

iGoldMine

Administrators Guide



VERSION 3.2 — 5.31.2007

COPYRIGHT AND TRADEMARK NOTICE

Copyright © 2007 FrontRange Solutions USA Inc. All Rights Reserved.

Window captures and dialog box sample views are the copyright of their respective owners.

USE OF THIS SOFTWARE AND ITS RELATED USER DOCUMENTATION IS SUBJECT TO THE TERMS AND CONDITIONS OF THE APPLICABLE END-USER LICENSE AGREEMENT (EULA), A COPY OF WHICH IS FOUND IN THE USER DOCUMENTATION. YOU MUST AGREE TO THE TERMS AND CONDITIONS OF THE EULA IN ORDER TO USE THIS SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THE EULA, PROMPTLY RETURN THE UNUSED SOFTWARE IN ITS UNOPENED CD PACKAGE TO THE PLACE FROM WHICH YOU OBTAINED IT FOR A REFUND.

WARNING: The software described in this manual and its related user documentation are protected by copyright law. In no event, shall any part of the related user documentation be copied, reproduced, distributed, transmitted, stored in a retrieval system, or translated into any language, without the express written permission of FrontRange Solutions USA Inc.

Contact FrontRange Solutions at our Web site: **www.frontrange.com**

(Dec. 2005) (iGoldMine 7121805)

Printed in the United States of America.

CONTACT INFORMATION

FrontRange Solution, Inc.
5675 Gibraltar Drive
Pleasanton, CA 94588

Direct: 925.404.1800
Sales: 800.776.7889
Fax: 925.404.1305

CONTENTS

Chapter I — Introduction

Introducing iGoldMine	p. 1
iGoldMine Features	p. 1
New iGoldMine Features	p. 3
System Requirements	p. 4

Chapter II — Configuring the Server

Installing the iGoldMine Server	p. 6
Manually Copying the License File	p. 7
Setting up the iGoldMine Server for Browser Logons	p. 7
Installing the Web Files on a System other than the iGoldMine Server	p. 8
Redundant License Servers	p. 8
Three-Server Redundancy	p. 8
License-File List Redundancy	P. 9
Configuring iGoldMine to use a Central License Server	p. 10
Configuring Support for Client Keyboards and/or IMEs	p. 11
Installing Additional Keyboards and IMEs	p. 12
Keyboard/IME Identifiers Used by iGoldMine	p. 14
Configuring Client Keyboard Options	p. 14
Client Keyboard Mapping Files	p. 15
Specifying Layout Text Substitutions	p. 16
Setting the Fallback IME Layout Text	p. 17
Keyboard Layouts Behind the Scenes	p. 17
Configuring Multiple Input Locales	p. 18

Chapter III — Administering User Accounts

Administering User Accounts	p. 20
Setting up User Profiles	p. 21
Setting File Permissions	p. 21
Setting up a Network Printer	p. 21

Chapter IV — The Cluster Manager

The Cluster Manager	p. 22
Managing Applications	p. 23
Installing Applications	p. 23
Adding Applications	p. 24
Editing an Application's Properties	p. 25
Duplicating an Application	p. 25
Renaming an Application	p. 26
Assigning Application Launch Parameters to Users or Groups	p. 26
Removing Applications	p. 27
Managing Sessions and Processes	p. 27
Terminating a Session	p. 27
Ending a Process	p. 27
Shadowing a Session	p. 27
Security Options	p. 29
Selecting SSL Transport	p. 29
Obtaining a Trusted Server Certificate	p. 29
Importing the Certificate on a Dependent Application Server	p. 30
Creating Your Own Certificate Authority	p. 31
Creating a CA Key and Certificate	p. 32
Creating and Signing Server Keys	p. 33
Generating a CSR Using IIS Certificate Wizard	p. 34
Notifying Users of a Secure Connection	p. 35
Encrypting Sessions	p. 35
Modifying the Host Port Setting	p. 36
Standard Authentication	p. 37
Integrated Windows Authentication	p. 38
Server-Side Password Caching	p. 39
Client-Side Password Caching	p. 39
Password Change	p. 41
Changing Passwords at Next Logon	p. 41
Prompting Users to Change Passwords Before Expiration	p. 42
Prompting Users to Change Passwords After Expiration	p. 43
Password Change and Integrated Windows Authentication	p. 43

Chapter IV — The Cluster Manager (continued)

Session Reconnect	p. 44
Setting the Session Termination Option	p. 44
Disconnecting a Session	p. 44
Shared Account	p. 45
Client Time Zone	p. 46
Monitoring Server Activity	p. 46
Viewing Session Information	p. 46
Viewing Process Information	p. 47
Refreshing the Cluster Manager	p. 47
Setting the Refresh Rate	p. 47
The Status Bar	p. 48
Setting the Broadcast Interval	p. 48
Session Startup Options	p. 49
Applying Group Policy	p. 49
Displaying Progress Messages	p. 50
Logon Scripts	p. 50
Setting Resource Limits	p. 52
Specifying the Maximum Number of Session	p. 53
Session Shutdown Options	p. 53
Specifying the Session Limit	p. 53
Specifying the Idle Limit	p. 54
Specifying the Warning Period	p. 55
Specifying the Grace Period	p. 55
Managing iGoldMine Servers from Client Machines	p. 56
Keyboard Shortcuts for the Cluster Manager	p. 57

Chapter V — Running the iGoldMine Client

Overview of iGoldMine Clients	p. 58
Preparing the iGoldMine Server for Web Access	p. 59
Java Client	p. 61
Startup Parameters for the Java Client	p. 61
Uninstalling the Java Client	p. 62
Netscape Plug-in	p. 63
Running the Netscape Plug-in for Windows	p. 63
Uninstalling the Netscape Plug-in for Windows	p. 63
Running the Netscape Plug-in for Linux	p. 63
Uninstalling the Netscape Plug-in for Linux	p. 64
Startup Parameters for the Netscape Plug-in	p. 64

Chapter V — Running the iGoldMine Client (continued)

ActiveX Control	p. 65
Startup Parameters for the ActiveX Control	p. 65
Uninstalling the ActiveX Control	p. 67
Windows Client	p. 67
Running the Windows Client from the Start Menu	p. 67
Running the Windows Client from a Shortcut	p. 68
Creating iGoldMine Shortcuts	p. 68
Command-Line Arguments for the Windows Client	p. 68
Uninstalling the Windows Client	p. 69
Linux Client	p. 69
Command-Line Arguments for the Linux Client	p. 70
Resizing the Client Window of the Linux Client	p. 70
Uninstalling the Linux Client	p. 70
Mac OS X Client	p. 71
Command-Line Arguments for the Mac OS X Client	p. 71
Resizing the Client Window of the Mac OS X Client	p. 72
Uninstalling the Mac OS X Client	p. 72
Browser Plug-in for Mac OS X	p. 72
Startup Parameters for the Browser Plug-on for Mac OS X	p. 73
Uninstalling the Browser Plug-in for Mac OS X	p. 74
Windows CE Client	p. 74
Installing the Windows CE Client	p. 74
Running the Windows CE Client from the Start Menu	p. 75
Running the Windows CE Client from a Shortcut	p. 76
Running the Windows CE Client from the Executable	p. 76
Command-Line Arguments for the Windows CE Client	p. 76
Including iGoldMine in a Windows Based Terminal CE Image	p. 77
Running the Windows CE Client on a WBT Device	p. 77
Uninstalling the Windows CE Client	p. 78
Pocket PC Client	p. 78
Installing the Pocket PC Client	p. 78
Running the Pocket PC Client from the Start Menu	p. 79
Running the Pocket PC Client from the iGoldMine Executable	p. 79
Using the Pocket PC Client	p. 80
Uninstalling the Pocket PC Client	p. 80

Chapter VI — Advanced Topics

Load Balancing	p. 81
Independent Application Servers	p. 81
Relay Servers	p. 82
Dependent Application Servers	p. 83
Administering Relay and Dependent Application Servers on Different Networks	p. 84
Client Printers in a Multi-user Environment	p. 85
Server Selection	p. 85
Relay Server Failure Recovery	p. 86
iGoldMine Server Performance Counters	p. 86
Configuration Requirements for Delegation Support	p. 87
Client Printing	p. 90
Configuring a Client Printer	p. 91
Enabling Support for Client Printers	p. 93
Enabling Client Printer Caching	p. 93
Designating Access to Printer Drivers	p. 94
Client Printer Naming Customization	p. 96
Client Sounds	p. 97
Clipboard Support	p. 97
Client File Access	p. 98
Remapping Client Drives	p. 98
Hiding Client Drives	p. 100
Hiding Server Drives	p. 101
Mapped Drives	p. 101
Obtaining the Name of the Client Computer	p. 102
Application Script Support	p. 102
Process Loader Options	p. 103
Proxy Tunneling	p. 104
Proxy tunneling via the HTTP CONNECT method	p. 104
Enabling Support for PAE	p. 105
Automatic Windows Update and Hotfix Compatibility	p. 105
Log Files	p. 106
Selecting a New Location for the Log Files	p. 106
Setting the Output Level	p. 107
Maintaining Log Files	p. 107
Serial and Parallel Port Redirection	p. 108

Introducing iGoldMine

iGoldMine is a server-based, thin-client solution that eliminates the need for Citrix MetaFrame or Windows Terminal Services. It is optimized for reliable, secure, scalable application delivery to virtually any network-attached device, regardless of platform or operating system. iGoldMine for Windows is a complete application deployment solution that can be integrated and bundled with any 32-bit Windows application.

iGoldMine Features

- **Network, remote dial-up, and remote Web accessibility.** iGoldMine provides access to 32-bit Windows-based applications from iGoldMine Servers via the network, remote dial-up, or through Web access. This is managed through the Cluster Manager, and is transparent to the end user.
- **Cross-platform compatibility.** iGoldMine provides access to any Windows application from virtually any client platform. Applications can be run from desktop computers such as Macintosh, Windows, and Linux—allowing users to work in their preferred computing environments. Windows-based applications deployed through iGoldMine look, feel, and function as if they were running on a Windows operating system, regardless of the client platform.
- **Client printing.** iGoldMine provides transparent access to client-side printers and produces printed output with the highest quality possible. In most cases, iGoldMine will determine the list of printers installed on the client computer, along with the printer driver and port for each client printer. If a printer driver is not installed on the server, iGoldMine will attempt to automatically install the driver. If a driver cannot be automatically installed, users can configure printer drivers using the Program Window's Client Printer Wizard.
- **Client sounds.** iGoldMine supports sound capability for applications that use PlaySound, sndPlaySound, or waveOut. It is not required that sound cards and/or speakers be installed on iGoldMine Servers. The client machine, however, does require a sound card and speakers.

- **Client file access.** iGoldMine supports seamless integration of client drives, including floppy, CD-ROM, hard disk, and mapped network drives. This allows users to access files stored on the client computer and to save files locally.
- **Server monitoring.** iGoldMine provides real-time monitoring of individual iGoldMine Servers, control of individual clients and processes, and logout and shutdown for individual users.
- **User roaming.** Internal and remote users can log on to an iGoldMine Server from any client workstation.
- **Session shadowing.** The session shadowing feature allows multiple users to view and control a single session and its applications. This feature allows help desk personnel and system administrators to help troubleshoot and debug user problems. Session shadowing may also be used for live collaboration.
- **Load balancing.** Load balancing distributes user sessions across multiple iGoldMine Servers. When load balancing is enabled, users can reconnect to a disconnected session running on any one of the load-balanced servers.
- **Session reconnect.** With session reconnect enabled, iGoldMine maintains client sessions on the server without a client connection. If a user deliberately disconnects from the server, or if the client's connection is lost due to network problems, the user's session and applications remain running on the server for the length of time specified by the administrator.
- **Performance Counters.** New performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a server. iGoldMine Server performance counters allow administrators to monitor server activity from any machine with network access to an iGoldMine Server.
- **Proxy Tunneling.** Proxy tunneling allows users to connect to iGoldMine Servers on the Internet via proxy servers.
- **Universal Printer Driver.** The Universal Printer Driver allows users that have a PDF viewer such as Adobe Reader installed on their computers to print to any client printer.
- **Group Policy Support.** Using Microsoft's Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options.
- **Drive Letter Mapping.** Through the Cluster Manager, administrators can hide client and server drives and remap client drives.
- **SSL Security.** iGoldMine provides support for Secure Socket Layer (SSL) as a method for communication between iGoldMine clients and servers.
- **Session Timeout.** Through the Cluster Manager administrators can specify time limits for the number of minutes that sessions are allowed to run on an iGoldMine Server.
- **Solaris Client.** The Solaris Client is a lightweight X based application that delivers excellent performance to Solaris desktops.
- **Inactivity Timeout.** Through the Cluster Manager administrators can specify time limits for the number of minutes of client inactivity.
- **Client Printer Name Customization.** Administrators can specify the format of client printer names and include information (including the user's name, the name of the session, and the client computer's IP address) in the name of the client printer.

New iGoldMine Features

- **Client-Side Password Caching.** With this feature, the user's user name and password are taken from the Logon dialog after the first manual authentication. These credentials are encrypted and transmitted to the client system. When the user makes subsequent connections to the server, the cached password is transmitted back to the server, where it is decrypted and then used to automatically log the user on to the iGoldMine Server.
- **Time Zone Redirection.** This option allows iGoldMine sessions to run in the time zone of the client computer, regardless of the time zone that is selected on the iGoldMine Server.
- **Backward Compatible Client and Server.** This allows a client to connect to an iGoldMine Server when the major and minor versions of the client and server match but the revision (service pack) or build numbers do not.
- **Relay Server Enhancements.** Dependent application servers can be located on a different network than their associated relay server. For example, dependent application servers can be located behind a firewall on an internal, Active Directory network, and the associated relay server can be located in a demilitarized zone (DMZ) outside the firewall.
- **Session Shadowing Notification.** iGoldMine notifies users when someone connects to their session and allows users to deny access.
- **Automatic License Retrieval and Installation.** Using iGoldMine's License Retrieval Wizard, administrators can automatically obtain a license file from the GraphOn license server and install the license file.
- **Automatic Windows Update and Hotfix Compatibility.** This feature automatically detects the locations of the internal operating system variables and functions used by iGoldMine. This ensures that virtually every time the system is booted, users are able to start sessions and run published applications regardless of what Windows Updates and Hotfixes are installed on the system.
- **Mac OS X Client.** This lightweight application provides seamless integration with the native Mac OS X environment. Users running Mac OS 10.3 and 10.4 can download and install iGoldMine.dmg, and then run iGoldMine from the Applications directory.
- **Browser Plug-in for Mac OS X.** Mac OS X users running Apple Safari or Mozilla Firefox can browse to an HTML page where they can install and run the iGoldMine plug-in.
- **Pocket PC Client.** This lightweight application provides seamless integration with the native device's environment. Mobile users can run the Pocket PC Client from the Start menu or directly from the iGoldMine executable.
- **Enhanced Feature Support for Windows CE Clients.** The Windows CE Client supports SSL security, serial port redirection, client audio support, and client printing.
- **Enhanced Feature Support for the Mac OS X Clients.** The Mac OS X Client and the Browser Plug-in for Mac OS X support SSL security, client printing, and limited client audio support.

System Requirements

iGoldMine Server

The iGoldMine Server requires one of the following Windows operating systems:

- Windows Server 2003 Standard or Enterprise Edition with Service Packs 1 and 2
- Windows Server 2003 R2 Standard or Enterprise Edition
- Windows XP Professional with Service Pack 2

Where applicable, these platforms are supported with or without the Security Rollup Package. Right-to-left languages are not supported.

iGoldMine Administrators must have administrative rights on the server to perform the installation, and the server must have TCP/IP as a network protocol.

A Web Server (for example, Microsoft Internet Information Server (IIS) or Apache HTTP Server) must be available in order to set up the server for browser deployment of iGoldMine.

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

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

iGoldMine Clients

Users can connect to an iGoldMine Server from any computer that supports an iGoldMine client. The following clients are available:

- The **Netscape Plug-in** lets users connect to an iGoldMine Server using Netscape Navigator. To connect to an iGoldMine Server, users simply browse to an HTML page that contains a link to the Plug-in. If the Plug-in is already installed on the client machine, it is automatically loaded and run by the browser. Otherwise, users are prompted to download the Plug-in and install it on the desktop computer. The Netscape Plug-in is available for Windows and Linux clients.
- The **Microsoft ActiveX Control** is available to Windows users running Internet Explorer. The ActiveX Control is automatically installed the first time a user accesses the HTML page containing the ActiveX Control.
- The **Windows Client** is a 32-bit Windows application that can be installed and run on most Windows computers.
- The **Windows CE Client** is a lightweight application that provides seamless integration with the native device's environment. Windows CE users can run iGoldMine from the Start menu, a desktop shortcut, or directly from the iGoldMine executable.
- The **Pocket PC Client** is a lightweight application that provides seamless integration with the native device's environment. Mobile users can run the Pocket PC Client from the Start menu or directly from the iGoldMine executable.
- The **Linux Client** is a lightweight native X Window Systems application that delivers excellent performance to Linux clients. Users can install the Linux Client and run iGoldMine from the Linux console.
- The **Mac OS X Client** is a lightweight application that provides seamless integration with the native Mac OS X environment. Users can download and install iGoldMine.dmg and run iGoldMine from the Applications directory.

- The **Browser Plug-in for Mac OS X** is available to Mac OS X users running Apple Safari or Mozilla Firefox. Users browse to an HTML page that contains a link to the Plug-in.
- The **Java Client** is available to Windows and Linux users. When running from a browser, users launch iGoldMine by browsing to an HTML page containing the Java applet. The browser automatically downloads the iGoldMine Client classes and launches the applet.

Installing the iGoldMine Server

iGoldMine is delivered as a self-extracting executable and can be installed by double-clicking the executable. It can also be unpacked and installed by running **setup.exe** in the root folder where it was unpacked. The setup installs all of the iGoldMine Server files as well as the files necessary to configure the iGoldMine Server for browser logons. After installing iGoldMine you will need to restart the server, then copy your license file into the Programs directory in the iGoldMine install path.

You can install the iGoldMine Web files on a system other than the iGoldMine Server if you plan to distribute the signed version of the Java Client, the Netscape Plug-in for Windows and Linux, and/or the ActiveX Control. Other iGoldMine clients will not be supported.

You will need the Product Code supplied by your FrontRange Solutions sales representative in order to complete the License Setup. If you do not have a Product Code and wish to obtain a temporary demo license, type **demo** in the **Product Code** box.

Note: Minimum permissions for the license file (license.lic) are:
Administrators: Full Control; **Users:** Read & Execute; **SYSTEM:** Full Control

After installing iGoldMine and running the License Retrieval Wizard, you will need to restart the server and then verify that the **Application Publishing Service** is running.

To verify that the Application Publishing Service is running

1. Click the **Start** button on the Windows taskbar.
2. Click Control Panel | Administrative Tools.
3. Double-click **Services**.
4. Find **iGoldMine Application Publishing Service** in the list of services.
5. Verify that the Application Publishing Service has "Started" and that the Startup is "Automatic."

