the log levels listed above.
4. Save log4j.properties.
5. Restart the **GO-Global Gateway** service.

To increase or decrease the log output on Linux

1. Stop the **gg-gateway-server** service.
2. Locate /usr/local/graphon/tomcat/webapps/go-global/log4j.properties.
3. Change the log level value for the root logger in this line:
log4j.rootCategory=WARN, CONSOLE, LOGFILE
from WARN to one of the log levels listed above.
4. Save log4j.properties.
5. Restart the **gg-gateway-server** service.

CHAPTER 4: HOST ADMINISTRATION

ADMINISTERING A HOST

To administer a host, a user must be a member of the host computer's Administrators group.

To edit the properties of a host

1. Double-click the host to connect to the host.
2. Select the host in the Navigation Pane or Content Pane.
3. Click **Edit Properties** on the toolbar.
4. Modify the host's properties.
5. Click **Save**.

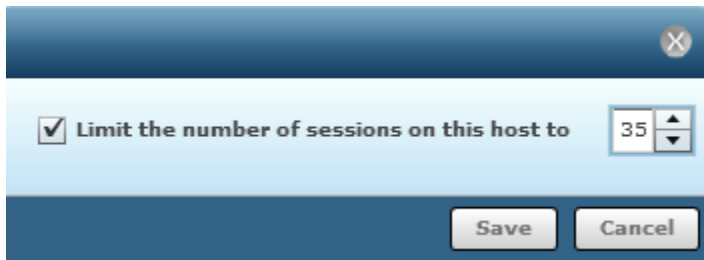
When the user is a host administrator, the status bar displays the following information about the host computer:

- Memory usage
- CPU usage

Administrators can limit the number of sessions allowed on a host via the gateway by clicking the **Edit** button *before signing in*. By default, there is no limit on the number of sessions. Administrators should adjust this value to one that is appropriate for the capacity of the host.

To limit the number of sessions that can be started on the host from the gateway

1. Before signing in, select the host.
2. Click the **Edit Properties** on the toolbar.
3. Enable **Limit the number of sessions on this host to __**.
4. Type the maximum number of sessions per user in the edit 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 **Save**.



SETTING THE MAXIMUM NUMBER OF SESSIONS

Alternatively, administrators can configure the host to limit the *total* number of sessions allowed on the host, which includes sessions started from a gateway and sessions started from clients connecting directly to the host. The session limit is set to 50 by default. Administrators should adjust this value to one that is appropriate for the capacity of the host.

To set the maximum number of total sessions per host

1. Sign in to the gateway as a host administrator.
2. Select the host.
3. Click the **Edit Properties** button on the toolbar.
4. Type the desired **Maximum number of sessions**.
5. Click **Save**.

APPLYING GROUP POLICY

GO-Global supports Microsoft's Group Policy. If a host is a member of a domain, Group Policy can optionally be applied when users sign in to gateways and hosts. Using Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options. For more information regarding this feature, go to:

<http://www.microsoft.com/windowsserver2003/techinfo/overview/gpintro.mspx>.

Group Policy is supported on Windows only and is disabled by default.

To apply group policy

1. Sign in to the gateway as a host administrator.
2. Select the host.
3. Click the **Edit Properties** button.
4. On the **General** tab, select **Apply Group Policy**.
5. Click **Save**.

CLIENT UPDATES

When the client is deployed via a browser's Add-on manager, the browser will automatically upgrade the client when users access a gateway that has a newer version of the client, as long as the user has sufficient rights to install browser Add-ons.

Alternatively, when the client is deployed using the client setup program, administrators can configure GO-Global Gateway to automatically upgrade the client using the GO-Global Update Client service.

To enable automatic client updates

2. Select the host and click the **Edit Properties** button on the toolbar.
3. In the **Host Properties** dialog, enable **Automatically update clients**.
4. Click **Save**.

When **Automatically update clients** is selected in the Host Properties dialog and a user signs in to the host from a Windows computer, GO-Global compares the version of the GO-Global software installed on the computer to the version in the Updates directory on the Host. If the files in the Updates directory are newer, GO-Global copies the newer files to a temporary directory on the client computer. Then, when the client closes, the **GO-Global Update Client** service installs the new files so they can be used in subsequent sessions.

In summary, new client software will be installed when the following conditions are met:

- **Automatically update clients** is enabled.
- The **GO-Global Update Client** service is installed and enabled on the client computer.
- A newer version of the client is available in the Updates directory on the host.
- All of the files in the new version have been downloaded to the client computer.
- The user has closed the client.

Users are not required to perform any upgrade tasks. They can, however, prevent updates from being installed by disabling the GO-Global Update Client service on the client computer.

To disable the GO-Global Update Client service

1. Right-click **My Computer**.
2. Click **Manage**.
3. Click Computer Management | Services and Applications | Services.
4. Select **GO-Global Update Client**.
5. Click **Properties**.
6. Under **Startup type**, select **Disabled**.

7. Click **Stop**.
8. Click **OK**.

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

SECURITY

GRANTING ACCESS TO A HOST

For a user to see a host listed in the gateway, the administrator must grant that user access to the host.

To grant a user access to a host

1. Sign in to the gateway as a domain administrator (i.e., using an account that is a member of the Domain Admins group). The host computer must be a member of the domain, and the Domain Admins group must be a member of the host computer's Administrators group.
2. Click the **Toggle navigation pane** on the toolbar.
3. Double-click the host to start a session.
4. Select the host from the Content Pane or the Navigation Pane.
5. Click the **Edit Properties** button on the toolbar.
6. Click the **Security** tab.
7. From the list on the left, select the user(s) and/or group(s) you would like to grant access to. Search for users or groups by typing all or part of the group or user's name in the **Search** box, then clicking the **Search** button.
8. Select the user, and click **Add**.
9. Click **Save**.

When an authorized user signs in to the gateway, the host will be listed.

CONNECTIONS

GO-Global provides support for both Transmission Control Protocol (TCP) and Secure Socket Layer (SSL) as methods for communication between clients and hosts.

SELECTING SSL TRANSPORT

When selecting the SSL transport, an SSL Certificate file must be specified. SSL certificates are required to secure communication between clients and hosts. 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 SSL certificates are also supported.

To select SSL Transport

1. Sign in to the gateway as a host administrator.
2. Select the host.
3. Click the **Edit Properties** button on the toolbar.
4. Click the **Advanced** tab.
5. In the **Transport** list, click **SSL**.
6. Type or browse to the path of the server's certificate file in the **SSL Certificate** box.
7. Click **Save**.

The screenshot shows the 'Host Properties' dialog box with the 'Security' tab selected. The 'Connections' section is active, showing the following configuration:

- Transport:** TCP (dropdown menu)
- Port:** 491 (text input)
- Encryption:** 56-bit DES (dropdown menu)
- SSL Certificate:** [Empty text box] [Browse button (...)]
- Notify users when connections are secure

At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

OBTAINING A TRUSTED SERVER CERTIFICATE

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).

To generate a CSR

1. Download **OpenSSL** from <http://www.openssl.org/related/binaries.html>. (Please note that you must install the *full* version of OpenSSL: Win32OpenSSL-v0.9.8a.exe.)
2. Install **OpenSSL** on the host.
3. Click Start | Run.
4. Type **cmd**, and press **Enter**.
5. Type the following command to generate a private key for the server:

```
[OPENSSL_DIR]\bin\openssl genrsa -out server.key 1024
```

 where `OPENSSL_DIR` is the path to the directory in which OpenSSL is installed (e.g., `C:\OpenSSL`).
6. Type the following command:

```
[OPENSSL_DIR]\bin\openssl req -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 e-mail address

Unless you are using a wildcard SSL Certificate, the Common Name *must* match the host name of the GO-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 SSL implementation is based on the OpenSSL toolkit, the tools used 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, save it as **server.crt**. Copy this file and the **server.key** file (generated in step 5 above) to a directory on the host that can be accessed from the System account and accounts that belong to the Administrator group but that cannot be accessed from normal user accounts. Finally, select the signed certificate file in the Host Properties dialog, as described below.

To select the server certificate

1. Sign in to the gateway as a host administrator.
2. Select the host.
3. Click the **Edit Properties** button on the toolbar.
4. Click the **Advanced** tab.
5. From the **Transport** list, click **SSL**.
6. Type or browse to the path of the server's certificate file in the **SSL Certificate** box.
7. Click **Save**.

USING AN INTERMEDIARY SSL CERTIFICATE

When using an intermediary SSL certificate, you must concatenate your existing certificate with the intermediary certificate. The following example uses the Go Daddy intermediary certificate.

1. Take the .crt and .key files that are being used on the host.
2. Download the Go Daddy intermediary certificate (e.g., GODaddyCA.crt). This should have come with the original certificate purchase but can also be located at the following Go Daddy site: <https://certs.godaddy.com/Repository.go>
3. Concatenate your .crt and the intermediary .crt file. (Combine them into a third file as follows: copy 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 host (e.g., c:\Data).
6. Sign in to the host using an administrator account.
7. Select the host and click the **Edit Properties** button on the toolbar.
8. Click the **Advanced** tab.
9. Change the transport to SSL and increase the encryption level to 256-bit AES, if you have a high-encryption license. If not, leave it at 56-bit.
10. Browse to the SSL 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.
11. Enable **Notify users when connections are secure** for testing purposes.
12. Click **Save**.
13. Sign in to the host from a different system.

CREATING YOUR OWN CERTIFICATE AUTHORITY

Sites with many hosts can create their own certificate authority, then sign each server's certificate from this authority and install the certificate authority certificates onto each client. This will prevent any warnings about untrusted authorities, without requiring the site to obtain a third-party certificate for each server.

There are many third-party applications and systems to assist in the creation and maintenance of a certificate authority that interoperate with the OpenSSL toolkit. These tools should be able to generate signed server certificates for use with GO-Global without modification.

A certificate authority is a virtual organization that will sign each of your server keys, allowing the client to assert that the server keys are authentic and have not been tampered with.

To establish the certificate authority, a CA key and self-signed certificate must be created. Once the CA certificate and key are created, import the CA certificate on the client device via the Internet Options dialog. Finally, the server keys are signed using the CA certificate, which will allow the client machines to recognize the authenticity of the signatures and allow connections to the server without warning the user about the trustworthiness of the CA.

Note: Nine files are created during this process: ca.key, ca.csr, ca.crt, ca.cfg, ca.serial, server.cfg, server.key, server.crt, and server.csr.

IMPORTING THE TRUSTED SERVER CERTIFICATE ON A HOST

To import the trusted server certificate on a host, add a Policy in Microsoft Management Console. This is only required when using a self-generated certificate.

1. On the host, click Start | Run. Type **mmc** in the **Open** box. This will open Microsoft Management Console.
2. Click Console | Add/Remove Snap-in. Click **Add**.
3. Click **Certificates** from the list of **Available Standalone Snap-ins** and click **Add**.
4. Select Computer account in the **Certificate Snap-in** dialog. Click **Next**.
5. In the **Select Computer** dialog, select Local computer. Click **Finish**.
6. Close the **Add Standalone Snap-in** dialog.
7. Return to the **Add/Remove Snap-in** dialog and click **Certificates (Local Computer)**.
8. Click **Ok**.
9. Under **Console Root**, expand **Certificates**. Click **Trusted Root Certification Authorities**. From the right pane, right-click **Certificates**.
10. Select All Tasks | Import. Browse for the Certificate **ca.cert**.

The server key and certificate files (e.g., server.key and server.crt) must have the same base filename and be located in the same directory on the host. Hosts do not need SSL certificates, but their designated gateway must have a valid SSL certificate that is signed by a CA and that is recognized by the hosts.

CREATING A CA KEY AND CERTIFICATE

The first step to establishing a certificate authority (CA) is to generate an RSA private key. This key should be kept very secret, as any entity with access to this key can generate false certificates that would certify unknown hosts as trusted. It is vitally important to protect the integrity of your certificate authority. To generate the CA key, use the following command:

```
[OPENSSL_DIR]\bin\openssl genrsa -out ca.key 1024
```

This command will generate your initial CA key, and place it in the file ca.key. After the key is created, generate a Certificate Signing Request (CSR) that will be used to create the CA certificate. To generate the CSR, use the following command:

```
[OPENSSL_DIR]\bin\openssl req -new -key ca.key -out ca.csr
```

This command will run interactively and prompt you for the information to be contained in the certificate. Example responses are shown below:

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Washington
Locality Name (e.g., city) []:Bellevue
Organization Name (e.g., company) [Internet Widgits Pty Ltd]:GraphOn Corporation
Organizational Unit Name (e.g., section) []:GraphOn Corporation CA
Common Name (e.g., YOUR name) []:GraphOn Corporation CA
Email Address []:hostmaster@graphon.com
Please enter the following extra attributes to be sent with your certificate request:
A challenge password []:[enter]
An optional company name []:[enter]
```

The prompts should be answered as:

```
Country Name: your two-letter country abbreviation
State or Province Name: your full state or province name
Locality Name: your city or town or suburb name
Organization Name: the name of your organization or company
```


Organizational Unit Name: the organizational name should be a representation of your CA's name

Common Name: This should either be a person responsible for the operation of the CA or a generic name representing the CA itself

Email Address: This should be an e-mail address that can be used to address concerns about certificates to someone responsible for the CA

The final step is establishing the CA certificate. To do this, create a settings file that contains some information about the CA. The file should be named **ca.cfg** and should contain the following:

```
extensions = x509v3
[ x509v3 ]
subjectAltName = email:copy
basicConstraints = CA:true,pathlen:0
nsComment = "[your company] site CA"
nsCertType = sslCA
```

After creating this file, you can sign your CA certificate with the following commands:

```
OPENSSL_DIR]\bin\openssl x509 -req -extfile ca.cfg -days 1825 -signkey
ca.key -in ca.csr -out ca.crt
```

The resulting certificate file, **ca.crt**, is the certificate that will need to be imported into the certificate store on each client device. It is also necessary to create a configuration file for signing server keys. This file should be named **server.cfg**, and should contain the following:

```
extensions = x509v3
[ x509v3 ]
subjectAltName = email:copy
nsComment = "Certificate signed by your company CA"
nsCertType = server
```

You must also create a file that will store the serial numbers of certificates signed by this CA. Use the following command:

```
echo 01 > ca.serial
```

CREATING AND SIGNING SERVER KEYS

To create a new server key, use the following command:

```
[OPENSSL_DIR]\bin\openssl genrsa -out server.key 1024
```

This will generate a new server key and place it in the file **server.key**. Next, generate a Certificate Signing Request (CSR) for the server key. This is essentially the same process used for generating the CSR for the CA key, but the inputs are slightly different. Use the following command:

```
[OPENSSL_DIR]\bin\openssl req -new -key server.key -out server.csr
```

This command will run interactively and prompt you for information about the server certificate that will be generated. Example input is shown below:

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Washington
Locality Name (eg, city) []:Bellevue
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Company Name
Organizational Unit Name (eg, section) []: Engineering
Common Name []:server
Email Address []:user@company.com
```

Please enter the following 'extra' attributes to be sent with your certificate request:

```
A challenge password []: [enter]
An optional company name []: [enter]
```

Your answers to these prompts should be:

```
Country Name: Your 2-letter country abbreviation
State or Province Name: Your full state or province name
Locality Name: The city, town, or suburb where your organization is located
Organization Name: The name of your company or organization
Organizational Unit Name: Either a department name or some name representing this server
Common Name: The name of this server, as it should appear on the certificate. Note that this is not the name of a person.
Email address: The e-mail address of a party responsible for this server
```

The Common Name *must* match the host name of the host. Any variation in the name will cause the client to issue a warning when connecting.

Finally, sign the server's key with the CA's certificate. Use the following command:

```
[OPENSSL_DIR]\bin\openssl x509 -req -extfile server.cfg -days 1825 -CA  
ca.crt  
-CAkey ca.key -CAserial ca.serial -in server.csr -out server.crt
```

Note that the `-days 1825` parameter will cause our server certificates to expire in 1825 days, or roughly 5 years. If you want certificates to expire earlier or later, adjust this number to fit your requirements.

Copy the **ca.crt**, **server.key** and **server.crt** files to a directory on the target server that can be accessed from the System account but cannot be accessed from the accounts of users who will sign in to the host. Finally, select the server certificate in the Host Properties dialog.

To select the server certificate

1. Sign in to the gateway as a host administrator.
2. Select the host.
3. Click the **Edit Properties** button on the toolbar.
4. Click the **Advanced** tab.
5. From the **Transport** list, click **SSL**.
6. Type or browse to the path of the server's certificate file in the **SSL Certificate** box.
7. Click **Save**.

Your host now has a new SSL certificate, signed by your own custom certificate authority.

GENERATING A CSR USING IIS CERTIFICATE WIZARD

The following example uses Microsoft's **IIS Certificate Wizard** to generate a Certificate Signing Request (CSR), and then uses OpenSSL to generate the certificate. In this example, the administrator is the CA.

In order for this certificate to work in GO-Global a private key is required. When you generate a CSR with the IIS Certificate Wizard, a private key is created but it is not presented to the user by default. As a result, the private key needs to be backed up separately using the MMC (Microsoft Management Console). For instructions, see <http://www.thawte.com/ssl-digital-certificates/technical-support/backup.html>, and look under the Microsoft IIS 6.0 heading.

The private key in this case is a `.pfx` file, not a `.key` file, and it must be converted to PEM format in order to work with GO-Global. Use the following command to convert the pfx file to the PEM format:

```
openssl pkcs12 -nocerts -in server.pfx -out server.pem -nodes
```

Change the extension of the file from `.pem` to `.key`. The resulting file is called **server.key** and is required for SSL to work in GO-Global. It must have the same file prefix as the certificate generated by the CA (i.e., `server.crt`).

GO-Global requires that the certificate be in PEM format. When requesting a Certificate from a third-party CA, we recommend requesting a certificate in PEM format. If this is not possible and the certificate can only be delivered in DER format, it can be converted to PEM using the following command:

```
openssl x509 -inform der -in MYCERT.cer -out MYCERT.pem
```

The resulting **MYCERT.pem** file can then be renamed to **MYCERT.crt** for use in GO-Global.

NOTIFYING USERS OF A SECURE CONNECTION

When the SSL transport mode is selected, you can opt to notify users with a Security Alert when connections are secure.

To notify users when connections are secure

1. Sign in to the gateway as a host administrator.
2. Select the host.
3. Click the **Edit Properties** button on the toolbar.
4. Click the **Advanced** tab.
5. From the **Transport** list, click **SSL**.
6. Type or browse to the path of the host's certificate file in the **SSL Certificate** box.
7. Click the **Notify users when connections are secure** option.
8. Click **Save**.

When the SSL transport is selected, all connections to that host use the SSL transport and the selected encryption algorithm.

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.

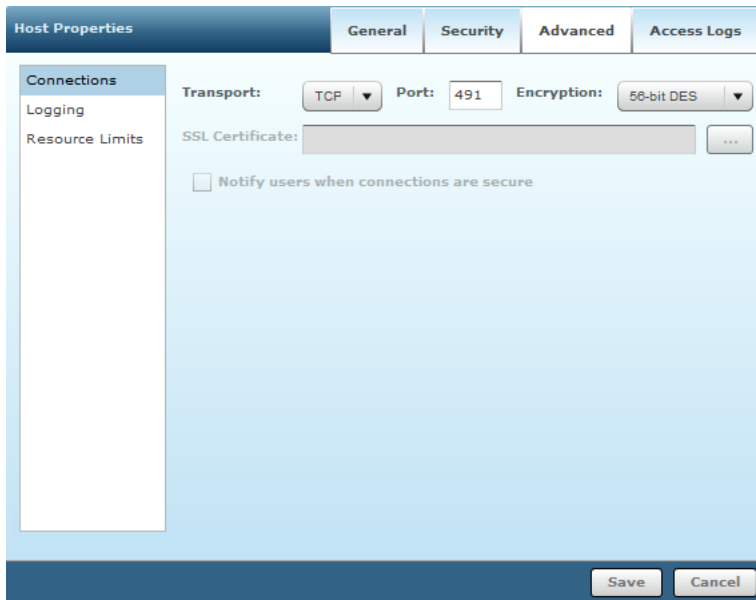
When TCP transport mode is selected, GO-Global uses **56-bit DES** encryption. The DES key is exchanged using RSA Public-Key Cryptography Standards. The RSA keys are 512-bits.

When SSL transport mode is selected, the following encryption algorithms are also available: **128-bit RC4**, **168-bit 3DES**, and **256-bit AES**. A special license is required to use these algorithms. To obtain this license, contact your GO-Global sales representative.

To encrypt a host's sessions

1. Sign in to the gateway as a host administrator.
2. Select the host.
3. Click the **Edit Properties** button on the toolbar.
4. Click the **Advanced** tab.
5. From the **Encryption** list, select an encryption level.
6. Click **Save**.

Once you have enabled encryption, all subsequent host 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 host, however, his or her session will be encrypted. The user must sign off the host, and sign back in for his or her session to be encrypted.



MODIFYING THE HOST PORT

In order for users to connect to a host 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 SSL is 491.

To modify the host port

1. Sign in to the host using an administrator account.
2. Select the host and click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Type a new port number in the **Port** box.
5. Click **Save**.

LOGGING

The 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.

Log files, whether they pertain to the client or host machine, are located in the **Log** folder on the host. (C:\Program Files\GraphOn\GO-Global\Log.)

Gateway logs are located at C:\Program Files\GraphOn\GO-Global\Tomcat\logs.

In the Log folder are three subfolders: **Backup**, **Codes**, 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 (to the nearest millisecond) the Application Publishing Service was started. (For example, `aps_2012-04-04_09-55-47-636.html`). 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 the host 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 Technical 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 `\Program Files\GraphOn\GO-Global\Log`. You can select a new location for the log files through the **Host Properties** dialog.

To select a new location for the Log files

1. Sign in to the host using an administrator account.
2. Select the host and click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Logging** on the left.
5. 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."

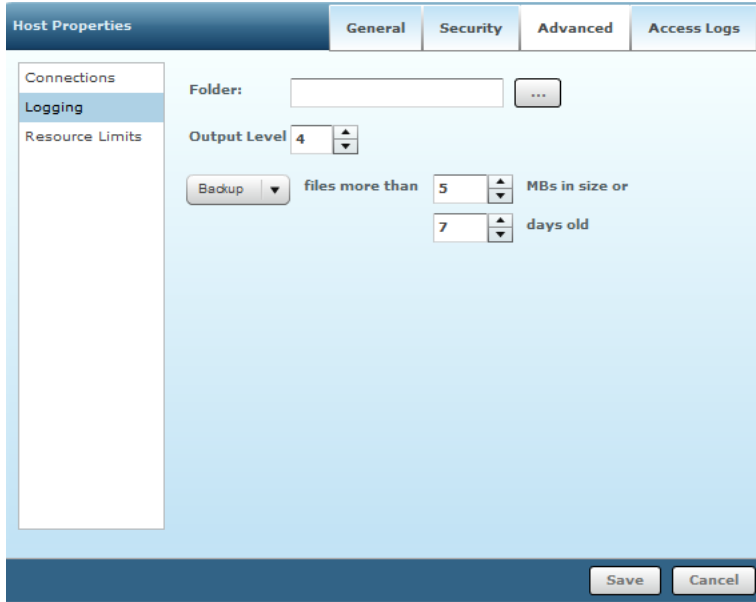
Note: You should move the Backup folder and existing log files to the new location, along with the Templates and Codes subfolders.

SETTING THE OUTPUT LEVEL

The host offers five log output levels, as follows:

- 1: Errors
- 2: Errors and Events
- 3: Errors, Events, and Warnings
- 4: Errors, Events, Warnings, and Diagnostic Messages
- 5: Errors, Events, Warnings, Diagnostic Messages, and Trace Messages

The default value for the Output level is 4.



To set the output level

1. Sign in to the host using an administrator account.
2. Select the host and click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Logging** on the left.
5. Type one of the above numeric values in the **Output level** box.
6. Click **OK**.

CAUTION!

Setting the log output value to 5 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 host.

MAINTAINING LOG FILES

The host 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, the host lets you delete or backup log files and set file size or age limits.

To delete log files

1. Sign in to the host using an administrator account.
2. Select the host and click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Logging** on the left.
5. Select **Delete**.
6. Specify how old (in days) log files can become before being deleted.
7. Specify at what size (in megabytes) log files are to be deleted.
8. Click **OK**.
9. Restart the **GO-Global Application Publishing Service**.

To backup log files

1. Sign in to the host using an administrator account.
2. Select the host and click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Logging** on the left.
5. Select **Backup**.
6. Specify how old (in days) log files can become before being moved to the Backup subdirectory of the Log folder.
7. Specify at what size (in megabytes) log files are to be moved to the Backup subdirectory of the Log folder.
8. Click **OK**.
9. Restart the **GO-Global 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 5 MB.

MEMORY USAGE

Administrators can prevent users from starting new sessions when certain resource limits are exceeded. These limits help administrators prevent servers from becoming loaded to the point where users experience performance problems and random resource allocation failures.

To set limits on memory usage

1. Select the host.
2. Click the **Edit Properties** button.
3. Click the **Advanced tab** on the Host Properties dialog.
4. Click **Resource Limits** from the list on the left.
5. Type a limit in the **Memory Usage** box. When this percentage of memory usage is reached, additional users will not be allowed to access the host.
6. Click **Save**.

ACCESS LOGS

Access to the host is recorded in the gateway's database. Access logs record when a user signs in and out of the host and when a host comes online or goes offline.

Access logs also record when a user signs in and out of a workspace, when a user starts and stops a process, and when a user opens and closes a file.

Access logs contain the following information:

- Date and time an item was accessed
- The name of the item that was accessed
- The name of the user or host that accessed the item
- A description of the access (e.g., sign in/sign out, connect/disconnect, etc.)

Administrators can use the information in Access logs to track when users access the host. Host Access logs can be viewed and searched through the **Host Properties** dialog.

To filter the Access Logs

1. Sign in to the host as admin.
2. Click the **Edit Properties** icon on the toolbar.
3. Click the **Access Logs** tab.
4. Select a date range by clicking the calendar icons next to the **From** and **To** boxes.
5. Click **Search**.

Administrators can save the Access Logs in XML format. The XML file exports all the data displayed in the table.

To export Access Logs

1. Sign in to the host as admin.
2. Click the **Edit Properties** icon on the toolbar.
3. Click the **Access Logs** tab.
4. If desired, select a date range.
5. Click **Search**.
6. Click **Export Logs**.
7. Open or save the .xml file.

HOST LOAD BALANCING

The gateway automatically assigns users to the host with the lightest load to ensure that users are not assigned to hosts that have run out of resources or are otherwise unable to support new users. It determines which host has the lightest load by comparing the CPU usage, memory usage and number of sessions running on each host. Specifically, it selects the host that has the lowest load based on the following equation.

$$\text{hostLoadValue} = \text{hostWeight} * ((\text{cpuUsage} * \text{cpuWeight}) + (\text{memUsage} * \text{memWeight}) + (\text{sessionUsage} * \text{sessionWeight}))$$

cpuUsage: the average CPU usage on the host during the previous 30 seconds

memUsage: the percentage of virtual memory that is in use on the host

sessionUsage: the number of sessions running on the host, as a percentage of the maximum allowed

The *hostWeight*, *cpuWeight*, *memWeight* and *sessionWeight* values are obtained respectively from the *LoadBalHostWeight*, *LoadBalCpuWeight*, *LoadBalSessionWeight* and *LoadBalSessionWeight* values in the host's **HostProperties.xml** file. These values may be adjusted to give greater or less weight to specific load variables. For example, if, in a given deployment, memory usage has little effect on the number of users that a host can support, the value of the *LoadBalSessionWeight* variable can be reduced from 100 to a lower value. If it is set to zero, memory usage will not be considered when selecting the host for a new user.

Regardless of the resource weight values, if the CPU usage, memory usage, or number of running sessions is greater than or equal to the host's limits for the respective resource, the gateway will not assign new users to the host.

Hosts report load information to the gateway every 30 seconds, and the gateway stores this information in its database. Since this information can become inaccurate when many users connect to the gateway at

the same time, the gateway increments the host's session count and increases its memory usage value by an estimated amount when it assigns a user to a host. It does not estimate how much CPU usage will increase because it is difficult to accurately predict how much CPU usage will increase when a user connects to a host.

SUPPORT REQUEST WIZARD

The host and the gateway include a Support Request Wizard that gathers information and log files that can be sent to technical support.

Administrators can run the Support Request Wizard from the Start menu by clicking Programs | GraphOn GO-Global 4 | Tools | Support Request Wizard. On Linux, run `/usr/local/graphon/gg-gateway-server/bin/srw` for the gateway.

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 upload the zipped file to the support ticket via the GO-Global support portal <http://www.graphon.com/customer-support/graphon-customer-support-portal> or reply to an existing support email (support@graphon.com) with the attachment.

CHAPTER 5:

OPTIONS CONFIGURATION

OPTIONS CONFIGURATION

Administrators can configure GO-Global options for users based on their membership in the domain and the domain's organizational units and groups. The default values for all options are set at the domain level.

To view the default values

1. Sign in to the gateway as a gateway administrator.
2. Select the domain.
3. Click **Edit Properties**.
4. Click the various tabs on the dialog to view the default values.

By default, any option that is enabled at the domain level is enabled for all users (all members of the domain). To enforce this, options that are enabled at the domain level are grayed out for the domain's organizational units and groups. For example, the Clipboard option on the **Client Access** tab is enabled (checked) at the domain level. As a result, if you select any other object in the directory and click Edit Properties | Client Access, the Clipboard option will be checked, but it will be grayed out.

This behavior also applies to other objects in the directory. For example, if the Client Access | Sound option is checked for an organizational unit, the Sound option will be checked and grayed out for all of the organizational unit's groups.

By default, the gateway only lets administrators edit options that are not already enabled at a higher level in the directory. Specifically, it only allows administrators to increase the amount of functionality granted. It does not let administrators disable options that are enabled at a higher level because this can make it difficult for administrators to know if changes to domain and organizational unit options will be applied to users.

The same general rule applies to options with numerical values—administrators can increase the amount of functionality granted, but cannot decrease it. For example, if the idle timeout is set to 30 minutes for an organizational unit, administrators will be able to increase the value above 30 minutes (e.g., to 60 minutes) for the organizational unit's groups, but not reduce the value (e.g., to 10 minutes).

Some options (e.g., the Drives "Assign consecutive letters start at" option) are settings that do not enable functionality. For these options, the gateway allows the administrator to set the option for any directory object. If this results in conflicts, GO-Global resolves the conflict by selecting the default value specified for the domain.