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

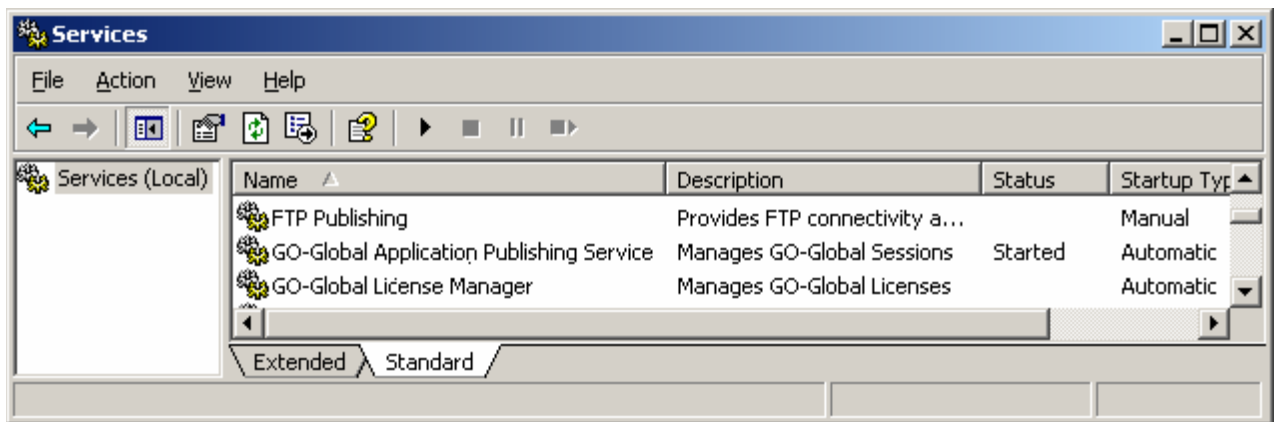
Manually Copying the License File

If you choose not to run the **License Retrieval Wizard**, you can copy your license file into the Programs directory in the iGoldMine install path. If you have configured iGoldMine to use a central license server, copy the license file to the license server. (For more information, see the section **Configuring a Central License Server** below.)

Once the license file has been copied over, you will need to stop and restart the **iGoldMine Application Publishing Service**.

To start the Application Publishing Service

1. Click the **Start** button on the Windows taskbar.
2. Click Settings| Control Panel | Administrative Tools.
3. Double-click **Services**.
4. Select **iGoldMine Application Publishing Service** from the list of services.
5. Click the **Start** button.



When the Application Publishing Service is stopped, all existing iGoldMine sessions and their applications will be terminated, and clients will not be able to log on to the server or start an application using iGoldMine. The iGoldMine installation configures the Application Publishing Service so that it starts automatically.

Setting up the iGoldMine Server for Browser Logons

The iGoldMine setup allows you to install the iGoldMine Web files directly into a sub-directory of your Web server home directory (for example, C:\InetPub\wwwroot\goglobal). During the setup, a dialog will prompt you to specify your Web server as **Microsoft Internet Information Server (IIS)**, **Apache HTTP Server**, or **None of the above**. If you select one of the first two, the setup will detect the location of your Web server's home directory and copy the files into a sub-directory of this location. If you select **None of the above** or the setup fails to detect the Web server's location, the files will be copied along with the rest of the iGoldMine files and you will have to copy the files manually into your Web server home directory after the setup. (The default HTML page for Web deployment is logon.html.)

To copy the Web files to the Web server home directory

1. Locate the iGoldMine Web files directory. The default iGoldMine Web files directory is \SYSTEM_DRIVE\FrontRange\iGoldMine Server\Web.
2. Copy the files from this directory to your Web server home directory. For example, using Microsoft IIS you would copy these files to the \InetPub\wwwroot folder on your server, or any other directory that you would like to specify as your Web server home directory.

Installing the Web Files on a System other than the iGoldMine Server

You can install the iGoldMine Web files on a system other than the iGoldMine Server if you plan to distribute the signed version of the Java Client, the Netscape Plug-in for Windows and Linux, and/or the ActiveX Control. Other iGoldMine clients will not be supported.

To install the Web files on a system other than the iGoldMine Server

1. During the iGoldMine Server installation you will be asked what Web server you are using. Select **None of the above**. The Web files will be placed in the following directory:
... \iGoldMine Server\Web
2. Copy the directory to the appropriate Web server.
3. Modify the appropriate HTML page on the Web server and put the iGoldMine Server name in the value for *Host* (the syntax will vary depending on whether you are using the signed Java Client or the ActiveX or embedded clients.)

Redundant License Servers

If you wish to use redundant 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 iGoldMine Server 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.

iGoldMine 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

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 iGoldMine Servers as well as the hostids (Ethernet addresses, in most cases) for each.

```
SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
DAEMON blm
INCREMENT session blm 3.200 31-dec-2007 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 3.200 31-dec-2007 uncounted D1D222D031C4 \
HOSTID=ANY
```

The three-server license file needs to be copied to each of the three license servers. Add the same port number on each server line. The iGoldMine Servers that will be using the license servers must have a license file such as the following:

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

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 **iGoldMine Application Publishing Service** and the **FrontRange License Manager** on the "master" server first (wilson, in the example above), then on the secondary and tertiary servers.

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

You can obtain Imtools from the Programs directory (`\iGoldMine Server\Programs`) or from Macrovision's Web site:

http://www.macrovision.com/support/by_category/fnp_utilities_download.shtml. The Imtools application is included for diagnostic purposes. Any questions on its functionality should be directed to Macrovision.

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. iGoldMine 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 FrontRange Solutions 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 3.200 permanent 5 DF9C8F5ADF34 HOSTID=ANY \
    user_info="Joe User joeu@mycompany.com" ISSUER="GraphOn \
    Corporation" ISSUED=17-feb-2007 NOTICE="Copyright (C) \
    1996-2007 GraphOn Corporation. All Rights Reserved" ck=142 \
    SN=12865-AA
INCREMENT any_app blm 3.200 permanent 5 1DF84A360E8F HOSTID=ANY \
    user_info=" Joe User joeu@mycompany.com " ISSUER="GraphOn \
    Corporation" ISSUED=17-feb-2007 NOTICE="Copyright (C) \
    1996-2007 GraphOn Corporation. All Rights Reserved" ck=84 \
    SN=12865-AA
```


License 2 for tokyo:

```

SERVER tokyo 00508BF77F7E 27000
DAEMON blm
INCREMENT session blm 3.200 permanent 5 16BE40E1D98D HOSTID=ANY \
    user_info="Joe User joeu@mycompany.com" ISSUER="GraphOn \
    Corporation" ISSUED=17-feb-2007 NOTICE="Copyright (C) \
    1996-2007 GraphOn Corporation. All Rights Reserved" ck=142 \
    SN=12865-AA
INCREMENT any_app blm 3.200 permanent 5 6DB6F3E402DF HOSTID=ANY \
    user_info=" Joe User joeu@mycompany.com " ISSUER="GraphOn \
    Corporation" ISSUED=17-feb-2007 NOTICE="Copyright (C) \
    1996-2007 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\iGoldMine Server\Programs** to reflect the new redundant servers. Separate the license server names with a semicolon (;). iGoldMine will attempt the first server in the list. If that fails for any reason, the second server is tried.
5. Restart the **iGoldMine 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 iGoldMine to use a Central License Server

Two methods can be used for configuring iGoldMine 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 iGoldMine Server. We recommend stopping the iGoldMine License Manager on the iGoldMine Server before getting started.

To stop the iGoldMine License Manager

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

Once you have stopped the FrontRange License Manager on the iGoldMine Server, you may proceed with one of the following methods for configuring a central license server:

On the iGoldMine Server, 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 iGoldMine Server, place USE_SERVER directly after the SERVER line in the license file on the iGoldMine Server. This is essentially the same as the preceding method but the change to the environment variable is not required. For example, License.lic file on iGoldMine Server (MACHINE-W2K) would appear as follows:

```
SERVER machine550 00d0b74f4023
USE_SERVER
DAEMON blm
INCREMENT session blm 3.200 30-oct-2007 2 9B41E3CD6E2C
HOSTID=00d0b74f4023
INCREMENT notepad blm 3.200 30-oct-2007 2 50476E23564E
HOSTID=00d0b74f4023
INCREMENT wordpad blm 3.200 30-oct-2007 2 4413BAE25745
HOSTID=00d0b74f4023
INCREMENT winword blm 3.200 30-oct-2007 2 53FDE4CA6038
HOSTID=00d0b74f4023
```

or in the case of a permanent license:

```
SERVER machine1550 00d0b74f4023
USE_SERVER
DAEMON blm
FEATURE session blm 3.200 permanent 5 9BB7562D18C5 ck=94
FEATURE winword blm 3.200 permanent 5 05B0813E18CA ck=96
```

Configuring Support for Client Keyboards and/or IMEs

Windows uses input languages, keyboard layouts, Input Method Editors (IME), and code pages to map keys on a keyboard to the characters on the display. When a key is pressed on the client's keyboard, iGoldMine sends a key code to the server, and the server translates the key code into a Windows input message using the session's active keyboard layout. The iGoldMine setup configures the server to support clients that use the same operating system, keyboard, and/or IME as the server. To support clients with different operating systems, keyboards, and/or IMEs some configuration needs to be performed. This is due to the fact that the identifiers used to identify keyboards and IMEs can be different on different versions of the Windows operating systems (specifically Windows 98) and the identifiers are not used at all by Java, UNIX, or Linux.

The following section describes mechanisms and procedures to manage keyboards and IMEs in sessions on client computers that do not match the server system.

Installing Additional Keyboards and IMEs

Before clients can use keyboards and/or IMEs that are different from the server's, the files used to support them must be installed on the iGoldMine Server. In most cases the layouts are copied during the installation of the operating system, but East Asian and right-to-left input languages are not.

To install keyboard layouts on a server running Windows XP or Windows Server 2003

1. From the Start menu, click Control Panel.
2. Double-click the Regional and Languages Options icon.
3. Click the **Languages** tab.
4. In the **Supplemental language support** box, click the check boxes next to the desired language groups.
5. Click **OK**.
6. Additional files will be copied to your machine. You may need to provide the Windows XP or Windows Server 2003 CD or the network share name.
7. Support for the new languages will become available after restarting.

Note:

Windows XP with Service Pack 2 supports a number of input locales that are not available on Windows Server 2003. Make sure the iGoldMine Server's operating system can support all the input locales required by all users.

The following is a list of keyboards that each iGoldMine client supports.

The **Linux Client** supports:

Linux Keyboard Layout Name(s)	Linux Keyboard Layout	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S. English	us	English (United States)	US	00000409	us.kbm
Japanese	jp	Japanese	Japanese (106/109 Key)	E0010411 (IME)	jp.kbm
French	fr	French (France)	French	0000040C	fr.kbm
Belgian (be-latin1)	be	French (Belgian)	Belgian French	0000080C	be.kbm
German, German (Latin1), German (Latin1 w/ no dead keys)	de	German (Germany)	German	00000407	de.kbm
Polish	pl	Polish	Polish (214)	00010415	pl.kbm
Brazilian (ABNT2)	br	Portuguese (Brazil)	Portuguese (Brazilian ABNT2)	00010416	br.kbm
*See the Client Keyboard Mapping Files section below for more information.					

The **Mac OS X Client** supports:

Mac OS X Keyboard Layout Name	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S.	English (United States)	U.S. International	00020409	us.kbm
French	French (France)	U.S. International	00020409	fr.kbm
German	German (Germany)	U.S. International	00020409	de.kbm
*See the Client Keyboard Mapping Files section below for more information.				

Note:

Due to physical differences between the Mac OS X and Windows keyboards, the Mac OS X keyboard mapping files use the **U.S. International** Windows keyboard layout to translate a majority of the keys to Windows applications.

The **Windows CE Client** supports:

Windows CE Keyboard Layout Name	Windows CE VM Language	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
English US	en	English (United States)	US	00000409	<i>internal</i>
Japanese	jp	Japanese	Japanese (106/109 Key)	E0010411 (IME)	ja_JP.kbm
French	fr	French (France)	French	0000040C	fr.kbm
German	de	German (Germany)	German	00000407	de.CH.kbm
*See the Client Keyboard Mapping Files section below for more information.					

The **Java Client** supports:

Windows		
English US	VM language = en	Windows Keyboard Layout = 00000409
Chinese	VM language = zh	Windows Keyboard Layout = 00000804
Japanese	VM language = ja	Windows Keyboard Layout = 00000411
French	VM language = fr	Windows Keyboard Layout = 0000040C
German	VM language = de	Windows Keyboard Layout = 00000407

Windows clients (including the native Windows Client, the ActiveX Control, and the Netscape Plug-in) support any keyboard that the iGoldMine Server has drivers for, provided iGoldMine is properly configured.

Keyboard/IME Identifiers Used by iGoldMine

iGoldMine uses two identifiers, collectively known as **iGoldMine Input Identifiers** (GGII), to specify a keyboard/IME for a session. The first is a keyboard layout. These are 8-digit string identifiers that Windows operating systems use to load keyboard drivers and IME programs. They are similar to locale IDs in that the last four digits typically match the 4-digit locale ID of the language supported by the keyboard. Keyboard layouts that specify an IME typically start with an "E". The list of available keyboard layouts can be viewed in the registry under the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts] key.

The second identifier used by iGoldMine is the layout text string, which is a registry value of each keyboard layout registry key. These strings are displayed in the dropdown box under Keyboard layout/IME when adding input languages.

In the following examples, the first has a keyboard layout GGII of 00000409 and a layout text GGII of US. The second example has a keyboard layout GGII of E0010411 and a layout text GGII of Japanese Input System (MS-IME2002).

Examples:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\00000409
Layout File = KBDUS.DLL
Layout Text = US
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\E0010411
Ime File = imejp81.ime
Layout File = Kbdjpn.dll
Layout Text = Japanese Input System (MS-IME2002)
```

Configuring Client Keyboard Options

You can specify the keyboard/IME for a session using the command-line argument `-kb` or the plug-in/applet parameter `"keyboard"`. These take both types of GGII's described above. The plug-in/applet parameter, for example, can be used to create Web pages that initialize the client with different keyboards.

If the `-kb` command-line argument is not specified, the Windows Client will use the layout text of the currently active keyboard layout on the client. The Java and Linux Clients do not send a layout text to the server if one is not specified on the command-line.

Examples:

Windows Client command-line using a keyboard layout:
`ggw.exe -h server1 -kb 00000409`

Java Client using a layout text:

```
<applet code= "com.graphon.ggw.Logon" Width="800" Height="600"
archive= "ggw.jar,ggw.res.jar">
<param name= "keyboard" value = "Japanese Input System (MS-IME2002)">
<param name= "user" value= "guest">
<param name= "password" value= "guest">
<param name= "host" value= "host">
</applet>
```

Client Keyboard Mapping Files

The Linux Client, Mac OS X Client, and the Windows CE Client support client keyboard mapping files. These clients use keyboard mapping files to ensure that the proper keyboard layout is loaded on the server and that the correct key codes are sent for each key press and release. Keyboard mapping files allow support for new keyboards to be added by simply copying a new keyboard mapping file to the client. Keyboard mapping files are installed into the **/etc/ggw/kbd** directory of these clients. An internal version of the **us.kbm** keyboard mapping file will be used if a keyboard mapping file is not found.

These clients can automatically load keyboard mapping files based on information obtained from the operating system.

The Keyboard Mapping File Installation Locations (i.e., default root paths)

Client OS	Native Install	Browser Plug-in Install	Default Layout	Layout Obtained by...
Linux	/etc/ggw/kbd	~/.mozilla/ggw/kbd	U.S. English	Environment variable or automatically from the OS
Mac OS X	/etc/ggw/kbd	/etc/ggw/kbd	U.S.	Environment variable or automatically from the OS
Windows CE	/GraphOn/iGoldMine Client/kbd	N/A	en	Automatically from the OS

Environment Variable	Description
GGW_KBD_FILE	This environment variable is used to specify the fully qualified path name of the mapping file to use. If specified, this will override all other means of obtaining the filename path. For example: On Linux, GGW_KBD_FILE=/home/someuser/KeyMappingFiles/MyCustomKeyMappingFile.kmf will cause that exact file to be loaded. If that file is not found the internal version of the us.kbm keyboard mapping file will be used.
GGW_KBD_FILE_ROOT	This environment variable is used to specify the root path name to the keyboard mapping files. The kbd directory that contains the keyboard mapping files will be expected to be in this directory. For example: On Linux, GGW_KBD_FILE_ROOT=/home/someuser , will cause the file /home/someuser/kbd/xxx.kbm to be loaded, where 'xxx' indicates the LAYOUT obtained from the following GGW_KBD_FILE_LAYOUT environment variable or automatically from the OS.
GGW_KBD_LAYOUT	This environment variable is used to specify which LAYOUT (or file name prefix) to use. This LAYOUT name along with the appended .kbm extension will be used as the file name. For example: GGW_KBD_LAYOUT=MyCustomKeyMappingFile will load the file /etc/ggw/kbd/MyCustomKeyMappingFile.kbm . If the above example for GGW_KBD_FILE_ROOT is also used, the file /home/someuser/kbd/MyCustomKeyMappingFile.kbm will be loaded. A subdirectory of the root path name to the mapping files can also be included here. For example: GGW_KBD_LAYOUT=thinclient/us will load /etc/ggw/kbd/thinclient/us.kbm provided a different root path is not specified. This will override the LAYOUT obtained automatically from the OS.

Notes:

Previous versions of the Linux Client use the command-line argument `-kb` and the plug-in/applet parameter "keyboard" to inform the server of the correct keyboard layout. For example, `-kb 0000040C` would override the environment variable `LANG = en_US` and cause the server to use the **French keyboard layout**. This is no longer recommended. Each keyboard mapping file contains the correct **keyboard layout** value that the server should use. Specifying a different **keyboard layout** with the command-line argument `-kb` or the plug-in/applet parameter "keyboard" could cause the keys to operate in undefined ways.

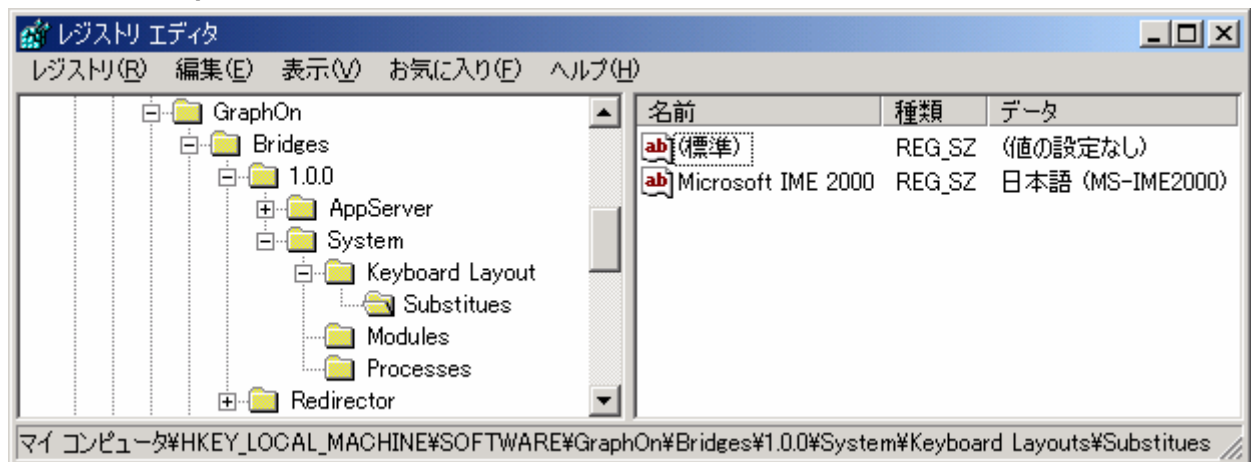
The command-line argument `-kb` and the plug-in/applet parameter "keyboard" can still be used to load an IME by specifying a **layout text**. For example, `-kb "Japanese Input System (MS-IME2002)"` can be used to load the Japanese IME available with Microsoft Office XP and Windows XP.

Specifying Layout Text Substitutions

Layout text substitutions can be specified on the server to map between client and server keyboard layout names. They can be used to:

1. Overcome differences in layout text names on different versions of Windows. For example, the **Japanese Input System (MS-IME2000)** layout text from a Windows 2000 iGoldMine client system can be substituted with the **Japanese Input System (MS-IME2002)** layout text from an iGoldMine Server running Windows Server 2003.
2. Substitute an ANSI name for a keyboard layout that has a UNICODE name. For example, when specifying a keyboard layout with a UNICODE name through the "keyboard" applet parameter in an ASCII HTML page, it is necessary to substitute an ASCII name for the UNICODE name.

Keyboard Layout Substitutions are specified under the [HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\Bridges\1.0.0\System\Keyboard\Layout\Substitues] registry key. Each REG_SZ value within this key has the name of a GGII, and the value is the name of a layout text from the server that should be used in place of the client name.

Example:

Setting the Fallback Layout Text

If there is no GGII specified from the client, or the one specified fails to load a valid keyboard layout, the iGoldMine Server uses a fallback mechanism to determine which keyboard layout should be used for the session. The fallback layout text should be the layout text for the keyboard layout that will be used by all clients connecting to the server, exclusive of those passing a valid GGII. The fallback layout text is automatically set during installation if the keyboard layout that is active is an IME. It may be modified after installation by editing the **Fallback Layout Text** value under the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\Bridges\1.0.0\System\Keyboard Layout

This functionality is typically used to automatically load an IME for the Java Client.

Keyboard Layouts Behind the Scenes

If the mechanisms described above are unable to provide the session with a keyboard layout, iGoldMine will attempt to load a keyboard layout that matches the client's keyboard. The Windows Client will send the default keyboard layout (but not an IME) of the operating system. The Java Client will send the operating system's locale ID. The Linux Client, the Mac OS X Client, and the Windows CE Client will send the WINDOWSKEYBOARDLAYOUT value from the keyboard mapping file. These will be used by the server to attempt to load the keyboard layout that best matches the client.

This means that in most installations that do not utilize IMEs, the administrator is not required to perform any special configurations. Any Java client that has a standard language keyboard that matches the language of the Java Virtual Machine should be able to connect to a server and communicate that fact. Standard language keyboards have Windows keyboard layouts that are identical to the language's locale ID. For example, the French locale ID is 040C and the standard French keyboard layout is 0000040C.

If the keyboard is not standard there might be mismatches. The keyboard layouts of non-standard keyboards are not unique across all Windows platforms. For example, the keyboard layout for the United States Dvorak keyboard is 00010409 on Windows XP and Windows 2003 and 00020409 on Windows 98. Obviously, the locale ID from the Java Client will not be able to specify non-standard keyboards. To solve this issue, set the command-line argument `-kb` or the plug-in/applet parameter `"keyboard"` to 00020409.

If all clients within an installation of iGoldMine use the same non-standard keyboard, the fallback layout text registry key can be used to specify it for all sessions. This will ensure that all clients will get the proper keyboard for each session. If client computers have different non-standard keyboards the best way to communicate this to the server is to specify the keyboard layout in the command-line option or plug-in/applet tag parameter.

When connecting to a Chinese iGoldMine Server, the Logon dialog appears from the shortcut along with the IME bar specifying Chinese as the default language. Clicking CTRL+spacebar does not toggle the languages. Users must manually click the IME bar with the mouse pointer to select English. Without manually clicking the IME bar, users will be unable to type a user name and password.

Notes: When running the Java Client on a Chinese machine, users must turn the client IME off by clicking CTRL+spacebar. Once an application has been launched through iGoldMine, users turn the server's IME on by clicking CTRL+~.

When running the Java Client on a Japanese machine, users must turn the client IME off by clicking ALT+~. Once an application has been launched through iGoldMine, users turn the server's IME on by clicking CTRL+~.

Configuring Multiple Input Locales

The **Default User** account profile can be configured with different and/or multiple input locales. Account profiles for new users logging on to an iGoldMine Server are automatically configured with the **Default User** account's input locales. Users can switch to any input locale that is defined in their account profile.

Note: Users with roaming profiles or profiles that already exist on the iGoldMine Server will not receive these new settings. These accounts must be configured manually.

As an example, the following instructions describe how to install and use the German input locale on an English Windows Server 2003.

1. Enable German on an English Windows Server 2003.

- 1.1 Log on to the iGoldMine Server interactively with a user account that you wish to set the Input Local for.
- 1.2 Click Start | Control Panel | Regional Language Options.
- 1.3 Click the **Languages** tab.
- 1.4 Click **Details**.
- 1.5 On the **Text Services and Input Languages** dialog click **Add**.
- 1.6 On the **Add Input Language** dialog, expand the list of **Input languages** and select **German (Germany)**.
- 1.7 In the **Keyboard layout/IME** box, note that this has been changed to German. This indicates that the physical keyboard should be German. If the physical keyboard is not German, select the appropriate keyboard layout and click **OK**.
- 1.8 On the **Text Services and Input Languages** dialog click **OK**.
- 1.9 On the **Regional and Language Options** dialog, click the **Advanced** tab. Click the **Apply all settings to the current user account and to the default user profile** check box.
- 1.10 After reading the **Change Default User Settings** message, click **OK**.
- 1.11 On the **Regional and Language Options** dialog click **OK**.

2. Verify that the input locale is correctly installed and configured.

- 2.1 Launch **Notepad** in this interactive session.
- 2.2 Type a few characters in English.
- 2.3 Type Left Alt + Shift.
- 2.4 Type a few characters and verify that they display in German.

The German input locale is now enabled for the **Default User** profile and the user that was logged on to the system in step 1.1.

3. Switch between input locales during an iGoldMine session.

- 3.1 Start an iGoldMine client and connect to the server with the account used in step 1.1.
- 3.2 Launch **Notepad**.
- 3.3 Type a few characters in English.
- 3.4 Type Left ALT + Shift.
- 3.5 Type a few characters and verify that they display in German.

Notes:

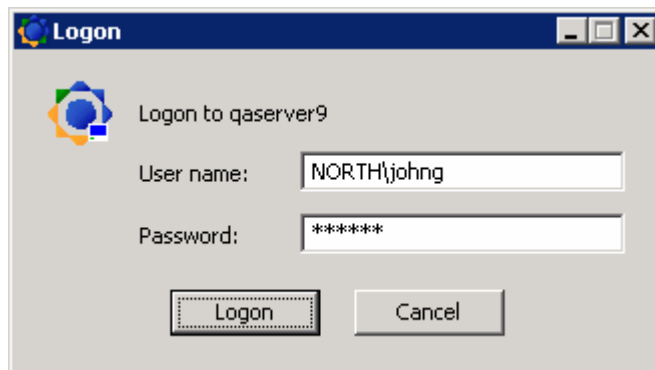
Users will not be able to switch input locales when the **Logon** dialog is displayed. The input locale for the default language of the iGoldMine Server will be used.

On Windows clients, the selected input locale of server-based applications is *not* displayed in the system tray of the client computer.

Administering User Accounts

To access applications on an iGoldMine Server, clients must log on to the server machine. When users start an iGoldMine client, they are prompted for their user name, password, and the name of the server they wish to access. This information is optionally encrypted and passed to the Application Publishing Service running on the iGoldMine Server. The Application Publishing Service then performs the logon operation using standard multi-user features of Windows.

When a user logs on to a server and a domain is not specified, the iGoldMine Server first attempts to authenticate the account on the local machine, followed by the machine's domain, and lastly the trusted domains. Users can override this default behavior and specify a domain by typing the domain name followed by a backslash (\) and their network user name in the **User name** box of the **Logon** dialog. For example, NORTH\johng.



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

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

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

Setting Up User Profiles

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

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

Notes: For a step-by-step article describing how to create roaming user profiles in Windows Server 2003, see Article ID 324749 in Microsoft's Knowledge Base (<http://support.microsoft.com/kb/324749>). For Windows XP, see Article ID 314478 (<http://support.microsoft.com/kb/314478>).

Setting File Permissions

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

You must use Windows Explorer to set the permissions for files on the server. By setting file permissions, you can restrict user access to applications, printers, and folders. File permissions can only be set on drives formatted with the Windows NT file system (NTFS). If you are using the FAT file system, you will be unable to set permissions for specific files or restrict access to applications.

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

Setting up a Network Printer

As the administrator, you can set up network printers for use by iGoldMine clients. You must first create a port on the iGoldMine Server that connects directly to the server and then install the printer locally. This provides direct access to the printer. Please note that network printers are set up using the **Windows Add Printer Wizard**, and not the **Client Printer Wizard**, which is accessible through the Program Window.

To add a port to the iGoldMine Server

1. Click Start | Settings | Printers.
2. Double-click **Add Printer**.
3. Select local printer, then click **Next**.
4. Click **Create a new port** and select **Local Port** as the type. Click **Next**.
5. In the **Port Name** dialog, type the UNC path to the printer (for example, \\PRINTSERVER\\LASERPRINTER) or the printer's IP address.
6. Select the printer manufacturer on the left and the printer model on the right or click **Have Disk**.
7. Follow the directions provided by the Add Printer Wizard to install the proper printer driver.

The Cluster Manager

The Cluster Manager allows you to administer, monitor, and control client access to the iGoldMine Server. The Cluster Manager displays a list of the users logged on to an iGoldMine Server, along with the applications the users are running, and the time the application was started. Through the Cluster Manager, you can perform a variety of administrative tasks, such as adding and removing applications, terminating user sessions, and ending processes running on the server.

To access the Cluster Manager

Double-click the Cluster Manager icon on the desktop.

—or—

1. Click the **Start** button on the Windows taskbar.
2. Click Programs | FrontRange Solution | iGoldMine | Cluster Manager

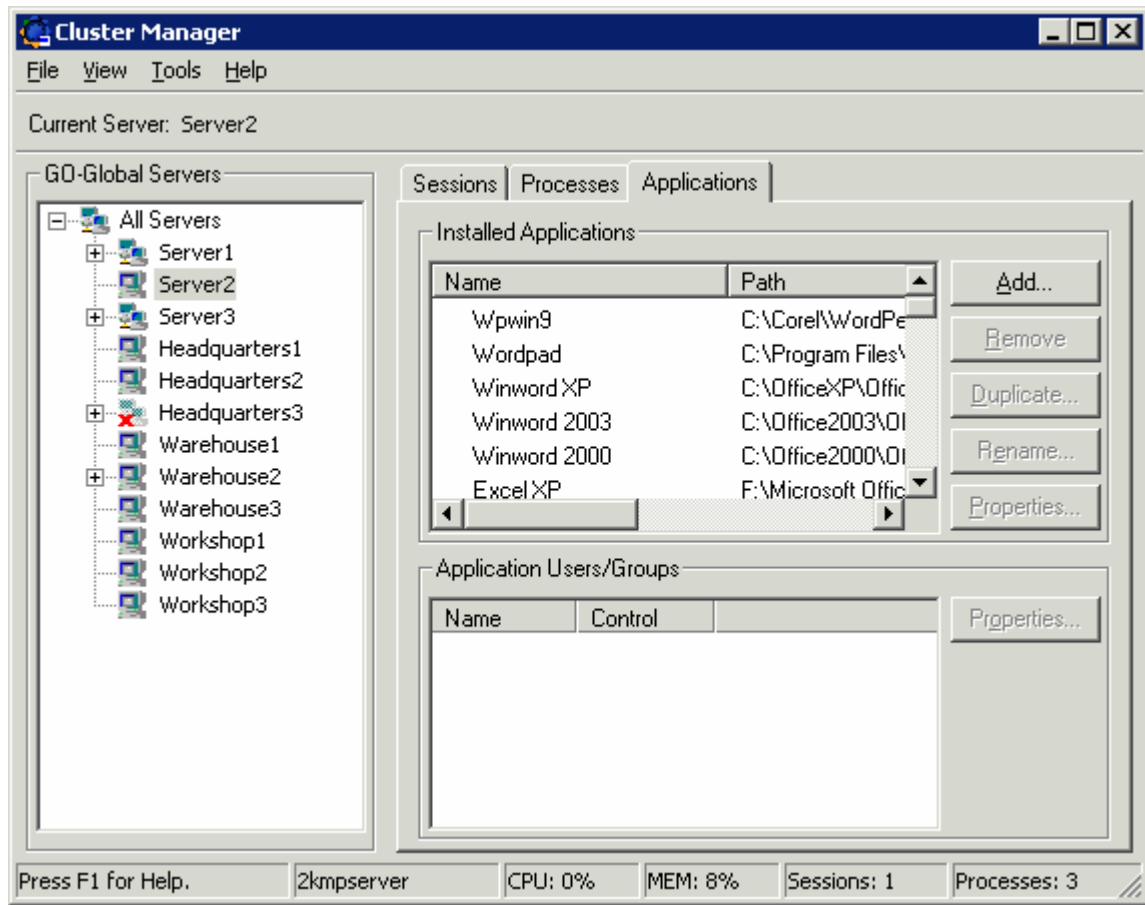
The left panel of the Cluster Manager lists the servers on the network running the Application Publishing Service. By default, the Cluster Manager displays information for the server running on your machine. To connect to other servers and view information about them, click the server name from the list of iGoldMine Servers.

If a server's icon has a red x, the administrator does not have administrative rights on the server. If the server's icon has a red x and is grayed out, the server is no longer running the Application Publishing Service or it has been turned off. In either case, the administrator is unable to access that server from the Cluster Manager.



Click the **All Servers** icon in the left panel of the Cluster Manager to view a list of all active sessions on the network. This allows you to view active iGoldMine sessions without connecting to individual servers. This is also helpful for locating a particular session's server.

You must belong to the Administrators group on each iGoldMine Server in order to access that server from the Cluster Manager. Without administrative rights on a server, you will be unable to add applications and terminate processes, etc.



Managing Applications

For clients to run an application via iGoldMine, the application must be added to the Cluster Manager. Clients are then able to connect to the iGoldMine Server and access the application.

Installing Applications

When installing applications to be run through iGoldMine, please consult the vendor's documentation for instructions on proper multi-user installation. You will likely need to install the application under an administrative account, but installation requirements will vary depending on the application. Installation should also adhere to Microsoft's guidelines for multi-user deployment. It is recommended that applications be installed on drives formatted with the Windows NT file system (NTFS). If you are using the FAT file system, you will be unable to set permissions for specific files or restrict access to applications.

Note:

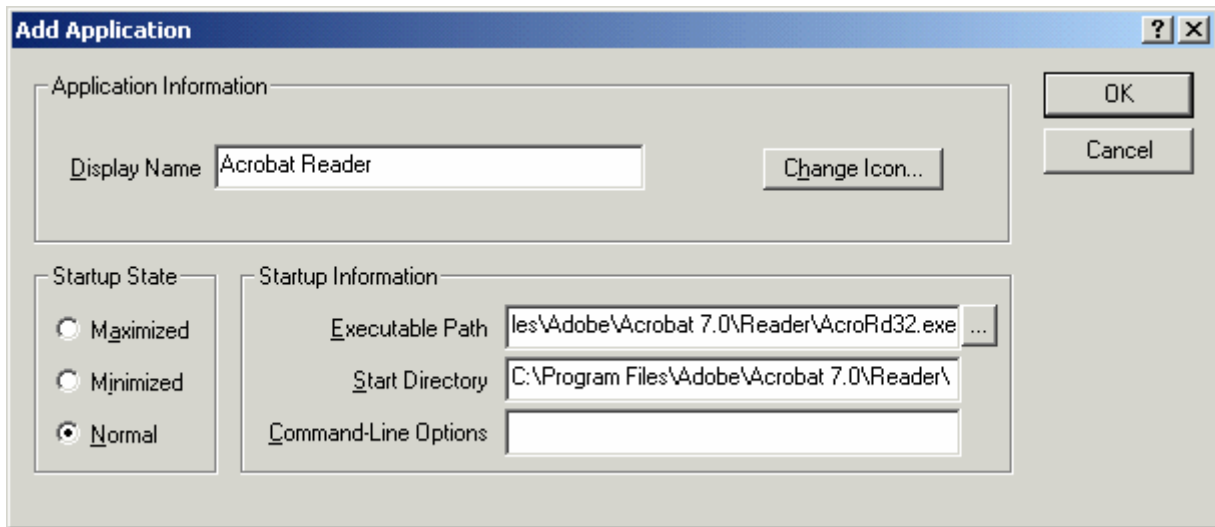
Please note that deploying applications via iGoldMine does not entitle your enterprise to unlimited access rights. You must still abide by the vendor's licensing agreement with regards to the number of applications that can be run concurrently.

Adding Applications

Applications must be added to the Cluster Manager before users can access them. When adding applications to the Cluster Manager, you can specify startup parameters that control how the application opens and what processes are initiated when the application is started.

To add an application to the Cluster Manager

1. Select the desired server from the list of **All Servers**.
2. Click the **Applications** tab.
3. Click the **Add** button.
4. Click the **Browse** button next to the **Executable Path** box to locate the application's executable file. (The executable file for Adobe Acrobat Reader 7, for example, is AcroRd32.exe.)
5. If you browsed for the application's .exe file in the preceding step, the file name will automatically be entered in the **Display Name** box. (This application name is displayed to users in the Program Window.) You can keep the default display name or you can type a new one. The application's Display Name cannot consist entirely of spaces and it cannot contain a backslash (\). This field cannot be left blank.
6. If you browsed for the application's executable file, the pathname of the directory will automatically be displayed in the **Start Directory** box. Otherwise, type the full pathname of the directory in which you want the application to start.
7. In the **Startup State** section, select whether the application starts maximized, minimized, or in normal mode.
8. In the **Command-Line Options** box, you can specify launch parameters for the application. Because these parameters are specific to each application, please refer to the application's documentation for information about specific launch parameters.
9. Click the **Change Icon** button if you would like to select an icon other than the application's default icon.
10. Click **OK** when you are finished.



Once you have registered an application with the Cluster Manager, the application's name and path will appear in the list of **Installed Applications**. You can sort items in the list in ascending or descending order by clicking the column's title. This holds true for all lists in the Cluster Manager.

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

Due to access restrictions, the Cluster Manager cannot verify the validity of paths specified in UNC format (e.g., \\Machine Name\Folder Name\...) or that reside on a mapped network drive. If the Executable Path or Start Directory of a published item involves a mapped drive or is specified with a UNC path, the Cluster Manager will accept the specified path regardless of whether or not it is valid. If the path is invalid, or if the client user does not have rights to access the specified executable file or folder, the published item will not appear in the Program Window. Select the item and click the **Properties** button. Try updating the item Executable Path or its Start Directory. If the item has been uninstalled or moved to a new location, it will not be displayed in the Cluster Manager once the Application Publishing Service has been restarted.

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

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

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

Editing an Application's Properties

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

To edit an application's properties

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

Duplicating an Application

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

To duplicate an application

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

Renaming an Application

The display name that you assign to an application will appear to the end user in the Program Window. You can change an application's display name at any time.

To rename an application's display name

1. From the list of Installed Applications, select the application you would like to rename.
2. Click Tools | Applications | Rename.

—or—

Click the **Rename** button to the right of the list of Installed Applications.

Assigning Application Launch Parameters to Users or Groups

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

Tip: Check the user's **About FrontRange iGoldMine** box to verify what Group or Groups the user is assigned to and in what order the Groups are listed in the system.

File permissions for users and groups are controlled by Windows NT file system (NTFS) security settings on the server. File permission are *not* set through the Cluster Manager. When you select an application from the Installed Applications list, the Application Users/Groups list displays the user permissions that have been specified for that file and/or application with NTFS. You can then edit the application's properties for specific users or groups. File permissions can only be set on drives formatted with NTFS. If you are using the FAT file system, you will be unable to set permissions for specific files or restrict access to applications.

To assign application launch parameters for a user or group

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

Note: If you are using the FAT file system, you cannot set permissions for specific files or restrict access to applications.

Removing Applications

iGoldMine-deployed applications are removed through the Cluster Manager. Removing an application from the Cluster Manager does not uninstall it from the server; it only prevents iGoldMine clients from accessing the application.

To remove an application

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

—or—

Click Tools | Applications | Remove.

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

Managing Sessions and Processes

Administrators can encrypt and shadow sessions and terminate processes and sessions through the Cluster Manager, as described below.

Terminating a Session

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

To terminate a session

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

Ending a Process

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

To end a process

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

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

Shadowing a Session

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

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

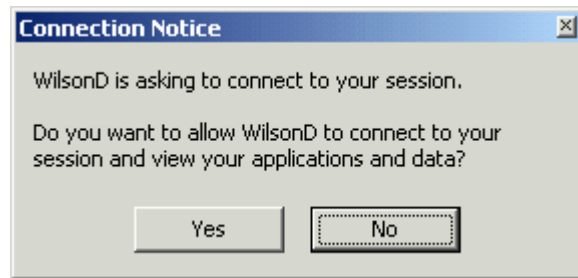
To shadow a session

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

—or—

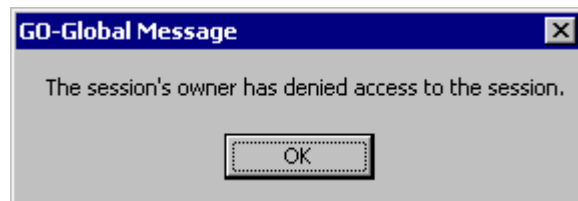
From the **Sessions Name** column, right-click the session you would like to shadow.

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



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

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



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 an iGoldMine communication failure.

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

Note: When an iGoldMine session is being shadowed, the server's cursor remains on the client until that session is closed. It does not go away even when the session is no longer being shadowed.

Security Options

Through the **Security** tab of the **Server Options** dialog, administrators can select the transport mode of communication between clients and the iGoldMine Server and select the level of encryption for data transmitted between client and server. Administrators can also modify the host port setting and enable Integrated Windows authentication and password caching.

Selecting SSL Transport

iGoldMine provides support for both Transmission Control Protocol (TCP) and Secure Socket Layer (SSL) as methods for communication between Windows and iGoldMine Servers. When selecting the SSL transport, an SSL Certificate file must be specified. SSL certificates are required to secure communication between iGoldMine clients and servers. 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.

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>.
2. Install **OpenSSL** on the iGoldMine Server.
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

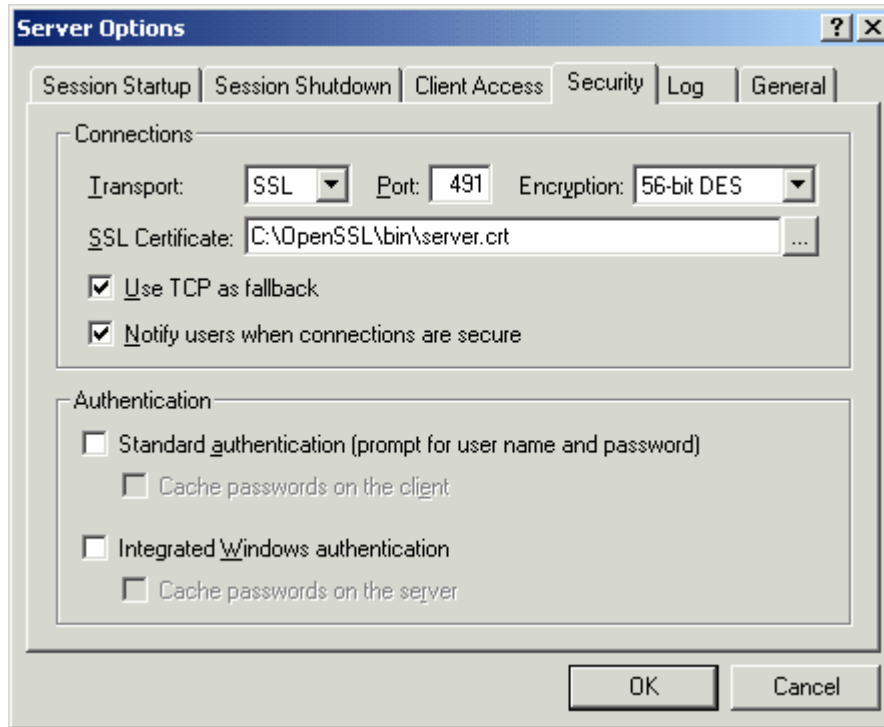
E-mail Address: your e-mail address

The Common Name *must* match the host name of the iGoldMine Server (i.e., the name that users will specify when connecting to the server). 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 iGoldMine'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 certificate, place it in the file **server.crt**. Copy both the **server.key** and **server.crt** files to a directory on the iGoldMine Server that can be accessed from the System account and accounts that belong to the Administrator's Group but cannot be accessed from normal user accounts. Finally, select the server certificate in the Cluster Manager.

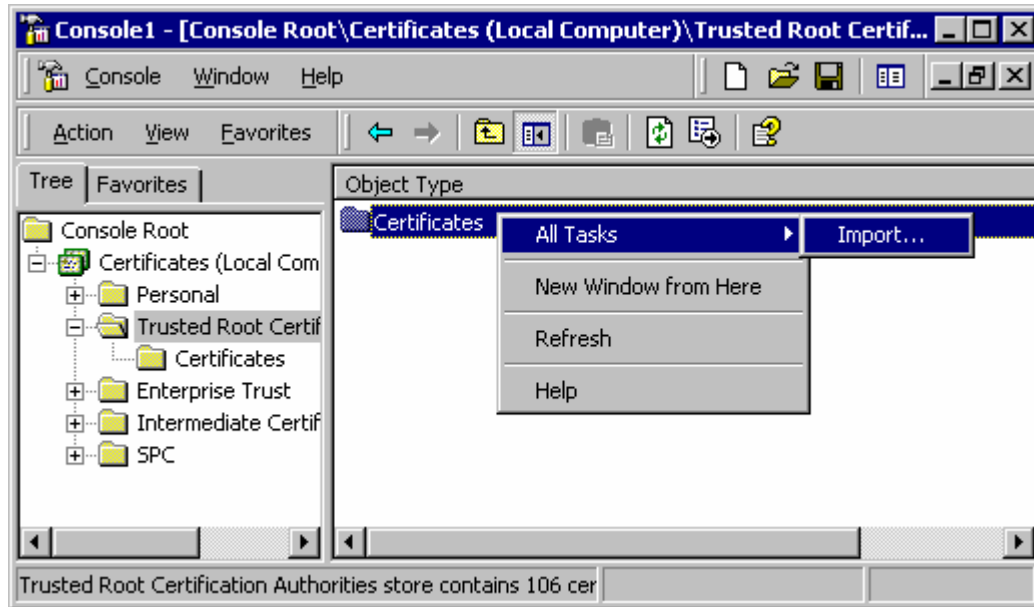
To select the server certificate

1. From the Cluster Manager, click Tools | Server Options.
2. Click the **Security** tab.
3. In the **Transport** list, select SSL.
4. Type or browse to the path to the server's certificate (e.g., server.crt) file in the **SSL Certificate** box.
5. Click **OK**.

**Importing the Trusted Server Certificate on a Dependent Application Server**

To import the trusted server certificate on a dependent application server, add a Policy in Microsoft Management Console.

1. On the dependent application server, 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 iGoldMine Server. Dependent application servers do not need SSL certificates, but their designated relay server must have a valid SSL certificate that is signed by a CA and that is recognized by the dependent application servers. You can verify that these conditions are met as follows:

1. Run the native Windows Client on the dependent application server:
2. Right-click **My Computer**.
3. Click **Explore**.
4. Browse to the \iGoldMine Server\Programs directory.
5. Double-click **ggw.exe**.
6. Enter the name of the relay server as it is specified in the Cluster Manager.
7. If the relay server has a valid SSL certificate that is signed by a CA and is recognized by the dependent application server, no Security Alert dialog will be displayed. If a Security Alert dialog is displayed, the dependent application server will not be able to connect to the relay server.

Creating Your Own Certificate Authority

Sites with many iGoldMine Servers 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 iGoldMine 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.

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 iGoldMine Server. 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 log on to the server. Finally, select the server certificate in the Cluster Manager.

To select the server certificate

1. From the Cluster Manager, click Tools | Server Options.
2. Click the **Security** tab.
3. In the **Transport** list, select SSL.
4. Type or browse to the path to the server's certificate (e.g., server.crt) file in the **SSL Certificate** box.
5. Click **OK**.

Your iGoldMine Server 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 iGoldMine 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 iGoldMine. 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 iGoldMine. It must have the same file prefix as the certificate generated by the CA (i.e., server.crt).

iGoldMine 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
```

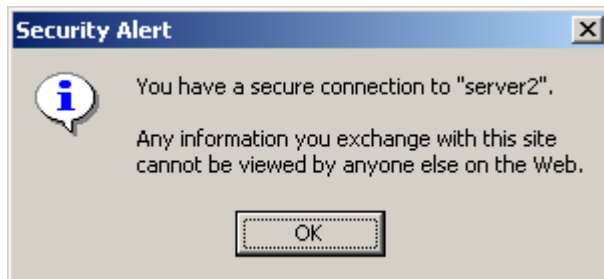
The resulting **MYCERT.pem** file can then be renamed to **MYCERT.crt** for use in iGoldMine.

Notifying Users of a Secure Connection

When the SSL transport is selected, you can opt to notify users with a Security Alert when connections are secure. The Security Alert also informs users of which encryption algorithm is used to compress and encrypt their data.

To notify users when connections are secure

1. From the Cluster Manager, click Tools | Server Options.
2. Click the **Security** tab.
3. In the **Transport** list, click SSL.
4. Type or browse to the path of the server's certificate file in the **SSL Certificate** box.
5. Click the **Notify users when connections are secure** option.
6. Click **OK**.



When the SSL transport is selected, all connections to that iGoldMine Server use the SSL transport and the selected encryption algorithm, including connections from Cluster Managers, clients, and Dependent Application Servers. Clients that do not support SSL (i.e., the Java Client) will be unable to connect to the server using the SSL transport unless the **Use TCP as fallback** option is enabled.

To select TCP as the fallback transport mode

1. From the Cluster Manager, click Tools | Server Options.
2. Click the **Security** tab.
3. Click the **Use TCP as fallback** option.
4. Click **OK**.

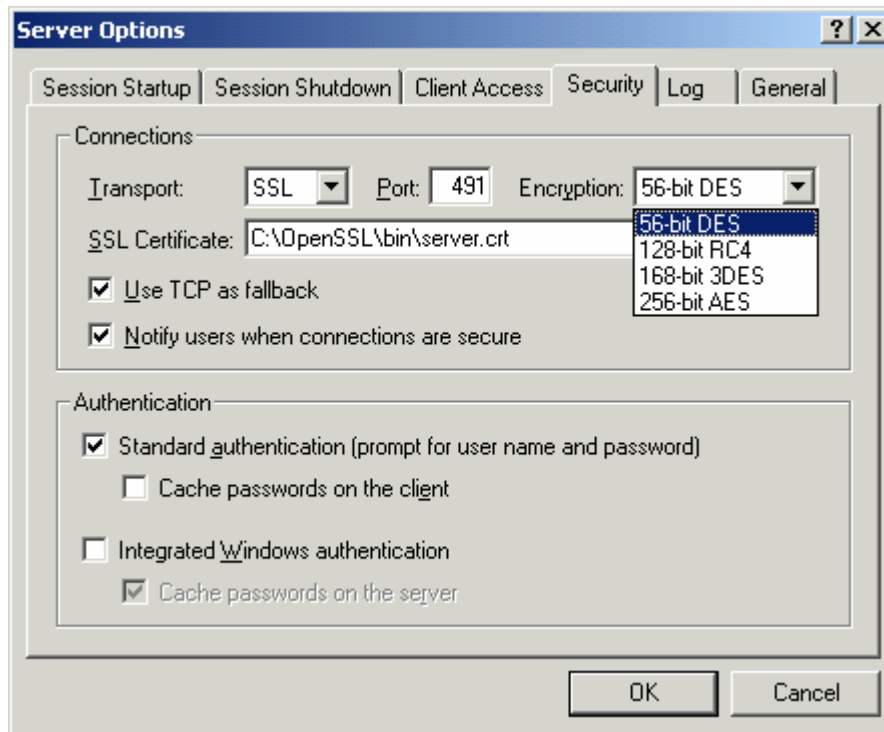
Encrypting Sessions

For purposes of security, administrators can optionally encrypt all data transmitted between the client and the server. 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 server. When TCP transport mode is selected, iGoldMine 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 iGoldMine sales representative.

To encrypt a server's sessions

1. Click Tools | Server Options.
2. Click the **Security** Tab.
3. From the **Encryption** list, select an encryption level.
4. Click **OK**.

Once you have enabled encryption, all succeeding iGoldMine sessions will be encrypted. Sessions that are active when the feature is enabled will remain unencrypted. The next time the user logs on to the iGoldMine Server, however, his or her session will be encrypted. The user must log off the iGoldMine Server, and log back on in order for his or her session to be encrypted.



Modifying the Host Port Setting

In order for users to access iGoldMine 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 setting

1. Select the desired server from the list of **All Servers**.
2. Click Tools | Server Options.
3. Click the **Security** tab.
4. Type a new port number in the **Port** box.
5. Once you have modified the host port setting, you will need to modify the **hostport** parameter in the logon HTML pages. For instructions on modifying logon HTML pages, see chapter 5, "Running the iGoldMine Client."
6. Click **OK**.

Examples:

Java Client

```
<applet code="com.graphon.ggw.Logon"
width="800"
height="600"
archive="ggw.jar,ggw.res.jar">
<param name= "host" value= "server1">
<param name= "hostport" value= "1667">
</applet>
```

Netscape Plug-in

```
<embed type= "application/x-ggw-plugin"
width= "800" height= "600"
host= "server1"
hostport="1667">
</embed>
```

If the host port has been modified, users running the Windows Client, the Windows CE Client, the Mac OS X, or the Linux Client will need to append the `-hp` argument (followed by the new port number) to the command-line. For example, `...\ggw.exe" -h server1 -hp 1667`

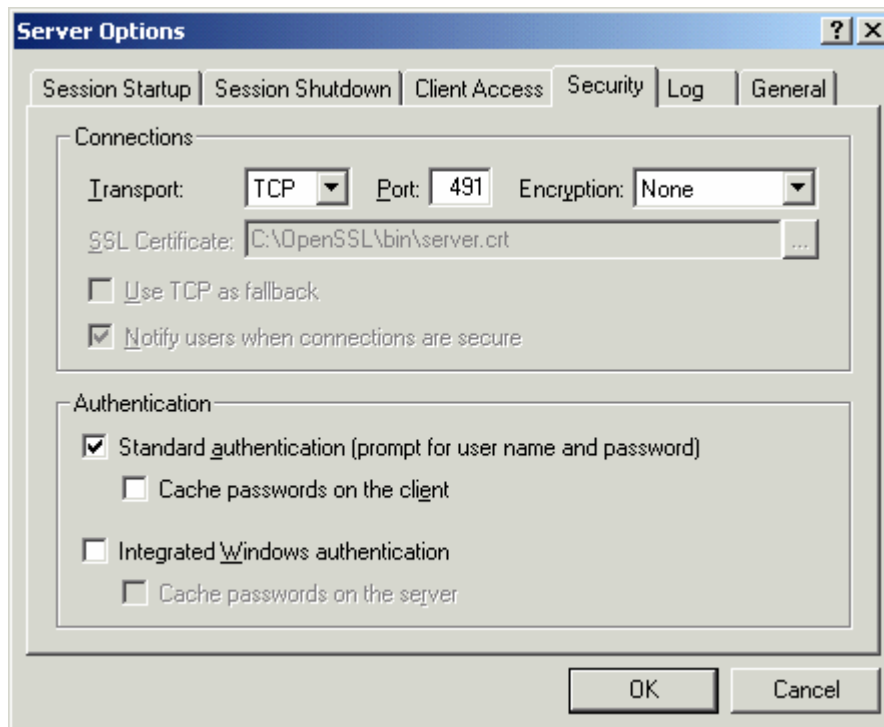
Users can also specify the port number in the **Connection** dialog when logging on to iGoldMine. In the **Server address** box, type the server name followed by a colon and the port number. For example, `server1:1667`. If the new port number is not specified by either of these methods, users will be unable to log on to iGoldMine.

Standard Authentication

Standard authentication is the default method for authenticating users on an iGoldMine Server. Standard authentication allows users to log on to iGoldMine via the Logon dialog by supplying their user name and password. Once authenticated, users are added to the server's INTERACTIVE group and given the same access rights as if they had logged on to the server at its console.

To enable Standard authentication

1. Click Tools | Server Options.
2. Click the **Security** tab.
3. Click **Standard authentication (prompt for user name and password)**.
4. Click **OK**.



Integrated Windows Authentication

Integrated Windows authentication allows users to connect to an iGoldMine Server and start a session without having to log on to the server and re-enter their user name and password. When Integrated Windows authentication is the only option enabled, the user's user name and password are never transmitted over the network. Instead, iGoldMine simply runs the user's session in the same security context as the iGoldMine Client. Users are added to the server's NETWORK group instead of its INTERACTIVE group. As a result, they may be denied access to some resources.

When users connect to an iGoldMine Server using Integrated Windows authentication, they are able to access most of the same resources on the server that they would be able to access if they logged on to the server interactively. However, depending on the authentication protocols supported by the client's and server's operating systems and the network, when users access resources that reside on other computers on the network they might be required to re-enter their user name and password. If network resources are unable to request a user name and password, access might be denied.