Given this design, it is recommended that administrators specify restrictive, "least common denominator," default values at the domain level and grant access to progressively more functionality as they move deeper into the directory.

The gateway does not allow administrators to set options for individual users. Users inherit their options from their parent organizational unit and/or any groups to which they belong.

To determine the option values for a user, the gateway

- Note:**
1. Identifies all of the groups to which the user belongs. *Note that groups that are defined in organizational units that are not accessible from the gateway are ignored.*
 2. Obtains the values of the options for each group. Both the values saved under the group's entry in the database and the values that the group inherits are obtained. In other words, the set of options for each group is the set that is displayed in the **Options** dialog when the group is selected.
 3. If the user's organization unit is not a parent of one of the groups, obtains the values for the user's organizational unit. As with groups, the set of options includes inherited values.
 4. Compares the values of each option in each option set and resolves any differences. For example, if a user is a member of two groups and Printers is enabled in one group and disabled in another, the Printers option is enabled for the user.

OVERRIDING PARENT'S OPTIONS

In some situations, it may be necessary to override the default behavior and disable an option that is enabled at a higher level in the directory. Administrators can do this by checking the **Override parent's options** checkbox in the **Options** dialog. For example, to disable an option for an organizational unit that is enabled for the domain:

1. Select the organizational unit.
2. Click **Edit Properties**.
3. Check **Override parent's options**. Controls that were previously grayed out will now be enabled.
4. Disable one or more options.
5. Click **Save**.

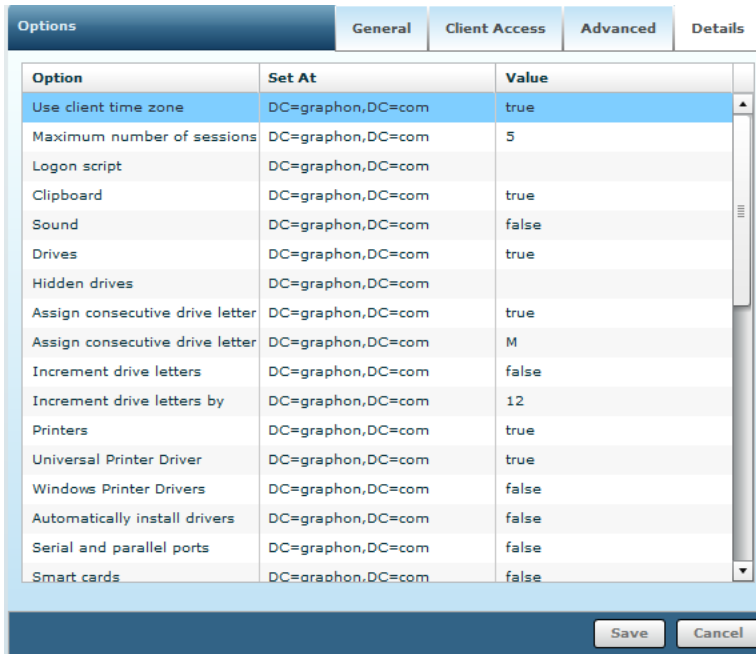
The screenshot shows a software configuration window titled "Options" with four tabs: "General", "Client Access", "Advanced", and "Details". The "Client Access" tab is selected. The window contains the following elements:

- A checked checkbox labeled "Use client's time zone".
- A label "Maximum number of sessions per user" followed by a spinner control set to the value "5".
- A label "Logon script" followed by an empty text input field.
- At the bottom, a checked checkbox labeled "Override parent's options".
- Two buttons labeled "Save" and "Cancel" are located at the bottom right.

In this example, the gateway saves all of the values shown in the dialog in the organizational unit's entry in the gateway's database. Thereafter, changes to the domain's options will not affect any of the organizational unit's values or the values of the children of the organizational unit. This will often make it difficult to know if changes to the parent's options will be applied to users. As such, **Override parent's options** should be used with care.

VIEWING OPTIONS DETAILS

The **Details** tab of the **Options** dialog lists the names of the dialog's options and the Distinguished Name of the directory object under which the value of the option is stored in the gateway's database.



Option	Set At	Value
Use client time zone	DC=graphon,DC=com	true
Maximum number of sessions	DC=graphon,DC=com	5
Logon script	DC=graphon,DC=com	
Clipboard	DC=graphon,DC=com	true
Sound	DC=graphon,DC=com	false
Drives	DC=graphon,DC=com	true
Hidden drives	DC=graphon,DC=com	
Assign consecutive drive letter	DC=graphon,DC=com	true
Assign consecutive drive letter	DC=graphon,DC=com	M
Increment drive letters	DC=graphon,DC=com	false
Increment drive letters by	DC=graphon,DC=com	12
Printers	DC=graphon,DC=com	true
Universal Printer Driver	DC=graphon,DC=com	true
Windows Printer Drivers	DC=graphon,DC=com	false
Automatically install drivers	DC=graphon,DC=com	false
Serial and parallel ports	DC=graphon,DC=com	false
Smart cards	DC=graphon,DC=com	false

CLIENT TIME ZONE

By default, sessions are run in the time zone of the host machine. Administrators can opt to run sessions in the time zone of the client computer by enabling the **Use client's time zone** option.

To enable client time zone

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button.
3. Select **Use client's time zone**.
4. Click **Save**.

MAXIMUM SESSIONS PER USER

Administrators can limit the number of sessions per users. By default, users are limited to 5 concurrent sessions.

To limit the number of sessions per user

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** on the toolbar.
3. Enable **Maximum number of sessions per user**.
4. Type the maximum number of sessions per user in the edit box.
5. Click **Save**.

RUNNING A LOGON SCRIPT

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

To run a logon script

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button.
3. Type the logon script in the **Logon Script** box.
4. Click **Save**.

CLIENT ACCESS

Applications running on Windows hosts can access resources on the drives of the client computer, including sound, printers, serial and parallel ports, and the clipboard. Client clipboard is also supported on Linux hosts.

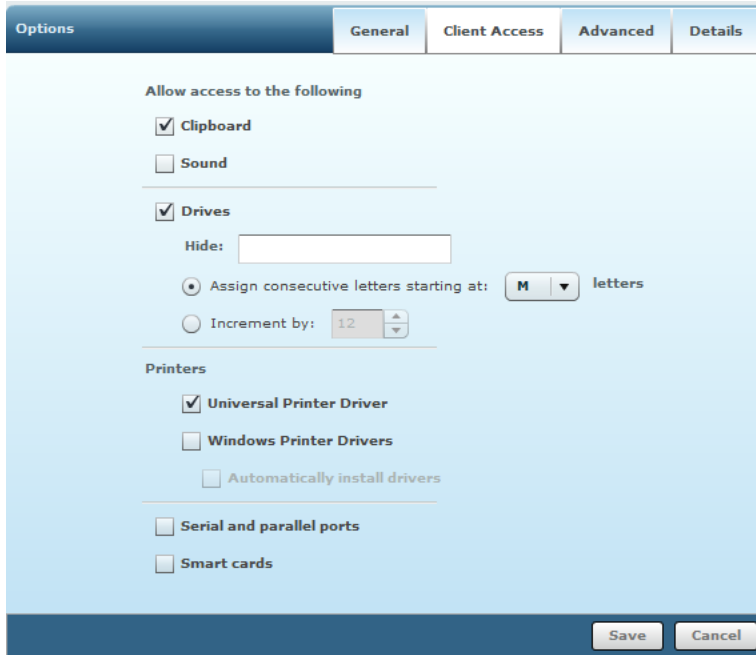
CLIENT CLIPBOARD

GO-Global allows client and server-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 host, and vice versa. Clipboard support is enabled by default.

To disable client clipboard

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.

3. Click the **Client Access** tab.
4. Click **Clipboard**.
5. Click **Save**.



CLIENT SOUND

GO-Global supports sound capability for any application that uses PlaySound, sndPlaySound, or waveOut. Speakers are not required on the host, but a sound card is recommended. The client machine, however, does require a sound card and speakers. Audio support is disabled by default.

Note: Client sound 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.

To enable audio support

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Client Access** tab.
4. Click the **Sound** check box.
5. Click **Save**.

CLIENT FILE ACCESS

GO-Global allows users to access files stored on the client computer and to save files locally. Client drives are 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 enabled by default.

To disable support for client drives

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Client Access** tab.
4. Click **Drives**.
5. Click **Save**.

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

REMAPPING CLIENT DRIVES

When applications are run 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. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Client Access** tab.
4. Click **Drives**.
5. Select **Assign consecutive letters starting at**:
6. Select the drive letter that should start the sequence.
7. Click **Save**.

For example, if a client computer has A, C, D, 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. This feature is disabled by default. Once enabled, the default drive

letter is M.

To increment client drive letters by a fixed value

1. Select a group, domain, or organizational unit from the toolbar.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Client Access** tab.
4. Click **Drives**.
5. Select **Increment by**.
6. Type a number greater than or equal to 1 that will yield the desired offset.
7. Click **Save**.

For example, if the client computer has the same drives as above (A, C, D, 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. The default value for this setting is 12.

All client drives are mapped by default.

HIDING CLIENT DRIVES

Administrators can hide client drives such as the client's operating system drive, floppy drive, and CD ROM drive, making them inaccessible. Drives listed in the Hide box can be listed in any order.

To hide one or more client drives

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Client Access** tab.
4. Click **Drives**.
5. In the **Hide** box, type the client drive letters you want to hide.
6. Click **Save**.

CLIENT PRINTING

When running applications, users can print to network printers and to printers that are directly connected to their computers (e.g., via serial, parallel and USB ports). By default, GO-Global automatically detects the client's default printer information once the user has signed in to the host. This includes the default printer's port and printer driver. If the printer driver is not installed on the host, GO-Global will attempt to locate the driver and automatically install it.

Administrators can control which, if any, printers are made available to users using the **autoConfigPrinters** startup parameter. Set the `autoConfigPrinters` parameter to "all", "none" or "default" to respectively make all, none or only the default printer available from applications running on the host. For example, to make all printers available:

1. Open the `logon.html` page (`\Program Files\GraphOn\GO-Global\Tomcat\webapps\go-global\rxp\logon.html`.)
2. Change the following line:
`var autoConfigPrinters = GetVar("printerconfig");`
to
`var autoConfigPrinters = "all";`
3. Save the file
4. Restart the gateway.

Client printing is enabled by default.

To disable support for client printers

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
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 **Save**.

DESIGNATING ACCESS TO PRINTER DRIVERS

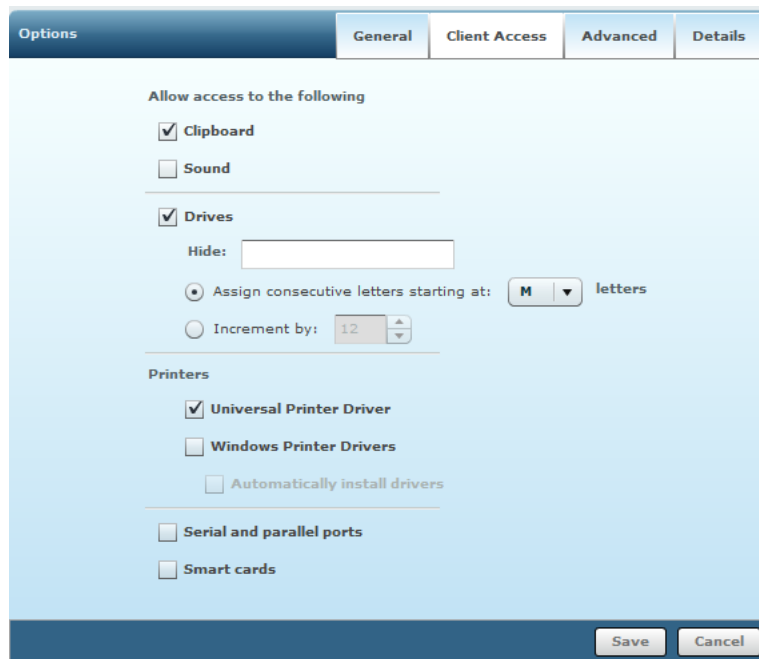
GO-Global can obtain printer drivers from the following sources:

- **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. To allow GO-Global to automatically install native printer drivers that ship with Microsoft Windows enable **Automatically install drivers**.

All printing options are enabled by default. If a printer's native driver is installed on the host or it is included with Windows, it will be used to configure the printer. If a printer's native driver is *not* installed and is *not* included with Windows, the printer is configured to use the Universal Printer Driver.

When neither the **Universal Printer Driver** or **Windows Printer Drivers** is enabled, no printers will be configured and client printing is disabled.

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.



When only the **Windows Printer Drivers** option is enabled, only native printer drivers that are installed on the host will be used. If a printer's native driver is not installed, that printer will not be configured. When **Windows Printer Drivers** and **Automatically install drivers** are enabled, only native printer drivers that

are installed on the host or those that are included with Windows will be used. If a printer's native driver is not installed and it is not included with Windows, that printer will not be configured.

When both the **Universal Printer Driver** and the **Windows Printer Drivers** are enabled, and a printer's native driver is installed on the host, the printer's native driver will be used to configure the printer. If it is not installed on the host, the printer is configured to use the Universal Printer Driver.

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.

Note: The **Universal Printer Driver** uses a standard printing properties dialog and may not offer some of the more advanced printing options other drivers do.

To designate access to printer drivers

1. Select a workspace.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Client Access** tab.
4. Click the box beside the desired driver source or sources.
5. Click **Save**.

MAPPING PRINTER DRIVERS

By default, GO-Global uses the same native driver as specified on the client. Administrators can override native drivers and force clients to use the Universal Printer Driver or another printer driver.

1. Stop the **GO-Global Application Publishing** Service on the host.
2. Locate MappedPrinterDrivers.xml in C:\ProgramData\GraphOn or C:\Documents and Settings\All Users\Application Data\GraphOn.
3. Open the file in Wordpad and search for the client printer driver name, for example,
<property id="HP LaserJet 2100 Series PS" type="STRING">
<value>HP LaserJet 2100 Series PS;Universal Remote Printer</value>
</property>
4. Delete the driver name from the value field. In the example above, delete HP LaserJet 2100 Series PS; (This is the driver used on the client machine.)
5. Save the file.
6. Restart the **GO-Global Application Publishing** Service.

The next time users connect to the host, they will print using the Universal Printer Driver.

To revert back to using the native printer driver

1. Stop the **GO-Global Application Publishing** Service on the host.
2. Open **MappedPrinterDrivers.xml** in a text editor and delete the entire modified line. For example, delete:


```
<property id="HP LaserJet 2100 Series PS" type="STRING">
<value>HP LaserJet 2100 Series PS;Universal Remote Printer</value>
</property>
```
3. Save the file.
4. Restart the **GO-Global Application Publishing** Service.

The MappedPrinterDrivers.xml file can be deleted to remove any prior changes. The file is recreated when users sign in to the host.

To designate an additional driver

1. Stop the **GO-Global Application Publishing** Service on the host.
2. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn or C:\Documents and Settings\All Users\Application Data\GraphOn.
3. Open the file in a text editor and search for the client printer driver name, for example,


```
<property id="HP LaserJet 2100 Series PS" type="STRING">
<value>HP LaserJet 2100 Series PS;Universal Remote Printer</value>
</property>
```
4. Specify an additional driver. For example, add HP LaserJet 2100 Series PS to the list, as follows:


```
<property id="HP LaserJet 2100 Series PS" type="STRING">
<value>HP LaserJet 2200 Series PS;HP LaserJet 2100 Series PS;Universal Remote Printer</value>
</property>
```
5. Save the file.
6. Restart the **GO-Global Application Publishing** Service.

Administrators can add an unlimited number of driver names to the value. GO-Global configures client printers using the drivers in the order they are specified. The semicolon-separated drivers specify the preferential order of drivers to be used when installing a proxy printer.

Notes:

Client printers are temporarily installed on the 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 host.

To add a default printer for all new users, consult the following article:

<http://support.microsoft.com/support/kb/articles/Q252/3/88.ASP>

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 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.

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.

CLIENT SERIAL AND PARALLEL PORTS

GO-Global allows applications running on a host to access client machines' serial and parallel ports. Serial and parallel ports are disabled by default.

Note: Client 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.

To enable serial and parallel ports

1. Select a group, domain, or organizational unit from the Navigation Pane
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Client Access** tab.
4. Click the **Serial and parallel ports** check box.
5. Click **OK**.

SMART CARD DOCUMENT SIGNING

GO-Global provides support for smart card document signing on Windows clients only. Smart card document signing is disabled by default. 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 Options dialog.

To enable smart card document signing

1. Select a group, domain, or organizational unit from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Client Access** tab.
4. Click the **Smart cards** check box.
5. Click **Save**.

DISPLAY

ENABLING CLEARTYPE

GO-Global supports Microsoft's ClearType subpixel rendering technology. ClearType improves readability on color LCD displays with a digital interface, such as those in laptops and high-quality flat panel displays.

To enable ClearType

1. Select a domain, organizational unit, or domain from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Display** from the list on the left.
5. Enable **ClearType**.
6. Click **Save**.

TIME LIMITS

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 host.

To specify the session limit

1. Select a domain, organizational unit, or group from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Time Limits** from the list on the left.
5. Enable **Session**.
6. In the edit box, type the number of minutes that a session is allowed to run before its user is logged off.
7. Click **Save**.

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 allowed on the host.

To specify the idle limit

1. Select a domain, organizational unit, or group from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Time Limits** from the list on the left.
5. Enable **Idle**.
6. In the edit box, type the number of minutes of idle time allowed on the host.
7. 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.
8. Click **Save**.

The minimum amount of idle time is 1 minute and the maximum is 44640 minutes (31 days). This feature is disabled 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. Select a domain, organizational unit, or group from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Time Limits** from the list on the left.
5. Enable **Warning Period**
6. 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
7. Click **Save**.

Note: 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 an automated logoff begins during which users may save files, close applications, etc.

To specify the grace period

1. Select a domain, organizational unit, or group from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Time Limits** from the list on the left.
5. Enable **Grace Period**.
6. In the edit box, specify the number of minutes after a logoff begins that users are able to save files and close applications, etc.
7. Click **Save**.

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.

SETTING THE SESSION TERMINATION OPTION

The session termination option is set to **never** by default.

To set the session termination option

1. Select a domain, organizational unit, or group from the Navigation Pane.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click **Time Limits** from the list on the left.
5. 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.)
6. Click **OK**.

USER SANDBOX

The User Sandbox feature allows administrators to prevent users from:

- Viewing the names of files and directories that are outside the user's workspace
- Running programs that are not published to a user or contained in a white list

RESTRICTING ACCESS TO FILES

To prevent users from accessing files outside their workspace

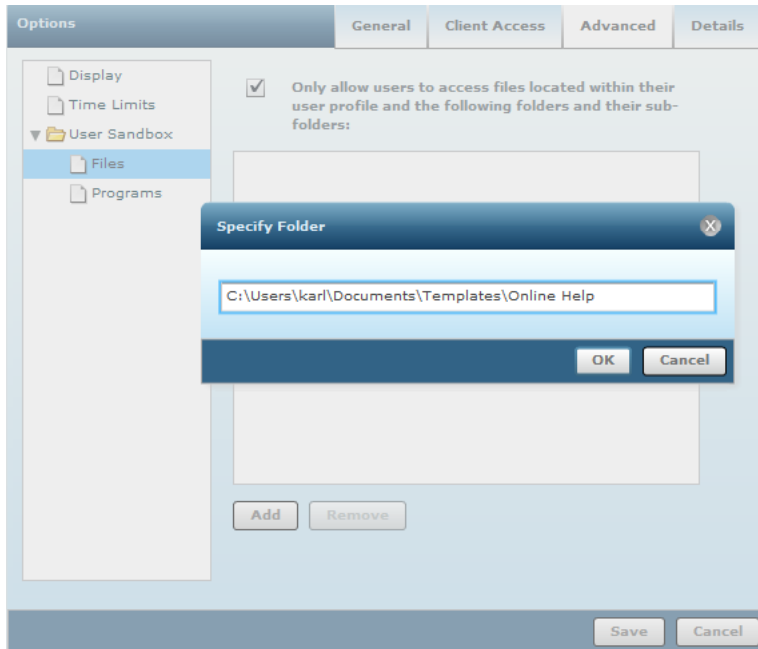
1. Select a group, domain, or organizational unit.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click the **User Sandbox** folder on the left.
5. Select **Files**.
6. Enable **Only allow users to access files located within their user profile and the following folders and their sub-folders**.
7. Click **Save**.

When this option is not enabled, users can browse the hard drive and see what programs are installed on the host computer and what other users have stored on the computer.

Administrators can grant users access to additional files by specifying the folder in the **Options** dialog.

To grant users access to specific folders outside their workspace

1. Select a group, domain, or organizational unit.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click the **User Sandbox** folder on the left.
5. Select **Files**.
6. Enable **Only allow users to access files located within their user profile and the following folders and their sub-folders**.
7. Click **Add**.
8. Type the folder's path in the **Specify Folder** dialog.
9. Click **Add** to select additional folders. Otherwise, click **Save**.



RESTRICTING ACCESS TO PROGRAMS

When a user connects to a host, the contents of both the user's *private Desktop folder* and the *public Desktop folder* are displayed in the Content Pane.

On Windows Vista and later, the public Desktop folder is **[Drive Letter]\Users\Public\Desktop**.

On Windows XP and Windows Server 2003, the public Desktop folder is **[Drive Letter]\Documents and Settings\All Users\Desktop**.

The user-private Desktop folder is **%USERPROFILE%\Desktop** on all Windows hosts.

When a host administrator connects to a host, only the items in the public Desktop folder are displayed in the Content Pane. Items from the administrator's private Desktop folder are not displayed. This prevents administrators from publishing applications that users won't be able to access due to Windows security restrictions.

When the user sandbox for programs is not enabled, users can generally run any program on the host computer. They can do this even if the program is not published to them. For example, if Microsoft Word is published to the user, the user can open Word's **File Open** dialog, browse to `c:\windows\system32`, right-click `cmd.exe` and click **Open**.

Users can run programs from shortcuts in the public and user-private Desktop folders regardless of whether the **Only allow users to run programs from shortcuts in the public and user-private Desktop folders and programs listed below** is checked or not. However, if **Only allow users to run programs from shortcuts in the public and user-private Desktop folders and programs listed below** is checked, users will

only be able to run programs from shortcuts in other locations if the programs are contained within the Programs white list as defined in the **Options** dialog.

If an administrator or user publishes an application to the home page from either the public or user-private Desktop folder, users will be able to open the published application regardless of whether **Only allow users to run programs from shortcuts in the public and user-private Desktop folders and programs listed below** is checked or not. If however, an administrator or user publishes a shortcut to the home page from a different location, users will only be able to access the program if the program is contained within the Programs white list as defined in the **Options** dialog.

To prevent users from running programs that are not published to their workspace

1. Select a group, domain, or organizational unit.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click the **User Sandbox** folder on the left.