In order to access other computers on the network, the Active Directory must be configured to allow authentication credentials to be passed to other computers. Microsoft refers to the right to pass authentication credentials to a third or more computers as "delegation." Delegation is supported by Windows 2000 or later on Active Directory networks with the proper settings. Please refer to your Microsoft Windows operating system documentation for instructions on properly configuring an Active Directory Domain Controller. Windows NT Domains do not support delegation. When Integrated Windows authentication is enabled in this environment, users might not have access to resources that reside on other computers on the network. To avoid these resource access limitations, see **Configuration Requirements for Delegation Support** in Chapter 6.

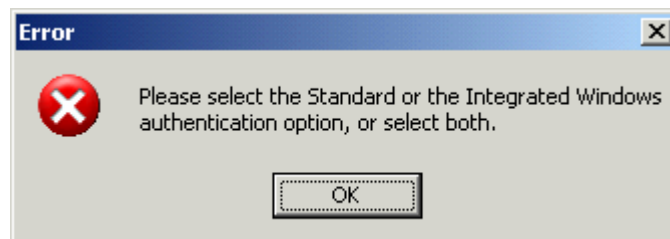
Note: The **Cache passwords on the server** option, described in the following section, can be enabled to obtain an INTERACTIVE group logon with Integrated Windows Authentication.

Integrated Windows authentication is only available to users who log on from Windows computers that are members of the same domain as the iGoldMine Server. Users must be running the Windows Client, the Active X Control, or the Netscape Plug-in for Windows.

To enable Integrated Windows Authentication

1. Click Tools | Server Options.
2. Click the **Security** tab.
3. Enable **Integrated Windows authentication**.
4. Click **OK**.

iGoldMine requires that either Standard authentication or Integrated Windows authentication be enabled. If neither one of these authentication methods is selected and you click **OK** to close the dialog, the following error message is displayed:



If both Standard authentication *and* Integrated Windows authentication are enabled, the iGoldMine Server will first attempt to log the user on via Integrated Windows authentication. If this fails, iGoldMine will then attempt to log the user on with Standard authentication by presenting the **Logon** dialog and requiring a user name and password.

Server-Side Password Caching

When a user logs on to an iGoldMine Server with standard authentication (either with a user name and password supplied by the Logon dialog, HTML parameters, or command-line arguments), that user is added to the server's INTERACTIVE group. Alternatively, a user that logs on to an iGoldMine Server using integrated Windows authentication is added to the server's NETWORK group. By default, members of the INTERACTIVE group have greater access to the server's resources than members of the NETWORK group. As a result, a user that logs on via Integrated Windows authentication may encounter "access denied" errors under a number of conditions.

Note:

Areas restricted from members of the NETWORK group include DCOM (also known as OLE and COM/COM+) security limitations, file security limitations, and application specific security checking. Administrators should verify that all resources (files, services, etc.) that Integrated Windows authenticated users need to access have the proper security settings to allow that access.

To avoid these errors, administrators can enable the **Cache passwords on the server** option. Doing so allows users to log on from Windows computers that are members of the same domain as the iGoldMine Server without having to enter their user name and password every time they connect. Users are prompted for a password when first connecting to the server or following a password change. Passwords are stored within their respective profiles and can only be decrypted from within their respective security contexts. With subsequent connections to iGoldMine, users are automatically logged on and added to the server's INTERACTIVE group. They are granted the same access rights had they logged on to the server at its console.

Server-side password caching requires delegation, which is supported by Windows 2000 or later on Active Directory networks with the proper settings. Please refer to your Microsoft Windows operating system documentation for instructions on properly configuring an Active Directory Domain Controller. For a list of configuration requirements for delegation see **Configuration Requirements for Delegation Support** in Chapter 6.

To enable server-side password caching

1. From the Cluster Manager click Tools | Server Options.
2. Click the **Security** tab.
3. Enable **Integrated Windows authentication**.
4. Enable **Cache passwords on the server**.
5. Click **OK**.

iGoldMine caches passwords on the server using the industry standard encryption algorithms provided by Microsoft's Data Protection application programming interface (DPAPI). For more information about DPAPI search the MSDN Library (<http://msdn.microsoft.com/library/default.asp>) for "Windows Data Protection."

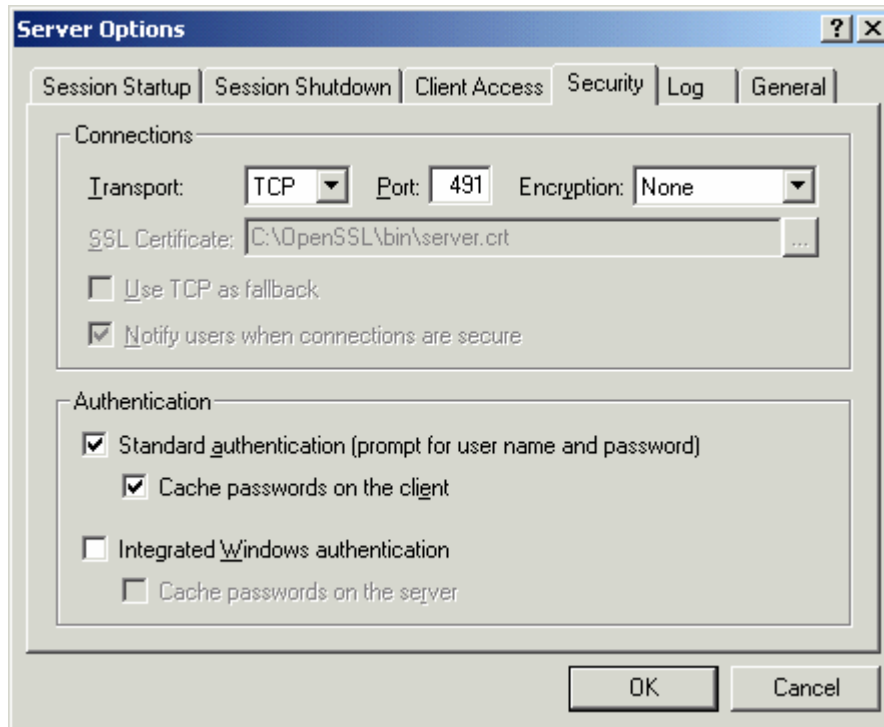
Client-Side Password Caching

Client-side password caching allows users who are not members of the iGoldMine Server's domain to log on to iGoldMine without having to enter their user name and password every time they connect to the server. After the first manual authentication, the user's logon credentials are encrypted on the server using the SYSTEM account context, transmitted over the network, and stored on client computers in user-private directories.

When the user makes subsequent connections to the server, the cached password is transmitted back to the server, where it is decrypted using the SYSTEM account context and then used to automatically log the user on to the iGoldMine Server. The user is added to the server's INTERACTIVE group and granted the same access rights had that user logged on to the server at its console.

To enable client-side password caching

1. From the Cluster Manager click Tools | Server Options.
2. Click the **Security** tab.
3. Enable **Standard authentication (prompt user for user name and password)**.
4. Enable **Cache passwords on the client**.
5. Click **OK**.



On most platforms, the cached password is stored in the user's home directory in a .dat file named for the iGoldMine Server. With the Pocket PC Client and the Windows CE Client, the cached password is stored in the user's Registry settings. The table below provides example locations of the cached password for each iGoldMine Client. In the examples, user1 is the user name, server1 is the name of the iGoldMine Server, and 192.168.100.111 is the IP Address of the iGoldMine Server.

iGoldMine Client	Password Locations
Mac OS X Client Browser Plug-in for Mac OS X	/Users/user1/.ggw/192.168.100.111.dat
Windows Client ActiveX Control Netscape Plug-in for Windows	C:\Documents and Settings\user1\Application Data\GraphOn\iGoldMine\server1.dat
Linux Client Netscape Plug-in for Linux	/Users/user1/.ggw/192.168.100.111.dat
Pocket PC Client	In the Registry: KEY_CURRENT_USER\Software\Graphon\Bridges\1.0.0\Client\CachedPasswordServers\SERVERNAME
Windows CE Client	In the Registry: HKEY_CURRENT_USER\Software\Graphon\Bridges\1.0.0\Client\CachedPasswordServers\SERVERNAME

Client-side password caching is supported on all iGoldMine clients, with the exception of the Java Client.

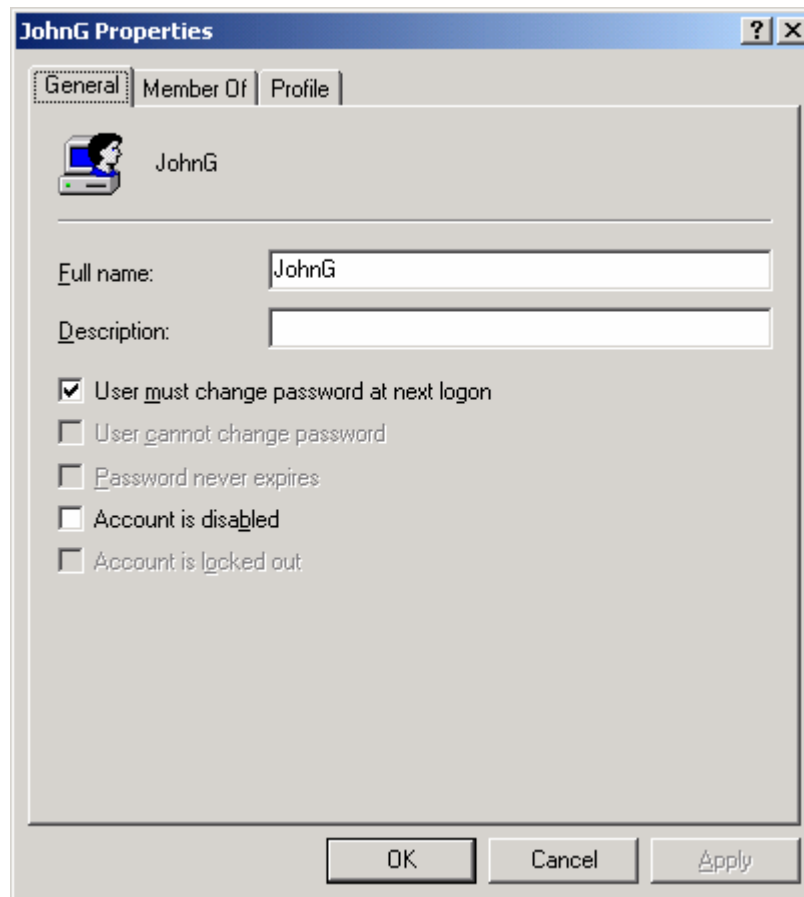
Password Change

Users can change passwords when:

- a. The administrator requires the user to change his or her password at the next logon;
- b. The security policy is configured to prompt users to change passwords before expiration; and
- c. The user's password has expired.

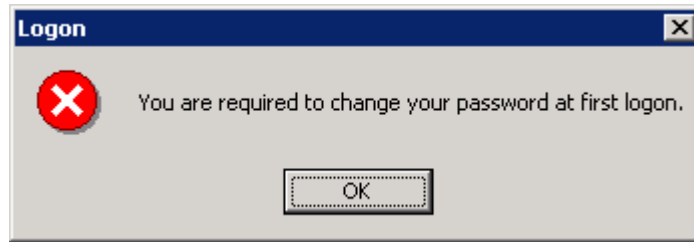
Changing Passwords at Next Logon

Administrators can require a user to change his or her password by checking the User must change password at next logon option in the **Administrator Properties** dialog. (For Local accounts, this dialog can be accessed by clicking My Computer | Manage | Local Users and Groups | Users | *UserName* | Properties).



To log on when the *User must change password at next logon* option is enabled for a user's account

1. Access the iGoldMine logon page (e.g., <http://server/logon.html>) and select an iGoldMine client.
2. Type the user name and password in the **Logon** dialog. If the client account does not exist in the domain in which the iGoldMine Server resides, include the domain name in the **User name** field as a prefix (e.g., domain\username).
3. Click **OK**.
4. Click **OK** to the following message:



5. Type a new password in the **New Password** and **Confirm New Password** fields of the **Change password** dialog.
6. Click **OK**.



Prompting Users to Change Passwords Before Expiration

By default, users are prompted to change their passwords whenever they log on within 14 days of their password's scheduled date of expiration. Administrators can modify the change password "prompt" period by editing the Prompt user to change password security setting. For example, the local security setting can be viewed and changed by clicking Start | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Option.

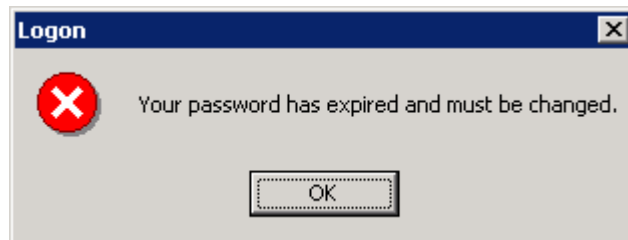
To log on during the password change "prompt" period

1. Access the iGoldMine logon page (e.g., <http://server/logon.html>) and select an iGoldMine client.
2. Type the user name and password in the **Logon** dialog.
3. Click **OK**.
4. The following message is displayed:
"Your password will expire in x day(s). Do you want to change your password now? Yes/No"
If the user clicks **No**, the iGoldMine session will start. If **Yes**, the **Change Password** dialog is displayed.
5. Type a new password in the **New Password** and **Confirm New Password** fields.

Prompting Users to Change Passwords After Expiration

To log on after a password has expired

1. Access the iGoldMine logon page (e.g., <http://server/logon.html>) and select the appropriate iGoldMine client.
2. Type the user name and password in the **Logon** dialog. If the client account does not exist in the domain in which the iGoldMine Server resides, include the domain name in the **User name** field as a prefix (e.g., domain\username).
3. Click **OK**.
4. Click **OK** to the following message:




5. Type a new password in the **New Password** and **Confirm New Password** fields of the **Change Password** dialog.
6. Click **OK**.

Password Change and Integrated Windows Authentication

When Integrated Windows Authentication is enabled, iGoldMine relies on the operating system of the client to change passwords. For example, iGoldMine supports the following scenario:

1. The administrator edits a user's settings and specifies that the **User must change password at next logon**.
2. Upon logging on, the user is prompted to change his or her password.
3. The user changes the password and logs on to the client computer.
4. The user starts the iGoldMine client and connects to an iGoldMine Server.
5. The password has already been changed, so the user is authenticated on the server without being prompted for a password, unless the **Cache passwords on the server** option is enabled. In this case, the user will be prompted to enter a new password.

If, however, the administrator specifies that the **User must change password at next logon** after the user has logged on to the client computer, and the user subsequently connects to an iGoldMine Server that has Integrated Windows authentication enabled, authentication may fail. If it fails and both the **Integrated Windows authentication** and **Cache passwords on the server** option are enabled, the user will be prompted to log on and make a password change as described above.

Note: In the Cluster Manager's dialog boxes, you can easily get Help by right-clicking an item, and then clicking **What's This?**. A pop-up window will appear, displaying a brief explanation of the item. You can also get Help by clicking  on the title bar of a dialog box and then selecting an item.

Session Reconnect

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

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

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

Setting the Session Termination Option

Administrators control how long client sessions and applications remain running on the iGoldMine Server through the Cluster Manager's **Server Options** dialog. Select **Immediately** if you want client sessions to terminate as soon as the client disconnects. This is the default setting. Select **Never** if you want sessions to terminate only when a user manually closes all applications running within a session or when an administrator manually terminates a session using the Cluster Manager. Select **After ___ minutes** to specify the number of minutes that a session will remain running after a client has disconnected from the session. Type the number of minutes in the edit field that a session should remain running after the client disconnects.

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

To set the session termination option

1. From the Cluster Manager, click Tools | Server Options.
2. Click the **Session Shutdown** tab.
3. Enable **Disconnected sessions terminate**.
4. 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.
5. Click **OK**.

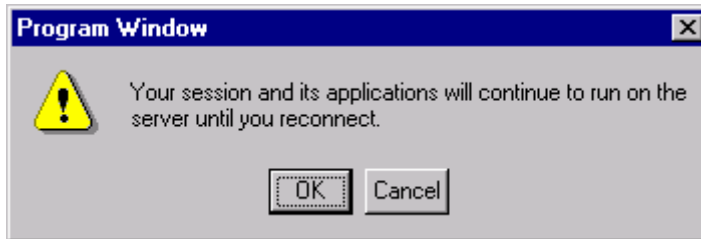
Disconnecting a Session

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

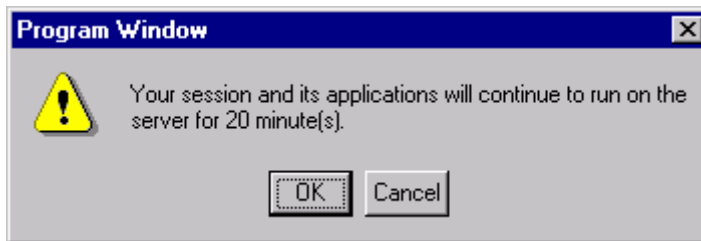
To disconnect a session

From the Program Window, click File | Disconnect.

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



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



If a user attempts to disconnect from a session and already has a disconnected session, the following message appears:

"You already have a session (*session_name*) that is disconnected. If you disconnect the current session, that previous session will be terminated. Do you want to continue?"

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

Note: When a user reconnects to a session, the command-line arguments -a, -r, and -ac are ignored.

Shared Account

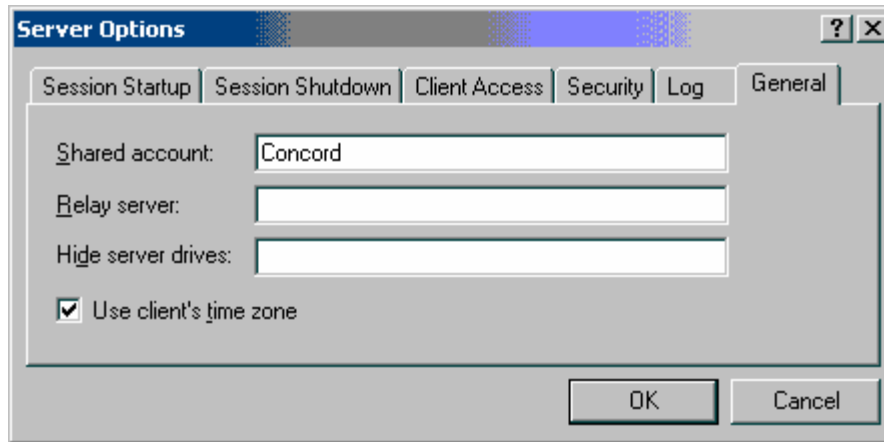
By specifying a shared account in the **Server Options** dialog, administrators can establish an account that can be shared by multiple users. Users of a shared account are unable to disconnect or reconnect to any iGoldMine session. The shared account session will terminate immediately after disconnecting from the server, regardless of the reconnect setting in the Cluster Manager.

To specify a shared account

1. Click Tools | Server Options.
2. Click the **General** tab.
3. Type the user name of the shared account in the **Shared account** edit box.
4. Click **OK**.

If an administrator designates an existing user name as a shared account while that user is disconnected from his or her session, the session will remain running on the server until the termination limit has been reached. The session will then be terminated. Before specifying a shared account, verify in the Cluster Manager that there are no connected or disconnected sessions using that account.

iGoldMine does not support the use of domain names (for example, NORTH\johng) for shared accounts.



Client Time Zone

By default, all iGoldMine sessions are run in the time zone of the iGoldMine Server machine. Administrators can opt to run iGoldMine sessions in the time zone of the client computer by enabling the **Use client's time zone** option from the Cluster Manager.

To enable client time zone

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

Monitoring Server Activity

The Cluster Manager displays information about server activity and processes taking place on the server. Administrators can use this information to determine which applications are no longer being used and whether additional servers are required, for example.

Viewing Session Information

The Cluster Manager displays the following session information:

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

To view session information

Click the **Sessions** tab.

Viewing Process Information

A process refers to the specific application that a user is running from the server. The Cluster Manager displays the following process information:

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

To view process information

Click the **Processes** tab.

Refreshing the Cluster Manager

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

To refresh the Cluster Manager

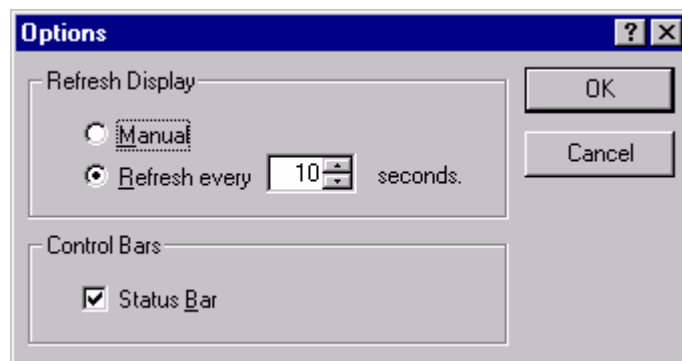
Click View | Refresh.

Setting the Refresh Rate

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

To set the refresh rate to allow only manual refresh

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



To set the refresh rate to refresh automatically

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

The Status Bar

The Status Bar is displayed at the bottom of the Cluster Manager window. The Status Bar provides brief descriptions of menu commands when the mouse pointer is placed over that item in the menu. The Status Bar indicates the name of the iGoldMine Server currently being accessed, as well as the Mem usage and CPU utilization for that server, as calculated by the Windows Task Manager. The last two items on the Status Bar, Sessions and Procs indicate the number of sessions and the number of processes running on the active iGoldMine Server.

If **All Servers** is selected, the **Sessions** number will reflect all the sessions running on the network, and the **Procs** number will reflect all the processes on the network.

To turn the Status Bar on or off

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

Setting the Broadcast Interval

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

To set the broadcast interval

1. Stop the **iGoldMine Application Publishing Service**.
2. From the Registry Editor, expand the HKEY_LOCAL_MACHINE key.
3. Locate the **AppServer** key: [Software\\GraphOn\\Bridges\\1.0.0\\AppServer]
4. Right-click the **Broadcast Interval** value and click **Modify**.
5. Type the desired number of seconds in the **Value data** box. (This value must be an integer greater than or equal to 1. The default value for Broadcast Interval is 10.)
6. Click **OK**.
7. Restart the **iGoldMine Application Publishing Service**.

Session Startup Options

Through the **Session Startup** tab of the Cluster Manager's **Server Options** dialog, administrators can enable startup options such as Group Policy, Progress Messages, and Logon Scripts. Administrators can also set various resource limits.

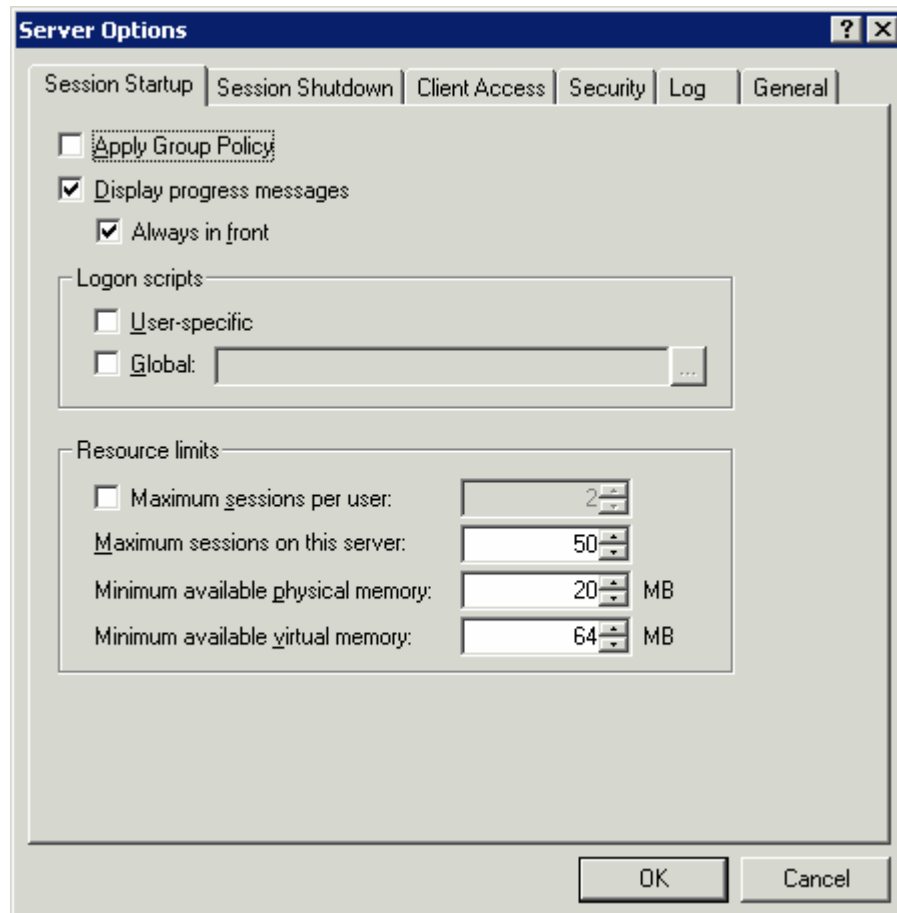
Applying Group Policy

iGoldMine supports Microsoft's Group Policy. Using Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options. For more information regarding this feature, go to:
<http://www.microsoft.com/windowsserver2003/techinfo/overview/gpintro.mspx>.

To apply Group Policy on an iGoldMine Server

1. From the Cluster Manager, click Tools | Server Options.
2. Click **Session Startup**.
3. Select **Apply Group Policy**.
4. Click **OK**.

Note: It may take users longer to log on to iGoldMine when Group Policy is enabled.



Displaying Progress Messages

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

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

To display session startup progress messages to users

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

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

Logon Scripts

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

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

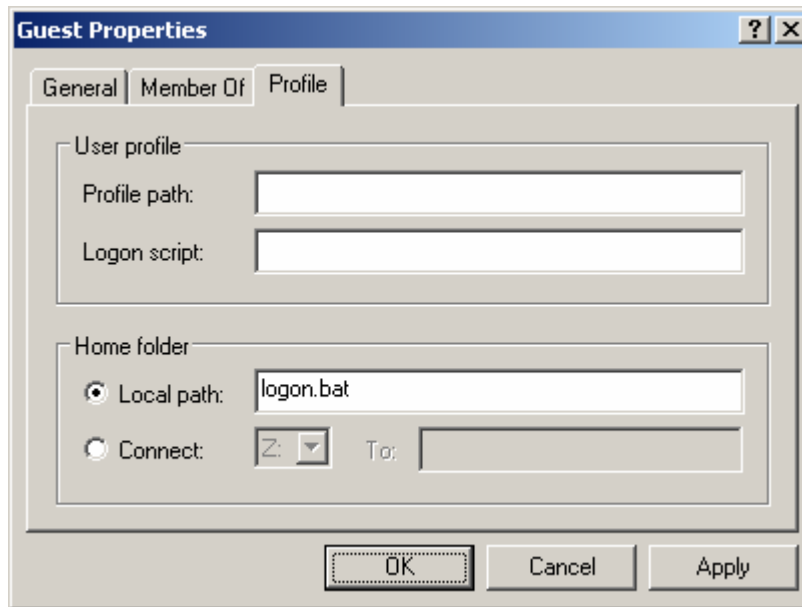
User-specific logon scripts are specified using the functionality provided by the operating system. For example, the logon script for local users on a Windows Server 2003 is specified as follows:

1. Right-click **My Computer** and click **Manage**.
2. Navigate to \System Tools\Local Users and Groups\Users.
3. Select a user and click **Properties**.
4. Click Profiles.
5. In the **Logon script** box, type the file name of the user's logon script.

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

1. If the user's account is a domain account:
 - a. \\pdcname\NETLOGON, i.e., the NETLOGON share of the primary domain controller.
 - b. \\pdcname\SYSVOL\domainname, i.e., the domain subdirectory of the primary domain controller's SYSVOL share.
2. If the user's account is a local account:
 - a. *systemroot\System32\Repl\Import\Scripts*
 - b. *systemroot\sysvol\sysvol\domainname*

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



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

To run user-specific logon scripts

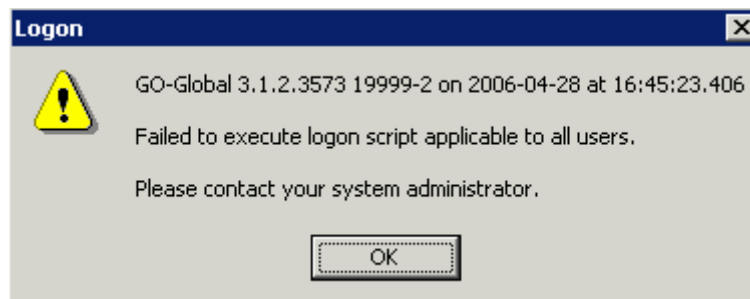
1. From the Cluster Manager, click Tools | Server Options.
2. Click **Session Startup**.
3. Select **User-specific**.
4. Click **OK**.

To run a global logon script

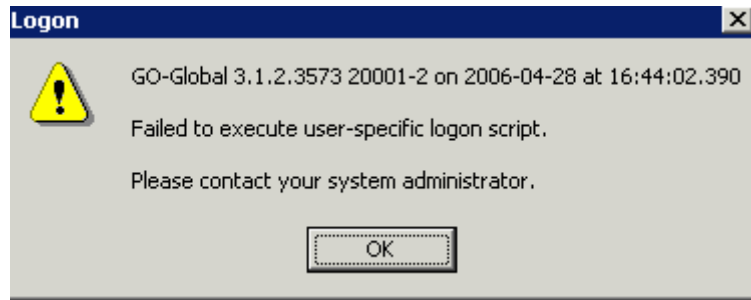
1. From the Cluster Manager, click Tools | Server Options.
2. Click **Session Startup**.
3. Select **Global** and specify the path of the global script file.
4. Click **OK**.

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

When a **global logon script** fails to map (in the case of an incorrect location, a non-existent location, or a problem with the script, etc.) the following error message appears on the client:



When a **user-specific logon script** fails to map (in the case of an incorrect location, a non-existent location, or a problem with the script, etc.) the following error message appears on the client:



When these errors occur, check the location of the logon script. If the user's account is a **domain** account:

- a. `\\pdcname\NETLOGON`, i.e., the NETLOGON share of the primary domain controller.
- b. `\\pdcname\SYSVOL\domainname`, i.e., the domain subdirectory of the primary domain controller's SYSVOL share.

If the user's account is a **local** account:

- a. `systemroot\System32\Repl\Import\Scripts`
- b. `systemroot\sysvol\sysvol\domainname`

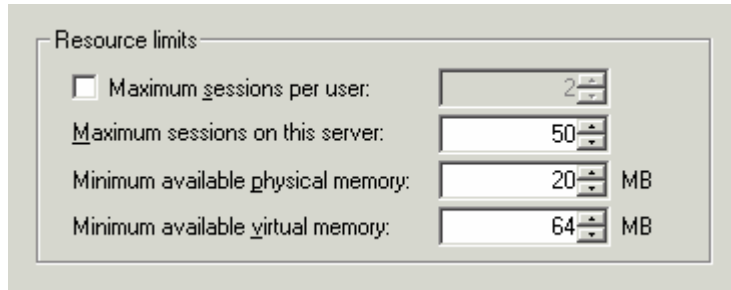
Additional tools such as DebugView, available from <http://www.microsoft.com/technet/sysinternals/utilities/DebugView.msp> can help track the cause of the problem when these errors occur. Open the DebugView executable on the server and check for any errors that point to the incorrect location of the script.

Setting Resource Limits

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

To limit the number of sessions per user

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



Specifying the Maximum Number of Sessions

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

To edit the maximum number of sessions per server

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

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

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

Session Shutdown Options

Through the Cluster Manager, 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 server. 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.

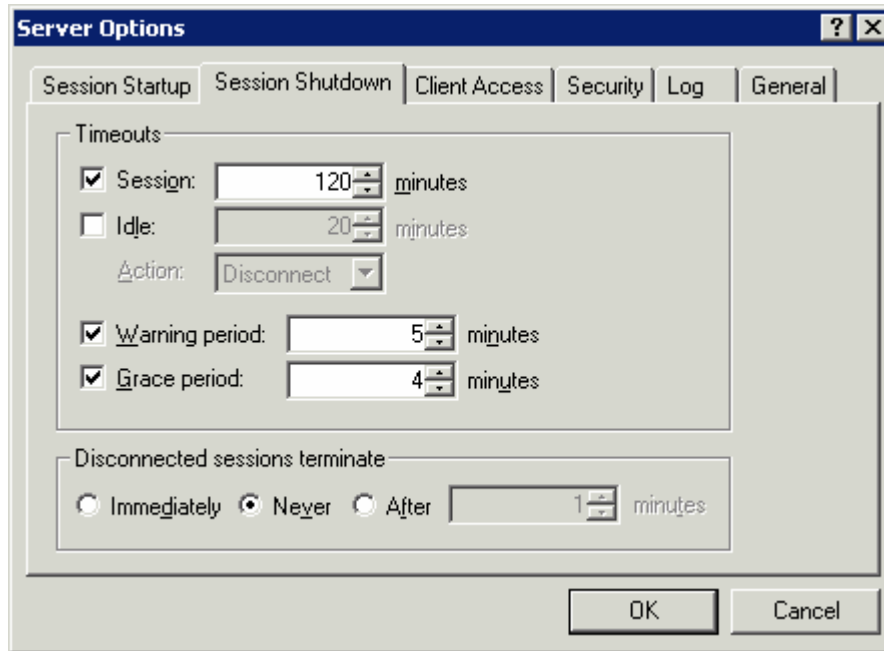
Specifying the Session Limit

The session limit is the number of minutes that a session is allowed to run on an iGoldMine Server.

To specify the session limit

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

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



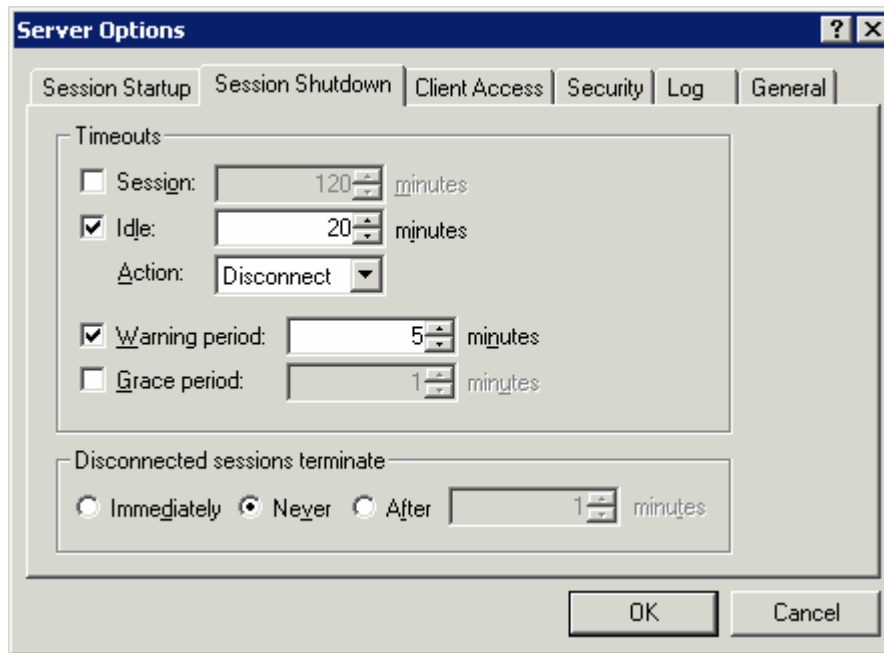
Specifying the Idle Limit

Idle time refers to the number of minutes since the last mouse or keyboard input event was received in a session. The idle limit is the number of minutes of idle time that an iGoldMine Server allows.

To specify the idle limit

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

The minimum amount of idle time is 1 minute and the maximum is 44640 minutes (31 days). 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. From the Cluster Manager, click Tools | Server Options.
2. Click **Session Shutdown**.
3. Enable **Warning period**.
4. In the edit box, type the number of minutes before a session or idle limit is reached when users are warned that they are about to be disconnected or logged off.
5. Click **OK**.

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. The session or idle limit determines when an automated logoff begins.

To specify the grace period

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

The minimum grace period value is 1 minute and the maximum value is 15. By default there is no grace period.

Managing iGoldMine Servers from Client Machines

Administrators can connect to the Cluster Manager from any client machine. This allows the administrator to end processes, terminate sessions, and administer applications from any machine running an iGoldMine client.

To access the Cluster Manager from a client machine

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

Keyboard Shortcuts for the Cluster Manager

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

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

Overview of iGoldMine Clients

iGoldMine clients are available for Windows, Windows CE, Linux, Pocket PC, Mac OS X and Java. iGoldMine also includes browser-based plug-ins for Windows, Linux, and Mac OS X; and a Microsoft ActiveX Control for Windows users running Internet Explorer.

The **Java Client** is available to Windows and Linux users. When running from a browser, users launch iGoldMine by browsing to an HTML page containing the Java applet. The browser automatically downloads the iGoldMine Client classes and launches the applet.

The **Linux Client** is a lightweight native X Window System application that delivers excellent performance to Linux desktops.

The **Windows Client** is a 32-bit Windows application that delivers excellent performance and can be installed and run on most Windows computers.

The **Windows CE Client** is a lightweight application that provides seamless integration with the native device's environment. Windows CE users can run iGoldMine from the Start menu, a desktop shortcut, or directly from the iGoldMine executable.

The **Pocket PC Client** is a lightweight application that provides seamless integration with the native device's environment. Windows mobile users can run iGoldMine from the Start menu or directly from the iGoldMine executable.

The **Netscape Plug-in** allows users to connect to an iGoldMine Server using Netscape Navigator. Users browse to an HTML page that contains a link to the Plug-in. The Netscape Plug-in is available for Windows and Linux clients.

The **Microsoft ActiveX Control** allows Windows users running Internet Explorer to automatically download and run the ActiveX Control. Users simply browse to an HTML page that contains the ActiveX Control.

The **Mac OS X Client** is a lightweight universal application that delivers excellent performance to Mac OS X desktops. Users can download and install iGoldMine.dmg and run iGoldMine from the Applications directory.