5. Select **Programs**.
6. Enable **Only allow users to run programs from shortcuts in the Public folder and programs listed below**.
7. Click **Save**.

To allow users to run specific programs that are not published to their workspace

1. Select a group, domain, or organizational unit.
2. Click the **Edit Properties** button on the toolbar.
3. Click the **Advanced** tab.
4. Click the **User Sandbox** folder on the left.
5. Select **Programs**.
6. Enable **Only allow users to run programs from shortcuts in the Public folder and programs listed below**.
7. Click **Add**.
8. Type the path in the **Specify Program Path** box.
9. Click **Add** to select additional programs. Otherwise, click **Save**.

CHAPTER 6: ADVANCED TOPICS

PROXY HOSTS

When hosts need to be accessed from the Internet, they are generally located on an internal network that cannot be accessed directly from the Internet and are connected to a proxy host in a DMZ that relays data between clients on the Internet and hosts on the internal network. This configuration ensures that hosts cannot be accessed directly from the Internet or from the DMZ and thereby helps protect the sensitive data often stored on hosts.

To install a proxy host on Windows and connect it to a gateway

1. Run the proxy host setup program (`gg-proxy-host.windows_x86.exe`) on a computer in the DMZ. This setup program is used on both the x86 and x64 versions of Windows.
2. Connect the proxy host to the gateway:
 - a. Click Start | All Programs | GraphOn | GO-Global 4 | Tools | Gateway Connector.
 - b. Sign in to the gateway as a gateway administrator (e.g., admin).
 - c. Follow the prompts to connect the proxy host to the gateway.
3. Configure the gateway to use the proxy host:
 - a. Edit `\Program Files\GraphOn\GO-Global\Tomcat\webapps\go-global\WEB-INF\classes\settings.override.properties`
 - b. Type the address of the proxy host in the `proxyConfig.proxyHost` property.
 - c. Change the value of the **proxyConfig.proxyPort** property to 491.
 - d. Save the file.
 - e. Restart the **GO-Global Gateway** service.
4. Register hosts with the gateway. New hosts will be automatically configured to use the proxy host. If hosts were previously registered with the gateway, configure them to use the proxy host as follows:
 - a. On the host computer, edit the GO-Global `config.xml` file. On Windows Server 2003 and earlier, the file is located in `C:\Documents and Settings\All Users\Application Data\GraphOn`. On Windows Vista and later, the file is located in `C:\ProgramData\GraphOn`.

- b. Enter the proxy host's address in the **smiaddress** field.
- c. Enter the proxy host's port (e.g., 491) in the **smiport** field.
- d. Save the file.
- e. Restart the **GO-Global Application Publishing Service**.

HOW DO PROXY HOSTS WORK?

When the proxy host starts up, it opens a connection (connection A) to the gateway. The gateway authenticates the connection and records the public address of the proxy host in its database. When the host starts up, it opens a second connection (connection B) to the proxy host, and the proxy host in turn notifies the gateway that the host is online over connection A. When the gateway receives the host online notification, it authenticates the host connection and then records in its database the internal address of the host and the ID of the proxy host to which the host is connected.

When a user wants to connect to the host, the gateway issues a command to the proxy host over connection A to create a session, and the proxy host sends a request over connection B to the host to start the session. The host then opens a new connection (connection C) to the proxy host that will be used to transmit session-specific data.

After the session has been created, the gateway sends a URL to the client that contains the address of the host, the address of the proxy host to which the host is connected, the ID of the host session, and a random string that the gateway will use to authenticate the connection. The client first tries to connect directly to the host. If the client and host are located on the internal network (either directly or via a VPN), this connection will generally succeed. Otherwise, if the client fails to connect to the host (e.g., if the client is connected to the Internet), the client will then attempt to connect to the proxy host. The connection from the client to the host/proxy host is connection D.

If the client connects to either the host or proxy host, the computer to which the client connected sends a notification message to the gateway. This message includes the session to which the client wants to connect, and the connection credentials. If the credentials match those that the gateway specified in the client URL, the gateway sends a request to the host/proxy host that accepted the connection to attach the client to the session. From that point on, all session-specific data is sent to the client over connection D. If the client is connected to a proxy host, the proxy host relays the data over connection C to the host.

If the proxy host is configured to use SSL, all connections to the proxy host (e.g., connections B, C and D) are encrypted. For example, when session-specific data is sent from the host to the client, it is encrypted on the host before it is sent over connection C, and it is decrypted when it is received in the proxy host. The data is then re-encrypted in the proxy host before it is transmitted to the client over connection D.

Hosts connect to only one proxy host in a cluster at a time, but in high availability clusters they are configured to have at least one backup proxy host. If a proxy host goes down, the connection between the proxy host and the gateway is broken. This notifies the gateway that the proxy host is offline, and the gateway sets the state of the proxy host and all of its hosts to offline. In addition, the connections between the hosts and the proxy host are also broken, and the hosts then attempt to open connections to the backup proxy host. When a host connects to the backup proxy host, the backup proxy host notifies the gateway that the host has connected, and the gateway sets the status of the host to online.

When a host comes back online, the gateway will again allow sessions to be created on it, and it passes the address of the backup proxy host to the client, not the address of the primary proxy host that is offline.

If a proxy host goes down, the clients and hosts that are connected to it begin searching for another proxy host. The clients will search all of the proxy hosts listed in the **hostaddress** field in the proxy hosts' config.xml files. The hosts will search all of the proxy hosts listed in the **smiaddress** field in their config.xml files. The values of the **hostaddress** and **smiaddress** fields must be identical on all hosts and proxy hosts.

If, during the process of searching for a new proxy host, a client connects to a proxy host and the host on which the client's session was running is not connected to the proxy host, the client will keep searching. The number of times the client will attempt to connect to each proxy host in its list is specified via the client's autoreconnect parameter. The client waits 10 seconds between each connection attempt to give the host time to recover and possibly reconnect to a new proxy host. Autoreconnect is disabled by default, i.e., set to 0.

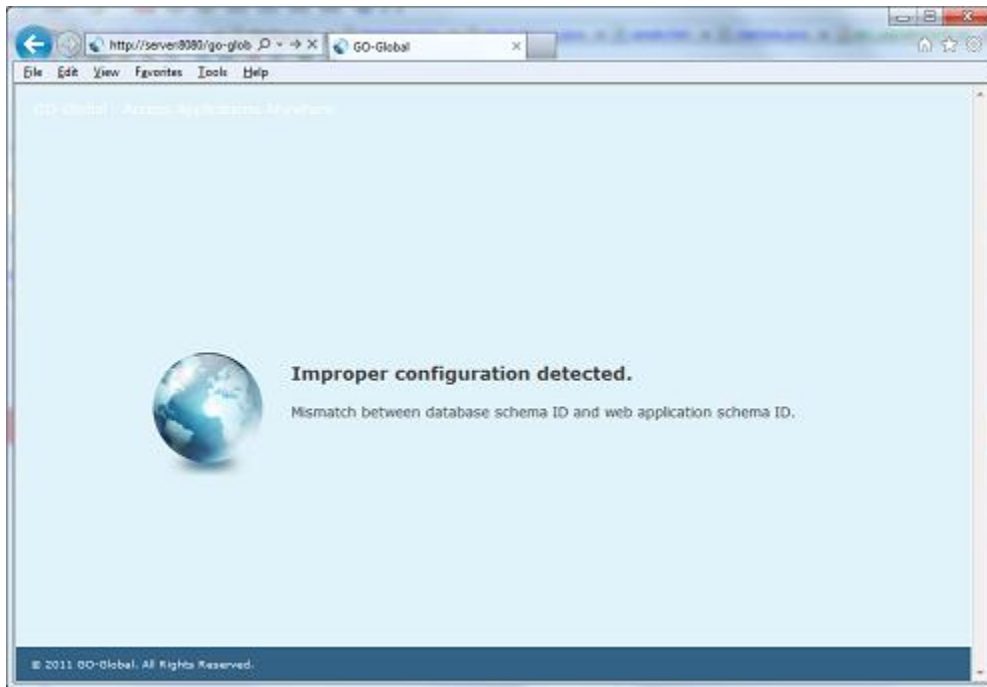
GO-Global proxy hosts are similar to Web reverse proxies in the way that they protect hosts. Specifically, both proxy hosts and reverse proxies do not allow direct connections to their respective servers, and connections must be authenticated before data is allowed to be transmitted between a client and server. However, the direction in which the connections are established is different in proxy hosts and Web reverse proxies.

When a connection is opened to a reverse proxy, the reverse proxy opens a connection to the web server. With proxy hosts however, connections are opened from the host to the proxy host. This provides additional security and does not require any firewall configuration to allow connections from the DMZ to the hosts on the internal networks.

Because GO-Global uses a propriety protocol that relies on persistent connections, the communication between GO-Global clients and hosts cannot be managed by reverse proxies except when the GO-Global Flash client is used (Windows host only.) The Flash client allows communication over reverse proxies because it tunnels GO-Global's protocol over HTTP. However, the performance and scalability of these connections is far lower than when a native client or browser add-on is used with a proxy host.

GATEWAY DATABASE SCHEMA ID

The gateway database contains a database schema ID value which is verified against the corresponding gateway application schema ID. If these schema IDs do not match, the following warning is displayed in the gateway:



Additionally, the following error is noted in the goglobal.log file:

```
[FATAL] 16 Sep 2012 14:00:01 impl.PublicServicesImpl Mismatch  
between database schema ID (42) and web application schema ID (41).
```

To update an existing gateway DB2 Database instance run the schema migration scripts. The database migration scripts are located in: <go_global_home>/db/migration.

There is one migration script, with file name prefix db2_, for each schema ID revision. The schema ID error, shown above in the gateway log file, will identify which schema ID version is needed. The following steps apply the schema migration script to an existing database:

```
login as: db2inst5
Using keyboard-interactive authentication.
Password:
db2inst5@ggdb2:~> cd sqllib/
db2inst5@ggdb2:~/sqllib> . db2profile
db2inst5@ggdb2:~/sqllib> cd bin/
db2inst5@ggdb2:~/sqllib/bin> ./db2batch -o s yes -d goglobal -f
~/db2_upgrade41to42.sql
```

LICENSING

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 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 redundancy:

- Via a set of three redundant license servers
- Via a license-file list in the LM_LICENSE_FILE environment variable

Note: 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.

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 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

INCREMENT session blm 4.0 31-dec-2012 5 99E82D1B9A64 HOSTID=ANY

INCREMENT any_app blm 4.0 31-dec-2012 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 host to the license server. This can be done in two different ways, either by copying the license to each 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 Programs directory (\GO-Global\Programs) or from: http://www.globes.com/support/fnp_utilities_download.htm#downloads. 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 sets of product codes with a count of five for each set from a GraphOn sales representative. 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
INCREMENT session blm 4.0 permanent 5 DF9C8F5ADF34 HOSTID=ANY \
    user_info="Joe User joeu@mycompany.com" ISSUER="GraphOn \
    Corporation" ISSUED=17-feb-2012 NOTICE="Copyright (C) \
    1996-2012 GraphOn Corporation. All Rights Reserved" ck=142 \
    SN=12865-AA
INCREMENT any_app blm 4.0 permanent 5 1DF84A360E8F HOSTID=ANY \
    user_info=" Joe User joeu@mycompany.com " ISSUER="GraphOn \
    Corporation" ISSUED=17-feb-2012 NOTICE="Copyright (C) \
    1996-2012 GraphOn Corporation. All Rights Reserved" ck=84 \
    SN=12865-AA
```

License 2 for tokyo:

```
SERVER tokyo 00508BF77F7E 27000
DAEMON blm
INCREMENT session blm 4.0 permanent 5 16BE40E1D98D HOSTID=ANY \
```

```
user_info="Joe User joeu@mycompany.com" ISSUER="GraphOn \
Corporation" ISSUED=17-feb-2012 NOTICE="Copyright (C) \
1996-2012 GraphOn Corporation. All Rights Reserved" ck=142 \
SN=12865-AA

INCREMENT any_app blm 4.0 permanent 5 6DB6F3E402DF HOSTID=ANY \
user_info=" Joe User joeu@mycompany.com " ISSUER="GraphOn \
Corporation" ISSUED=17-feb-2012 NOTICE="Copyright (C) \
1996-2012 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\Programs 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.

CONFIGURING GO-GLOBAL TO USE A CENTRAL LICENSE SERVER

Two methods can be used for configuring GO-Global to use a license server that serves multiple machines. In the following examples, machine550 is the name of the license server and machine-w2k is the name of the host. We recommend stopping the GO-Global License Manager service on the host before getting started. The License Manager should be disabled on all secondary servers of the Central License Server.

To stop the GO-Global License Manager

1. Click the **Start** button on the Windows taskbar.
2. Click Control Panel | Administrative Tools.
3. Double-click **Services**.
4. Select **GO-Global License Manager** from the list of services.
5. Click the **Stop** button.

Once you have stopped the GO-Global License Manager on host, you may proceed with one of the following methods for configuring a central license server:

On the host, place `port@host` (e.g., `27000@machine550`) in the `LM_LICENSE_FILE` environment variable instead of the path to the license file. FLEXnet Publisher's `LMTOOLS.EXE` reports that the license file on machine550 is being read correctly.

—OR—

On the host, place `USE_SERVER` directly after the `SERVER` line in the license file on the host. This is essentially the same as the preceding method but the change to the environment variable is not required.

For example, the permanent license file (e.g., `license.lic`) on host (`MACHINE-W2K`) would appear as follows:

```
SERVER machine550 00d0b74f4023
USE_SERVER
```

OPENING THE LICENSE MANAGER PORT IN A FIREWALL

If there is a firewall between the hosts and the license server, the ports for FLEXnet (27000, by default) and for the license manager (BLM) need to be open in the firewall. For the license manager, add

```
port=<port#>
```

to the license on the license server for a specific port. (Unless you manually assign a specific port number, an ephemeral port number is used.)

Example:

```
SERVER caspian 000476BA8F74 27000
DAEMON BLM port=5678
INCREMENT session blm 4.0 31-dec-2012 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 4.0 31-dec-2012 uncounted D1D222D031C4
HOSTID=ANY
```

CONFIGURING THE GATEWAY FOR SAML AUTHENTICATION

The gateway can be authenticated directly using the Security Assertion Markup Language (SAML) protocol. SAML authentication requires an identity provider (IdP), such as Nordic Edge, that authenticates user credentials.

To configure the gateway for SAML Authentication

1. Stop the Tomcat server hosting GO-Global.
2. Edit `<tomcat_home>/webapps/go-global/WEB-INF/web.xml` and change the line:
`/webapps/go-global/WEB-INF/spring/security/form-authentication.xml`
to
`/webapps/go-global/WEB-INF/spring/security/iwa-ldap-SAML-
authentication.xml`
3. Update the service configuration file located in `<tomcat_home>/webapps/go-global/WEB-INF/classes`.
For an ActiveDirectory configuration, rename `service-beans.xml.ldap` to `service-beans.xml`.
For an OpenLDAP configuration, rename `service-beans.xml.openldap` to `service-beans.xml`.
4. Edit LDAP configuration as follows:
 - a. Open the following file for editing:
`<tomcat_home>/webapps/go-global/WEB-INF/spring/security/iwa-ldap-SAML-authentication.xml`
 - b. Locate `<bean id="ldapContextSource">` and modify the following to match your LDAP server location and login credentials. The user account name specified below can be the name of any user account that has rights to search the directory. Generally, it should be a normal user account, i.e., not an administrator account.

```
<constructor-arg value="ldap://[domain server address]:[domain server  

port (e.g., 389)]/dc=[domain name],dc=[domain suffix (e.g., com)]"/>
```

```

<property name="managerDn">
  <value>domain\username</value>
</property>
<property name="managerPassword">
  <value>password for above user account</value>
</property>

```

- c. Determine the number of organizational units (OU) that the user search should query. By default, the LDAP configuration file is configured with two OU search beans, `ldapOUsSearch1` and `ldapOUsSearch2`. Copy or cut the OU search bean definitions to add or remove OU search definitions. Modify the first constructor argument of each search bean to specify the OU to search:

```

<constructor-arg index="0">
  <value>ou=HomeOffice</value>
</constructor-arg>

```

- d. Edit the `multiOUUserSearch` bean list to match the number of OU search beans configured in the previous step. By default, the `searchFilterList` list contains references to `ldapOUsSearch1` and `ldapOUsSearch2`

```

<bean id="multiOUUserSearch"
class="com.graphon.goglobal.security.spring.MultipleOUUserSearch">
  <property name="searchFilterList">
    <list>
      <ref bean="ldapOUsSearch1"/>
      <ref bean="ldapOUsSearch2"/>
    </list>
  </property>
</bean>

```

- e. Locate `<bean id="ldapAuthoritiesPopulator">` and modify the value to contain the LDAP user or group designated as the gateway administrator.

```

<list>
  <value>CN=Universal,CN=Users,DC=goglob4,DC=com</value>
</list>

```

- f. Locate bean `<property name="defaultIDP" value="nordicedge.graphon.com"/>` and modify the value to match the `EntityDescriptor.entityID` attribute as defined in file `<tomcat_home>/webapps/portal/WEB-INF/classes/security/idp.xml`.

```

<property name="defaultIDP" value="portal.idp"/>

```

5. Edit idp.xml

Edit `<tomcat_home>/webapps/portal/WEB-INF/classes/security/idp.xml` to point to your NordicEdge server.

The Location of the following line should specify your NordicEdge host name

```
<SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="http://<your_nordic_edge_host>/necs/SAMLResponder"/>
```

6. Restart the gateway.

Nordic Edge Certificate Services (CS)

Beyond the initial setup and configuration of the Nordic Edge OTP and CS components, only the CS `necs.properties` file requires an additional line to integrate with the GO-Global Gateway. The following lines should be added to `necs.properties`:

```
# GraphOn Gateway Configuration
SAML.SP.gateway.domain.com_8080go-
global.DefaultAssertionConsumerURL=http://<goglobal_gateway.domain.com:
8080/go-global/saml/SSO
```

where `goglobal_gateway.domain.com` should be replaced with your host and domain name. Also modify the gateway port number if it is using a port other than 8080.

PREVENTING USERS FROM BYPASSING THE GATEWAY

By default, the host allows users to connect to it directly, start a session, and attempt to authenticate. If, however, the **AllowCreateSessionOnConnect** host property is set to false, users will only be able to sign in to the host via a gateway. In other words, users cannot even attempt to authenticate to a host unless an administrator has granted them access to the host in the gateway.

To set **AllowCreateSessionOnConnect** to false

1. Locate the file **HostProperties.xml** in one of the following directories:
C:\Documents and Settings\All Users\Application Data\GraphOn (On Windows XP and Windows 2003); C:\ProgramData\GraphOn (On Windows Vista, Windows 2008 and later)
2. Open **HostProperties.xml** in WordPad and locate the following section:
HostProperty.xml

```
<property id="AllowCreateSessionOnConnect" group="Miscellaneous" type="BOOL">
<value>true</value>
</property>
```
3. Change the **AllowCreateSessionOnConnect** value to **false**.
4. Save the file.

PERFORMANCE AUTO-TUNING

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 one of the following directories:
C:\Documents and Settings\All Users\Application Data\GraphOn (On Windows 2003);
C:\ProgramData\GraphOn (On Windows 2008).
2. Open **HostProperties.xml** in WordPad and locate the following section:

```
</property>
<property id="ClientProcessingBatch" group="Miscellaneous" type="UINT32">
<value>0</value>
</property>
```
3. Change the **ClientProcessingBatch** value from 0 to 1.

4. Stop and start the **GO-Global Application Publishing** Service.

Note: Make sure to create a backup of **HostProperties.xml** before making any changes.

Performance auto-tuning is enabled by default on the Flash Client. Administrators may want to disable it when it is necessary for every frame of an animation to be shown through GO-Global, or if there are display issues with specific applications.

To disable Performance Auto-Tuning for the Flash Client

1. Locate the file **HostProperties.xml** in one of the following directories:
C:\Documents and Settings\All Users\Application Data\GraphOn (On Windows 2003);
C:\ProgramData\GraphOn (On Windows 2008).
2. Open **HostProperties.xml** in WordPad and locate the following section:
</property>
<property id="ClientProcessingBatchFlash" group="Miscellaneous" type="UINT32">
<value>1</value>
</property>
3. Change the **ClientProcessingBatchFlash** value from 1 to 0.
4. Stop and start the **GO-Global Application Publishing** Service.

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 DWORD registry value. Here is the documented list of process redirector bits and a description of what they configure.

- **0x00000001*** - Prohibit a process from running within a session
- **0x00000002** - 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.
- **0x00000004** - 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.
- **0x00000008** - 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.

- **0x00000010*** - Disable the use of the GO-Global 'UI' skin module.
- **0x00000020*** - Enable the use of the GO-Global 'UI' skin module.
- **0x00000080*** - Enable the Windows ProcessIdToSessionId() API to return the GO-Global session ID.
- **0x00000100*** - On 64-bit systems, enable the Windows ProcessIdToSessionId() API to return the GO-Global session ID for 32-bit processes only. This is required for printing to work in 32-bit processes on 64-bit systems. Including this bit in settings for 64-bit processes has no effect.
- **0x00000200** - 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.
- **0x00000400** - 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.
- **0x00000800*** - Enable the Windows GetComputerName() API to return the client computer name.
- **0x00001000*** - 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.
- **0x80000000*** - 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.

** Indicates advanced options that should only be used if instructed to by your support contact.*

Note: 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. 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 | DWORD 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 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 host has the following applications installed:

- 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:

0x00000110 - These are the bits originally set in DefaultLoaderOptions.

0x00000800 - This is the bit that enables the Windows GetComputerName() API redirection.

0x00000910 – This is the hexadecimal DWORD 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:

0x00000110 - These are the bits originally set in DefaultLoaderOptions.

0x00000008 - This is the bit that disables Client Printing.

0x00000200 - This is the bit that disables Client Sound.

0x00000400 - This is the bit that disables Client Serial and Parallel Ports.

0x00000718 – This is the hexadecimal DWORD to be set in the DataProcessor.exe registry value.

The DataView.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.

0x00000110 - These are the bits originally set in DefaultLoaderOptions.

0x00000400 - This is the bit that disables Client Serial and Parallel Ports.

0x00000510 – This is the hexadecimal DWORD 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.

BROWSER-SPECIFIC LIMITATIONS

When users do not have a GO-Global Add-on (e.g., ActiveX Control, Firefox or Safari Plug-in) installed, there are browser-specific limits on the number of connections that can be opened per HTTP session that limit the number of instances of GO-Global that can be run simultaneously. These limits are as follows:

- Internet Explorer 7: 1 instance per browser process
- Internet Explorer 8: 5 instances per client computer
- Internet Explorer 8 in Compatibility Mode: 1 instance per client computer
- Mozilla Firefox: 5 instances per client computer
- Apple Safari: 1 instance per client computer

When these limits have been reached, the following message is displayed to the user:

Failed to connect to the gateway.

When running Internet Explorer in Compatibility Mode, users will only be able to sign in to one host at a time per browser session. In addition, if a user closes the window in which applications are displayed via its X button, the connection will not be released, and the user will not be able to reopen the application window within that browser session. If one of these limits is encountered in Internet Explorer 7, the workaround is to start a new instance of the browser.

If a user running Internet Explorer 8 connects to a gateway in Compatibility View mode, the workaround is to either disable Compatibility View mode or run Internet Explorer with the “-NoFrameMerging” command-line option. Otherwise, the user will not be able to run another instance of GO-Global until the HTTP session times out or the computer is restarted.

None of the above limits apply if a GO-Global Add-on is installed.

UNINSTALLING CLIENTS

To uninstall the Plug-in from Firefox

1. Start Mozilla Firefox.
2. Click Tools | Add-ons.
3. Click **Uninstall** in the GraphOn GO-Global section.
4. Close Mozilla Firefox.

After uninstalling GO-Global, it is recommended that users clear the Firefox browser cache.

To uninstall the Plug-in for Linux

1. Launch the Linux console.
2. Remove the Plug-in by typing:

```
rm -rf ~/.mozilla/plugins/libnpg.so ~/.mozilla/plugins/libpbr.so > ~/.mozilla/ gg-client
```

If you plan to reinstall the Plug-in, we recommend clearing the Firefox browser cache.

To uninstall the ActiveX from Internet Explorer

1. Start Internet Explorer.
2. Click Tools | Manage Add-ons.
3. Select **GO-Global 4**.
4. Click **Delete**. If there is no Delete button (e.g., in Internet Explorer 8):
 - a. Double-click **GO-Global 4**.
 - b. Click **Remove**.
 - c. Click **Close**.

If users have difficulty reinstalling and running the ActiveX Control, clear the browser cache. To do this, open Internet Explorer and click Tools | Internet Options. Click the **General** tab and under **Temporary Internet Files**, click **Delete Files**. Users should then check for any conflict directories using a Command Prompt window.

To check for conflict directories

1. Open a Command Prompt window.
2. Type the location of the **Downloaded program files** folder and check for any conflict directories. If any exist, delete them.
3. Close the Command Prompt window.

To uninstall the client on Windows

1. Open Control Panel.
2. Double-click **Programs and Features**.
3. Select **GO-Global Client**.

Click **Remove** (Windows XP or Windows Server 2003) or **Uninstall** (Windows Server 2008, Vista and above). Click **Yes** to proceed with the uninstall or **No** to cancel the uninstall.

INDEX

A

Access logs, 45, 65, 66
Active Directory, 12, 14, 33
Active Directory Configuration, 12
ActiveX Control, 24
Add Folder, 37
Add-on manager, 24, 25
Adobe AIR, 16, 25
Adobe Flash, 26
Adobe Flash Player, 25
ADSI Edit, 14
Apache Tomcat, 11, 12
Apple Safari, 106
Application Publishing Service, 61, 64
aps, 61
autoConfigPrinter, 76
Automatically install drivers, 77
Autoreconnect, 90

B

Backup, 64
Backup folder, 62
BLM, 96

C

CA, 58
CA certificate, 54, 56
CA key, 54, 55
ca.cfg, 56

ca.crt, 56, 58
CD ROM drive, 75
CD ROMs, 74
Central license server, 96
Certificate Authority, 51
Certificate Signing Request, 52, 55, 57, 58
Certificate Wizard, 58
Client drives, 74
Client file access, 74, 105
Client Installation, 24
Client Platforms, 10
Client printer name, 80
Client Printer Naming, 80
Client Printing, 102
Client Serial and Parallel Ports, 81
Client Sound, 105
Client time zone, 71
Client Time Zone, 102
Client updates, 49
Clipboard, 72
Close workspace, 40
Codes, 62
Common Name, 52, 56, 57
Compatibility Mode, 106
config.xml, 90
Content Pane, 32, 36
Copy, 38
CPU usage, 42, 66
Cut, 38

D

Database, 45, 65
 Database schema ID, 91
 DataDownloader.exe, 104, 105
 DataProcessor.exe, 104
 DataView.exe, 104
 Default printer, 79
 DefaultLoaderOptions, 105
 DES encryption, 59
 Desktop folder, 37, 86
 Details, 36
 Diagnostic Messages, 62
 DMZ, 88
 Document Sharing, 7, 37
 Domain, 32
 Domain Admins, 19
 Drag and drop, 36
 DVD-ROMs, 74

E

Encryption, 60
 Errors, 62
 Events, 62
 Explorer.exe, 103
 Export Logs, 45, 66

F

Firewall, 61, 96
 FLEXnet, 96
 floppy disks, 74
 Floppy drive, 75

G

Gateway Connector, 19
 Go Daddy, 53
 GO-Global Add, 26
 GO-Global Add-on, 25, 106
 GO-Global Display Driver, 17
 GO-Global Gateway service, 20
 GO-Global Host, 63
 GO-Global libraries, 73
 GO-Global License Manager, 96
 GO-Global Setup Program, 24

GO-Global Update Client service, 49
 Grace period, 84
 Group, 33
 Group policy, 26
 Group Policy Object, 25

H

Hide, 75
 High availability clusters, 90
 Home directory, 37
 Home page, 32
 Host Platforms, 9
 Host Port, 61
 hostid, 92
 HostProperties.xml, 66
 Hyperlink Access, 7

I

Icons, 32
 Idle limit, 83
 Idle time, 83
 InstallShield Wizard, 11
 intermediary certificate, 53
 Internal network, 88
 Internet, 88
 Internet Explorer, 106
 Internet Options, 54
 IP address, 42
 iwa-ldap-authentication.xml, 19

J

Java Runtime Environment, 11

L

License Manager Port, 96
 License Retrieval Wizard, 17
 License server, 96
 License-file list, 92
 License-file list redundancy, 94
 LM_LICENSE_FILE, 92, 94, 95, 96
 lmttools, 93
 Locality, 52
 Locality Name, 55, 57

Log Files, 64
Log folder, 64
Logon scripts, 72

M

MAC address, 80
Manage Sessions, 44
MappedPrinterDrivers.xml, 79
Master, 92
Maximum sessions, 47
Memory usage, 42, 66
Messages, 61
Microsoft Management Console, 58
MMC, 14
Modifying the Host Port Setting, 61
Mozilla Firefox, 24, 106

N

Native printer drivers, 77
Navigation Pane, 32

O

Open desktop, 39
Open Programs, 38
OpenSSL toolkit, 52, 54
Organization Name, 55, 57
Organizational Unit, 52
Organizational Unit Name, 56, 57
Organizational units, 33
Output Level, 62
Override parent's options, 69

P

Parallel Ports, 81
Paste, 38
PEM format, 58
Performance Auto-Tuning, 100
Plug-in, 24
Port, 61
PostgreSQL, 11
Printer drivers, 79
PrinterNameFormat, 80
Process ID, 42, 62

Process name, 42
Product Code, 17, 18
Proxy hosts, 90
Proxy printer names, 80

R

Red Hat, 12
redirection settings, 104
Redistributable Package, 11
Redundant license Servers, 92
Redundant servers, 92
Remapping drives, 74
Removable drives, 74
Resource limits, 65
Reverse proxies, 90
RPM database, 12
RSA private key, 55

S

Secure Socket Layer, 51
Security, 50
Security Alert, 59
Serial and Parallel Ports, 102, 105
Serial ports, 81
Server keys, 57
server.cfg, 56
server.crt, 55, 58
server.key, 55, 58
Session, 40
 encrypting, 59
Session ID, 41
Session limit, 82
Session Process Configuration, 102
Session shadowing, 44
Sessions, 47, 48
Sessions page, 41
Share, 37
Shortcut, 39
SSL, 51
SSL Certificate, 51, 59
SSL transport, 59
Start menu, 26
Support Request Wizard, 67
SUSE, 12

Suspend workspace, 40

T

TCP, 51

Templates, 62

Three-server redundancy, 92

Time limits, 40

Toggle navigation pane, 32

Toolbar, 34

Trace Messages, 62

Transmission Control Protocol, 51

U

Uninstalling, 30

Universal Driver, 77

Universal Printer Driver, 76

Update Client service, 25, 49

USB drives, 74

User Account Control, 11, 16, 20

User profiles, 37

V

VPN, 89

W

Warning period, 83

Warnings, 62

Web API, 7

Web applications, 7

web.xml, 12

Wildcard SSL certificates, 51

Windows folder, 77

Windows Logo testing, 17

Windows Printer Drivers, 76

Workspace, 37