The **Browser Plug-in for Mac OS X** is available to Mac OS X users running Apple Safari or Mozilla Firefox. Users browse to an HTML page that contains a link to the Plug-in.

Preparing the iGoldMine Server for Web Access

The iGoldMine setup allows you to install the iGoldMine Web files directly into a sub-directory of your Web server home directory (for example, C:\InetPub\wwwroot\goglobal). During the setup, a dialog will prompt you to specify the name of your Web server. The setup will detect the location of your Web server's home directory and copy the files into a sub-directory of this location. logon.html is the default Web page for logging on to iGoldMine. logon.html automatically detects the client's operating system and lists only the iGoldMine clients that are installable on that client. Users can view the entire list of iGoldMine clients by clicking the "show all clients" link and accessing clients.html. You can modify logon.html and clients.html by deleting any clients you do not wish to make available. You can also modify these pages by adding your own corporate colors and logo, for example.

The following iGoldMine clients can be installed and run via logon.html and/or clients.html:

Windows Clients

- **Netscape Plug-in: loose windows** — Windows users running Netscape Navigator can run the Program Window outside the Web browser.
- **Netscape Plug-in: embedded windows** — Windows users running Netscape Navigator can run the Program Window inside the Web browser.
- **Microsoft ActiveX Control: loose windows** — Windows users running Internet Explorer can run the ActiveX Control outside the Web browser.
- **Microsoft ActiveX Control: embedded windows** — Windows users running Internet Explorer can run the ActiveX Control inside the Web browser.
- **Windows Client** — Windows users can install the Windows Client on their client computer and run iGoldMine from the Start menu or a desktop shortcut.
- **Windows CE Client** — Windows CE users can install the CE Client on their client device and run iGoldMine from the Start menu, the desktop shortcut, or directly from the iGoldMine executable.
- **Pocket PC Client** — Pocket PC 2003 and Windows Mobile 5 users can run the Pocket PC Client from the Start menu or directly from the iGoldMine executable.

Linux Clients

- **Netscape Plug-in: loose windows** — Linux users running Netscape Navigator can run the Program Window outside the Web browser.
- **Netscape Plug-in: embedded windows** — Linux users running Netscape Navigator can run the Program Window inside the Web browser.
- **Linux Client** — Linux users can install the Linux Client and run iGoldMine from the Linux console.

Mac OS X Clients

- **Browser Plug-in: loose windows** — Mac OS X users running Apple Safari or Mozilla Firefox can browse to an HTML page where they can install the iGoldMine Plug-in and run the Program Window outside the Web browser.
- **Browser Plug-in: embedded windows** — Mac OS X users running Apple Safari or Mozilla Firefox can browse to an HTML page where they can install the iGoldMine Plug-in and run the Program Window inside the Web browser.
- **Mac OS X Client** — Mac OS X users can download and install iGoldMine.dmg, then run iGoldMine from the Applications directory.

Java Clients

- **Signed Java Client** — The signed Java Client allows users to take advantage of the clipboard, client printing, and client file access features of iGoldMine.
- **Unsigned Java Client** — The unsigned Java Client is designed for users who do not want the Java applet to have access to their machine's file system. With the unsigned Java Client, client printing, client file access, and clipboard features are unavailable.

In addition to logon.html and clients.html, the following HTML pages are located in the sub-directory of your Web server home directory:

HTML Page	Description
embeddedactivexlogon.html	Logon page for users running the Microsoft ActiveX Control in embedded windows mode.
embeddedlinuxpluginlogon.html	Logon page for Linux users running the Netscape Plug-in in embedded windows mode.
embeddedmacpluginlogon.html	Logon page for Mac OS X users running the Browser Plug-in in embedded windows mode.
embeddedwindowspluginlogon.html	Logon page for Windows users running the Netscape Plug-in in embedded windows mode.
installICE.html	Install page for the Windows CE Client.
installnativelinux.html	Install page for the native Linux Client. (ggw.rpm)
installnativemac.html	Install page for the native Mac OS X Client.
installnativewindows.html	Install page for the native Windows Client. (goglobal-client.exe)
installpluginlinux.html	Install page for the Netscape Plug-in for Linux.
installpluginmac.html	Install page for the Browser Plug-in for Mac OS X.
installPPC.html	Install page for the Pocket PC Client.
javalogonsigned.html	Logon page for users running the signed Java Client.
javalogonunsigned.html	Logon page for users running the unsigned Java Client.
looseactivexlogon.html	Logon page for users running the ActiveX Control in loose windows mode.
looselinuxpluginlogon.html	Logon page for Linux users running the Netscape Plug-in in loose windows mode.
loosemacpluginlogon.html	Logon page for Mac OS X users running the Browser Plug-in in loose windows mode.
loosewindowspluginlogon.html	Logon page for Windows users running the Netscape Plug-in in loose windows mode.
netscapeplugininstaller.html	Install page for Windows users running Netscape.

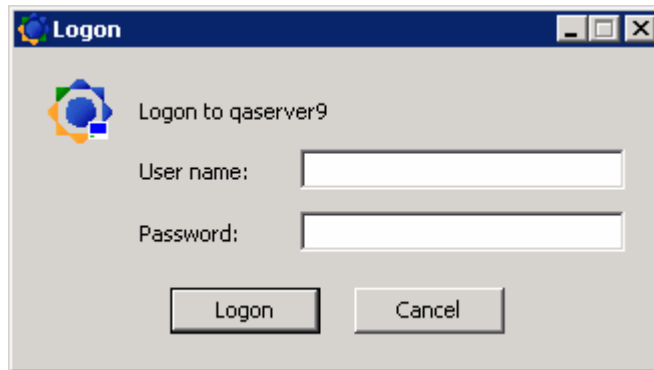
Java Client

The Java Client is available to Windows and Linux users. Users launch iGoldMine by browsing to an HTML page containing the logon applet.

To run the Java Client

1. Start Netscape Navigator or Internet Explorer.
2. In the Location box, type `http://` followed by the server name and the iGoldMine logon file. For example, `http://server/logon.html`
3. Select either the **signed** or **unsigned** Java Client from the list of iGoldMine clients.
4. When the **Logon** dialog appears, type the following information:
 - Network username in the **User name** box.
 - Network password in the **Password** box.

Note: 32-bit True Color does not work well with certain applications deployed via the Java Client. Clients should change their color palette settings to anything less than True Color.



Note: iGoldMine allows users three invalid logon attempts before shutting down the logon process.

The signed Java Client is designed for users who wish to take advantage of the client integration features of iGoldMine, and are not concerned with the Java applet having access to their file system and clipboard. Users who do not want the applet to have access to their machine's file system should select the unsigned Java Client. With the unsigned version, clipboard, client printing, and client file access features are unavailable.

Startup Parameters for the Java Client

iGoldMine allows for specifying startup parameters in the install HTML pages. For example, you can modify the Web pages to launch specific applications, and to bypass the Logon dialog. The Web pages can be modified in any HTML editor. The parameters for the **Java Client** are as follows:

user	The client's network user name.
password	The client's network password.
host*	The name of the machine the Application Publishing Service is running on.
application	The application the client wishes to run, as registered with the Cluster Manager. (If this parameter is not specified in the HTML file, the Program Window will launch.)

compression	Administrators should activate compression if the iGoldMine client is running over dial-up network, or whenever there is low bandwidth. COMPRESSION= "true" enables compression. COMPRESSION= "false" disables compression. (Compression is enabled by default.)
desktopcolor	This argument is used to set the background color of the desktop when iGoldMine is run inside the browser. Possible values are as follows: black, blue, cyan, darkgray, gray, green, lightgray, magenta, orange, pink, red, white, and yellow.
args	This passes on specific application parameters for the application about to be launched. The signed version of the Java Client requires double \\ characters when using the args parameter. For example, "args", "C:\\word\\test.doc"
height	Height of the applet in pixels.
width	Width of the applet in pixels.
hostport	Modifies the host port setting for the Application Publishing Service.

*The host parameter is available for the signed Java Client only. It is not available to users of the unsigned Java Client.

Example:

```
<APPLET CODE= "com.graphon.ggw.Logon"
WIDTH= "800" HEIGHT= "600"
ARCHIVE= "ggw.jar, ggw.res.jar">
<PARAM NAME= "user" VALUE= "Jane">
<PARAM NAME= "password" VALUE= "Doel">
<PARAM NAME= "application" VALUE= "Notepad">
<PARAM NAME= "compression" VALUE= "true">
<PARAM NAME= "desktopcolor" VALUE= "blue">
<PARAM NAME= "args" VALUE= "C:\\Readme.txt">
<PARAM NAME= "hostport" value= "443">
</APPLET>
```

Note: By configuring logon pages to bypass the Program Window, users will be unable to add or modify client printers.

Uninstalling the Java Client

To remove the Java Client files, clear the cache in the web browser:

- In Netscape Navigator, click Edit | Preferences. Click the **Advanced** category and select **Clear Cache**.
- In Internet Explorer, click Tools | Internet Options. Click the **General** tab and under **Temporary Internet Files**, click **Delete Files**.

Netscape Plug-in

The Netscape Plug-in is available to Windows and Linux users running Netscape Navigator. The Plug-in can be run in either loose or embedded windows mode. The embedded windows mode runs the Program Window inside the Web browser. The loose windows mode runs the Program Window outside the Web browser.

Running the Netscape Plug-in for Windows

The Netscape Plug-in for Windows supports Windows machines running Netscape Navigator.

To run the Netscape Plug-in for Windows

1. Start Netscape Navigator.
2. In the Location box, type `http://` followed by the server name and the iGoldMine logon file. For example, **`http://server/logon.html`**
3. Select the appropriate **Netscape Plug-in** link from the list of Windows clients.
4. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Uninstalling the Netscape Plug-in for Windows

After uninstalling the Netscape Plug-in, we recommend that users clear the Netscape browser cache.

To uninstall the Netscape Plug-in for Windows

1. Close Netscape Navigator.
2. Locate the Netscape **Plugins** folder.
3. Delete all **iGoldMine** client DLLs.

Running the Netscape Plug-in for Linux

The **Netscape Plug-in for Linux** is available to Linux users running Netscape Navigator.

To install the Netscape Plug-in for Linux

1. Start Netscape Navigator.
2. In the Location box, type `http://` followed by the server name and the iGoldMine logon file. For example, **`http://server/logon.html`**.
3. Select the appropriate **Netscape Plug-in** link from the list of Linux clients. This Web page will either prompt you to download the Netscape Plug-in or will launch the **Logon** dialog automatically.
4. Install the Plug-in from your home directory with the following command:
`tar xzf ggw-plugin.tgz`

To run the Netscape Plug-in for Linux

1. Start Netscape Navigator.
2. In the Location box, type `http://` followed by the server name and the iGoldMine logon file. For example, **`http://server/logon.html`**
3. Select the appropriate **Netscape Plug-in** link from the list of Linux clients.
4. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Installing the native Linux Client with the **ggw.rpm** package will also install the Netscape Plug-in for Linux. Users simply browse to the logon page containing the Netscape Plug-in. If the user accessing the machine does not have root access, however, he or she will have to install the Plug-in.

Uninstalling the Netscape Plug-in for Linux

To remove the Netscape 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/ggw`
3. If you plan to reinstall the Netscape Plug-in, we recommend clearing the Netscape browser cache.

Startup Parameters for the Netscape Plug-in

Install HTML pages for the Netscape Plug-in can be modified in any HTML editor. The parameters for the **Netscape Plug-in** are as follows:

Parameter	Description
user	The client's network user name.
password	The client's network password.
host*	The name of the machine the Application Publishing Service is running on.
application	The application the client wishes to run, as registered with the Cluster Manager. (If this parameter is not specified in the HTML file, the Program Window will launch.)
compression	Administrators should activate compression if the iGoldMine client is running over dial-up network, or whenever there is low bandwidth. compression= "true" enables compression. compression= "false" disables compression. compression=true by default.
args	This passes on specific application parameters for the application about to be launched.
isembeddedwin	Determines whether the Plug-in is run in loose or embedded windows mode. isembeddedwin= "true" signifies embedded windows mode. isembeddedwin="true" by default.
autoclosebrowser	When autoclosebrowser="true" closing the Program Window closes the associated browser window and ends the user's iGoldMine session. When autoclosebrowser="false", closing the Program Window ends the user's iGoldMine session, but does not close the browser window. autoclosebrowser="false" by default.
inbrowserprocess	When inbrowserprocess="true" closing the browser that contains the iGoldMine Plug-in will end the user's iGoldMine session. When inbrowserprocess="false" closing the browser will not end the user's iGoldMine session. inbrowserprocess="true" by default.
autoconfigprinters	Determines how printers are initialized at startup. When autoconfigprinters="all" all client printers are automatically configured. When autoconfigprinters="none" client printers are not automatically configured. When autoconfigprinter= "default" the default printer is configured automatically. This is the default setting.
hostport	Modifies the host port setting for the Application Publishing Service.

*If no host is specified in the logon HTML page, the Plug-in detects the machine from where the logon file was downloaded, and makes the connection to that server. The user bypasses the **Connection** dialog and is presented with the **Logon** dialog only.

If host= "?" the **Connection** dialog will appear and clients must type in a server address. If you specify a server address in the logon HTML page using the host tag (e.g., host= "server"), the user will bypass the **Connection** dialog and will connect to that specified server.

Example:

```
<EMBED TYPE="application/x-ggw-plugin" width="1" height="1" user="Jane"
password="Doel" host="server1" application="Notepad" args="
C:\Readme.txt" isembeddedwin="false" compression="true"
autoclosebrowser="false" inbrowserprocess="true" hostport="1667">
</EMBED>
```

When using parameters with the Netscape Plug-in, the text **"** must be used to accommodate spaces in application names and application arguments. For example, if the application is registered with the Cluster Manager with a space **"** must be used. For example,

```
<EMBED TYPE="application/x-ggw-plugin" width="1" height="1"
application="&quot;Acrobat Reader&quot;"
args="&quot;C:\My Documents\Reports.doc&quot;" C:\Bootlog.txt"
</EMBED>
```

Note: If inbrowserprocess is set to "false" and autoclosebrowser is set to "true", the user's browser will close as soon as the iGoldMine session launches.

ActiveX Control

The Microsoft ActiveX Control is available to Windows users running Internet Explorer.

To run the ActiveX Control

1. Start Internet Explorer.
2. In the Address box, type http:// followed by the server name and iGoldMine logon page. For example, **http://server/logon.html**
3. Select the appropriate **ActiveX Control** from the list of Windows clients.
4. Trust the digitally signed ActiveX Control.
5. When the **Logon** dialog appears, type the following information:
 - Network username in the **User name** box.
 - Network username in the **Password** box.

Startup Parameters for the ActiveX Control

Install HTML pages for the ActiveX Control can be modified in any HTML editor. The parameters for the **ActiveX Control** are identical to the parameters for the Netscape Plug-in:

Parameter	Description
user	The client's network user name.
password	The client's network password.
host*	The name of the machine the Application Publishing Service is running on.
application	The application the client wishes to run, as registered with the Cluster Manager. (If this parameter is not specified in the HTML file, the Program Window will launch.)
compression	Administrators should activate compression if the iGoldMine client is running over dial-up network, or whenever there is low bandwidth. compression= "true" enables compression. compression= "false" disables compression. compression=true by default.
args	This passes on specific application parameters for the application about to be launched.

isembeddedwin	Determines whether the Plug-in is run in loose or embedded windows mode. isembeddedwin= "true" signifies embedded windows mode. isembeddedwin="true" by default.
autoclosebrowser	When autoclosebrowser="true" closing the Program Window closes the associated browser window and ends the user's iGoldMine session. When autoclosebrowser="false", closing the Program Window ends the user's iGoldMine session, but does not close the browser window. autoclosebrowser="false" by default.
inbrowserprocess	When inbrowserprocess="true" closing the browser that contains the ActiveX Control will end the user's iGoldMine session. When inbrowserprocess="false" closing the browser will not end the user's iGoldMine session. inbrowserprocess="true" by default.
autoconfigprinters	Determines how printers are initialized at startup. When autoconfigprinters="all" all client printers are automatically configured. When autoconfigprinters="none" client printers are not automatically configured. When autoconfigprinter= "default" the default printer is configured automatically. This is the default setting.
hostport	Modifies the host port setting for the Application Publishing Service.

*If no host is specified in the logon HTML page, the ActiveX Control detects the machine from where the logon file was downloaded, and makes the connection to that server. The user bypasses the **Connection** dialog and is presented with the **Logon** dialog only.

If host= "?" the **Connection** dialog will appear and clients must type in a server address. If you specify a server address in the logon HTML page using the host tag (e.g., host= "server"), the user will bypass the **Connection** dialog and will connect to that specified server.

Example:

```
<OBJECT ID="Control1" WIDTH=0 HEIGHT=0
  CLASSID="CLSID:76850F2A-FCAA-454F-82D3-BD46CB186EF5"
  CODEBASE="ggw-activex.cab#Version=2,0,0,0" >
<PARAM NAME="user" VALUE="Jane">
<PARAM NAME="password" VALUE="Doel">
<PARAM NAME="host" VALUE="server1">
<PARAM NAME="application" VALUE="Acrobat">
<PARAM NAME="args" VALUE="C:\Readme.txt ">
<PARAM NAME="isembeddedwin" VALUE="false">
<PARAM NAME="compression" VALUE="true">
</OBJECT>
```

When using parameters with the ActiveX Control, the text **"** must be used to accommodate spaces in application names and application arguments. For example,

```
<OBJECT ID="Control1" WIDTH=0 HEIGHT=0
  CLASSID="CLSID:76850F2A-FCAA-454F-82D3-BD46CB186EF5"
  CODEBASE="ggw-activex.cab#Version=2,0,0,0" >
<PARAM NAME="application" VALUE="&quot;Acrobat Reader&quot;">
<PARAM NAME="args" VALUE="&quot;c:\my test\my file.txt.txt&quot;">
</OBJECT>
```

Note: If users experience slow scrolling with iGoldMine, try disabling the smooth scrolling option on the server. In Internet Explorer, click Tools | Internet Options. Click the **Advanced** tab. In the **Settings** box, under **Browsing**, disable **Use smooth scrolling**.

Uninstalling the ActiveX Control

To uninstall the ActiveX Control

1. Close Internet Explorer.
2. Locate and delete **IEGCtrl Class** in Winnt or Windows\Downloaded Program files.

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.

Windows Client

The Windows Client is a 32-bit Windows application that can be installed and run on most Windows computers.

To install the Windows Client

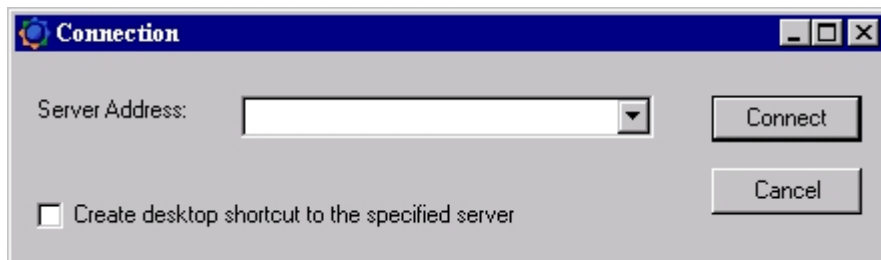
1. Start Netscape Navigator or Internet Explorer.
2. In the Location box, type http:// followed by the server name and iGoldMine logon page. For example, **http://server/logon.html**
3. Select the **Windows Client** link from the list of iGoldMine clients.
4. Follow the on-screen instructions which will prompt you to download the Windows client executable. (ggw-client.exe)

Running the Windows Client from the Start Menu

Users can run the Windows Client from the Start menu or from a Windows shortcut.

To run iGoldMine from the Start menu

1. Click the **Start** button on the Windows taskbar.
2. Select Programs | FrontRange Solutions iGoldMine | iGoldMine Client.
3. Type your server address in the **Connection** dialog. If you would like to create a desktop shortcut to the specified server, select the check box. Once the shortcut is set up, you will bypass the Connection dialog when connecting to the specified server.
4. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.



Running the Windows Client from a Shortcut

A Windows shortcut named **iGoldMine Client** is created during installation of the Windows Client. This shortcut launches the Program Window.

To run the Windows Client from a shortcut

1. Double-click the **iGoldMine Client** shortcut.
2. Type your server address in the **Connection** dialog. If you would like to create a desktop shortcut to the specified server, select the check box. Once the shortcut is set up, you will bypass the Connection dialog when connecting to the specified server.
3. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Creating iGoldMine Shortcuts

Users can create additional shortcuts that launch specific applications.

To create an iGoldMine shortcut

1. Right-click on the desktop.
2. Click New | Shortcut.
3. In the **Create Shortcut** dialog box, browse to the iGoldMine Client executable. For example, \Program Files\GraphOn\iGoldMine Client\ggw.exe
4. Type a name for the shortcut and click **Finish**.

Command-Line Arguments for the Windows Client

Command-line arguments can be used to make the logon process easier. For instance, by adding the argument **-h** followed by the server name, and **-u** followed by the user name, the user will only be required to type a password in the **Logon** dialog.

To run iGoldMine using command-line arguments

1. Right-click on an iGoldMine shortcut and click **Properties**.
2. In the **Shortcut** tab, place the cursor in the **Target** edit box and append any of the following command-line arguments after the quote ("):

Argument	Description
-h	The iGoldMine Server address or host name.
-u	The client's network user name.
-p	The client's network password.
-a	The display name of the application to be launched. The application's display name should be identical to the application registered with the Cluster Manager.
-c or -nc	-c enables compression. -nc disables compression. (Compression is enabled by default.)
-r	Startup parameters for the application
-ac	Determines how printers are initialized at startup. When -ac is followed by all , all client printers are automatically configured. When -ac is followed by none , client printers are not automatically configured. When -ac is followed by default , only the default printer is configured automatically. This is the default setting.
-hp	Modifies the host port setting for the Application Publishing Service.

Example: ...\\ggw.exe" -h server -p password -a application -c -ac all -hp 443

- Command-line arguments are optional and case-insensitive. Arguments can be appended in any order, with the exception of **-r**. If **-r** is used, it must be the last argument on the command-line and it must be used with the **-a** argument.

- When the **-a** argument is used, the Program Window is not launched, even if the application does not exist.
- Startup parameters passed on by the **-r** argument are specific to each application. Please refer to the application's documentation for information about launch parameters.
- If a user does not have a password, **-p ""** can be used to bypass the **Logon** dialog, as long as the user name has also been specified on the command-line.
- In order to accommodate spaces in user names, passwords, application display names, or application arguments, quotation marks must be included when using command-line arguments. For example, the argument **-a "Acrobat Reader"** would launch Adobe's Acrobat Reader. Likewise, user name Jim C would be specified as **-u "Jim C"**.

Uninstalling the Windows Client

Uninstall the Windows Client through **Add/Remove Programs**.

Linux Client

The Linux Client is a lightweight native X Window System application that delivers excellent performance to Linux desktops.

To install the Linux Client

1. Launch your Web browser.
2. In the location box, type `http://` followed by the server name and the iGoldMine logon file. For example, **`http://server/logon.html`**
3. Click the **Linux Client** link from the list of Linux clients.
4. Save the iGoldMine package.
5. Launch the Linux console and become root (Super User).
6. Install the package using: **`rpm -Uvh`**. (For example, **`rpm -Uvh ggw.rpm`**)

Installing the Linux Client with the **ggw.rpm** package will also install the Netscape Plug-in for Linux. Users simply browse to the logon page containing the Netscape Plug-in in order to run iGoldMine. Users on the client machine without root access, however, will have to install the Plug-in.

To run the Linux Client

1. In the Linux console, type **ggw**
2. Type the server address in the **Connection** dialog.
3. When the **Logon** dialog appears, enter the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Command-Line Arguments for the Linux Client

The Linux Client supports the following command-line arguments:

Argument	Description
-h	The iGoldMine Server address or host name.
-u	The client's network user name.
-p	The client's network password. Please note that if you specify a password on the command-line, the password may be visible to other users running process reporting tools such as ps. To protect the user's password, use -p - to request the password at startup.
-a	The display name of the application. The application's display name must be identical to the application name registered with the Cluster Manager.
-c or -nc	-c enables compression. -nc disables compression. (Compression is enabled by default.)
-f	The Linux Client runs in a loose window mode by default. To enable the restricted frame option, i.e., to have all of the session's windows embedded within a frame on the client computer, append -f to the command line.
-r	Passes on startup parameters for the application being launched.
-ac	Determines how printers are initialized at startup. When -ac is followed by all , all client printers are automatically configured. When -ac is followed by none , client printers are not automatically configured. When -ac is followed by default , only the default printer is configured automatically. This is the default setting.
-hp	Modifies the host port setting for the Application Publishing Service.

Example: `ggw -h server1 -p password -ac all -hp 443`

- Startup parameters passed on by the **-r** argument are specific to each application. Please refer to the application's documentation for information about launch parameters.
- Command-line arguments are optional and case-insensitive. Arguments can be appended in any order, with the exception of **-r**. If **-r** is used, it must be the last argument on the command-line and it must be used with the **-a** argument.
- In order to accommodate spaces in user names, passwords, application display names, or application arguments, quotation marks must be included when using command-line arguments. For example, user name Jim C would be specified as **-u "Jim C"**.

Resizing the Client Window of the Linux Client

The command-line argument **-geometry** can be used to modify the size of the client window when running in frame mode. Without -geometry on the command-line, the client window will be maximized. When the Linux Client is run in loose window mode, **-geometry** will have no effect.

To resize the client window

Append **-geometry** to the command-line, followed by the desired width and height.

Example:

```
ggw -h 196.125.101.222 -f -geometry800x600
-or-
ggw -h 196.125.010.222 -f -geometry=800x600
```

Uninstalling the Linux Client

The Linux Client can be uninstalled by typing **rpm -e ggw** in the Linux console.

Mac OS X Client

The Mac OS X Client is a lightweight application that provides seamless integration with the native Mac environment.

To install the Mac OS X Client

1. Launch a Web browser.
2. In the location box, type `http://` followed by the server name and the iGoldMine logon file. For example, `http://server/logon.html`.
3. Click the **Mac OS X Client** link from the list of clients.
4. Follow the instructions to download and install **iGoldMine.dmg**.

To run the Mac OS X Client

1. From the menu bar, click Go | Applications.
2. Double-click **ggw** to launch iGoldMine.
3. Type the server address in the **Connection** dialog.
4. When the **Logon** dialog appears, enter the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Command-Line Arguments for the Mac OS X Client

The Mac OS X Client supports the following command-line arguments:

Argument	Description
-h	The IP address of the iGoldMine Server.
-u	The client's network user name.
-p	The client's network password. Please note that if you specify a password on the command-line, the password may be visible to other users running process reporting tools such as ps. To protect the user's password, use -p - to request the password at startup.
-a	The display name of the application. The application's display name must be identical to the application name registered with the Cluster Manager.
-c or -nc	-c enables compression. -nc disables compression. (Compression is enabled by default.)
-f	The Mac OS X Client runs in a loose windows mode by default. To enable the restricted frame option, i.e., to have all of the session's windows embedded within a frame on the client computer, append -f to the command line.
-r	Passes on startup parameters for the application being launched.
-ac	Determines how printers are initialized at startup. When -ac is followed by all , all client printers are automatically configured. When -ac is followed by none , client printers are not automatically configured. When -ac is followed by default , only the default printer is configured automatically. This is the default setting.
-hp	Modifies the host port setting for the Application Publishing Service.

- Startup parameters passed on by the **-r** argument are specific to each application. Please refer to the application's documentation for information about launch parameters.
- Command-line arguments are optional and case-insensitive. Arguments can be appended in any order, with the exception of **-r**. If **-r** is used, it must be the last argument on the command-line and it must be used with the **-a** argument.
- In order to accommodate spaces in user names, passwords, application display names, or application arguments, quotation marks must be included when using command-line arguments. For example, user name Jim C would be specified as **-u "Jim C"**.

To use command-line arguments with the Mac OS X Client

1. Open Terminal.
2. Change to the /Applications/ggw.app/Contents/MacOS/ directory.
3. Type **./ggw** and append command-line arguments.

Example:

```
./ggw -h 196.125.101.222 -c -ac all -hp 443
```

Resizing the Client Window of the Mac OS X Client

The command-line argument **-geometry** can be used to modify the size of the client window when the command-line argument **-f** is used. Without **-geometry** on the command-line, the client window will be maximized. When the Mac OS X Client is run in loose window mode, **-geometry** will have no effect.

To resize the client window

Append **-geometry** to the command-line, followed by the desired width and height.

Example:

```
./ggw -h 196.125.101.222 -f -geometry800x600  
-or-  
./ggw -h 196.125.010.222 -f -geometry=800x600
```

Uninstalling the Mac OS X Client

1. Open Terminal.
2. Log on as **root**. (Type **su** and hit **Enter**, then provide the root password).
3. Change to the /Applications/ggw.app/Contents/Utils/ directory.
4. Run the script by typing **./Uninstall.sh**
5. Close Terminal.

Browser Plug-in for Mac OS X

The **Browser Plug-in for Mac OS X** is available to Mac OS X users running Apple Safari or Mozilla Firefox.

To install the Browser Plug-in for Mac OS X

1. Launch a Web browser.
2. In the Location box, type **http://** followed by the server name and the iGoldMine logon file. For example, **http://server/logon.html**.
3. Select the appropriate Browser Plug-in link from the list of Mac OS X clients. This Web page will either prompt you to download the Plug-in or will launch the Logon dialog automatically.
4. Install the Plug-in by downloading and running **iGoldMine.dmg**.

Installing the native Mac OS X Client with the iGoldMine package (iGoldMine.pkg) will also install the Browser Plug-in for Mac OS X. Users simply browse to the logon page containing the Browser Plug-in.

To run the Browser Plug-in for Mac OS X

1. Start the Web browser.
2. In the Location box, type `http://` followed by the server name and the iGoldMine logon file. For example, **`http://server/logon.html`**
3. Select the appropriate **Browser Plug-in** link from the list of Mac OS X clients.
4. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box

Startup Parameters for the Browser Plug-in for Mac OS X

The default logon HTML pages for the Browser Plug-in for Mac OS X (`loosemacpluginlogon.html` and `embeddedmacpluginlogon.html`) include startup parameters that can be modified in any HTML editor.

Parameter	Description
user	The client's network user name.
password	The client's network password.
host*	The name of the machine the Application Publishing Service is running on.
application	The application the client wishes to run, as registered with the Cluster Manager. (If this parameter is not specified in the HTML file, the Program Window will launch.)
compression	Administrators should activate compression if the iGoldMine client is running over dial-up network, or whenever there is low bandwidth. <code>compression= "true"</code> enables compression. <code>compression= "false"</code> disables compression. <code>compression=true</code> by default.
args	This passes on specific application parameters for the application about to be launched.
isembeddedwin	Determines whether the Plug-in is run in loose or embedded windows mode. <code>isembeddedwin= "true"</code> signifies embedded windows mode. <code>isembeddedwin="true"</code> by default.
autoclosebrowser	When <code>autoclosebrowser="true"</code> closing the Program Window closes the associated browser window and ends the user's iGoldMine session. When <code>autoclosebrowser="false"</code> , closing the Program Window ends the user's iGoldMine session, but does not close the browser window. <code>autoclosebrowser="false"</code> by default.
autoconfigprinters	Determines how printers are initialized at startup. When <code>autoconfigprinters="all"</code> all client printers are automatically configured. When <code>autoconfigprinters="none"</code> client printers are not automatically configured. When <code>autoconfigprinter= "default"</code> the default printer is configured automatically. This is the default setting.
hostport	Modifies the host port setting for the Application Publishing Service.

*If no host is specified in the logon HTML page, the Plug-in detects the machine from where the logon file was downloaded, and makes the connection to that server. The user bypasses the Connection dialog and is presented with the Logon dialog only.

Example:

```
<EMBED TYPE="application/x-ggw-plugin" WIDTH="800" height="600"
user="Jane" password="Doel" host="server1" application="Notepad"
isembeddedwin="true" compression="true" hostport=""
autoclosebrowser="false" inbrowserprocess="true"
autoconfigprinters="default">
</EMBED>
```

When using parameters with the Browser Plug-in for Mac OS X, the text **"** must be used to accommodate spaces in application names and application arguments. For example, if the application is registered with the Cluster Manager with a space **"** must be used.

Uninstalling the Browser Plug-in for Mac OS X

1. Open Terminal.
2. Log on as **root**. (Type **su** and hit **Enter**. Then provide the root password.)
3. Change to the /Applications/ggw.app/Contents/Utils/ directory.
4. Run the script by typing **./Uninstall.sh**
5. Close Terminal.

Windows CE Client

To run the Windows CE Client, devices must have TCP/IP as a network protocol. SEH (the C++ Structured Exception Handling component) and RTTI (the Run-Time Type Information component) are required to run iGoldMine on a Windows CE device. To determine if these components exist on the device, open **ceconfig.h** found in the Windows folder.

On a Windows CE 4 device, if the following lines:

```
#define COREDLL_CRT_RTTI 1
#define COREDLL_CRT_CPP_SEH 1
```

are included in this file, RTTI and SEH are supported.

On a Windows CE 5 device, if the following line:

```
#define COREDLL_CRT_CPP_EH_AND_RTTI 1
```

is included in this file, RTTI and SEH are supported.

Installing the Windows CE Client

Once the Windows CE Client has been installed, users can log on to an iGoldMine Server from the Start menu, from a desktop shortcut, or directly from the iGoldMine executable. The Windows CE install program attempts to delete **iGoldMine.CAB** at the end of installation. As such, we recommend setting the iGoldMine.CAB file permission to read-only before installing it on the client device.

To install the Windows CE Client with .CAB file support

1. Start Internet Explorer.
2. In the Address box, type `http://` followed by the server name and iGoldMine logon page. For example, **`http://server/logon.html`**
3. Click the **Windows CE Client** link.
4. Determine which processor your Windows CE device is using and download the appropriate .CAB file (ARMV4, ARMV4I or X86).
5. Double-click the .CAB file.

The Windows CE Client can be installed manually by launching **iGoldMine.CAB** from the corresponding CPU folder on the client device. For example, `Clients\CE\X86\iGoldMine.CAB`

To install the Windows CE Client on devices without .CAB file support

1. Locate the following files from the appropriate CPU folder in `Clients\CE\CPU\Programs` (for example, `Clients\CE\X86\Programs*.*`):
ggw.exe
clipc.dll
cs.dll
dc.dll
filec.dll
pbru.dll
sc.dll
scres.dll
sndc.dll
printc.dll
upc.dll
2. Copy these files to a common directory on the client device. (For example, copy `Clients\CE\X86\Programs*.*` to `YourCEDevice\iGoldMine\`)
3. In the directory created in step 2, create a subdirectory named **kbd**. Copy any desired keyboard mapping file(s) from `Clients\CE\kbd` to this new directory. (For example, copy `Clients\CE\X86\Programs\fr_FR.kbm` to `YourCEDevice\iGoldMine\kbd\`.)

Running the Windows CE Client from the Start Menu

Users running CE devices with taskbar support can run the Windows CE Client from the Start menu.

To run iGoldMine from the Start menu

1. Click the **Start** button on the Windows taskbar.
2. Select `Programs | GraphOn iGoldMine | iGoldMine Client`.
3. Type your server address in the **Connection** dialog.
4. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Running the Windows CE Client from a Shortcut

On Windows CE devices with desktop shortcut support, a Windows shortcut named **iGoldMine Client** is created during installation of the Windows CE Client. This shortcut launches the Program Window.

To run the Windows Client from a shortcut

1. Double-click the **iGoldMine Client** shortcut.
2. Type your server address in the **Connection** dialog.
3. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Running the Windows CE Client from the iGoldMine Executable

Users with CE devices that do not support the shortcut or Start menu launching options can run iGoldMine directly from the iGoldMine client executable.

To run the Windows CE Client

1. Run **ggw.exe** on the client device.
2. Type the server address in the **Connection** dialog and click **Connect**.
3. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Command-Line Arguments for the Windows CE Client

If a shortcut for ggw.exe can be created on the CE device's desktop, command-line arguments can be used to expedite the logon process. For example, the command-line arguments **-a** allows users to directly launch an application. Command-line arguments can also be used to pass on application specific startup parameters and to enable compression.

To run iGoldMine using command-line arguments

1. Right-click on an iGoldMine shortcut and click **Properties**.
2. In the **Shortcut** tab, place the cursor in the **Target** edit box and append any of the following command-line arguments after the quote ("):

Argument	Description
-h	The iGoldMine Server address or host name.
-u	The client's network user name.
-p	The client's network password.
-a	The display name of the application to be launched. The application's display name should be identical to the application registered with the Cluster Manager.
-r	Startup parameters for the application
-hp	Modifies the host port setting for the Application Publishing Service.
-c or -nc	-c enables compression. -nc disables compression. (Compression is enabled by default.)

Example: `...\ggw.exe" -h server -u username -p password -c -hp 443`

- Startup parameters passed on by the **-r** argument are specific to each application. Please refer to the application's documentation for information about launch parameters.

- Command-line arguments are optional and case-insensitive. Arguments can be appended in any order, with the exception of **-r**. If **-r** is used, it must be the last argument on the command-line and it must be used with the **-a** argument.
- In order to accommodate spaces in user names, passwords, application display names, or application arguments, quotation marks must be included when using command-line arguments. For example, user name Jim C would be specified as **-u "Jim C"**.

Including iGoldMine in a Windows Based Terminal CE Image

The iGoldMine client can be added to a WBT (Windows Based Terminal) platform using Platform Builder for easy integration into the standard Microsoft WBT shell.

To include iGoldMine in a WBT CE Image

1. Copy all files from **Clients\CE\Your CPU\Programs** folder to ...**Your WBT Platform\WINCE420\Your BSP\oak\files** directory on your platform build machine.
For example: from Clients\CE\X86\Programs* to
C:\WINCE420\WTC\WINCE420\Geode\oak\files
2. Copy the **ggw.bib** and **ggw.reg** file from **Clients\CE\WBT** to the same **files** directory on your platform build machine.
3. Copy the two .exe files from **Clients\CE\WBT\YourCPU** to the same files directory on your platform build machine. For example, from Client\CE\WBT\X86*. * to
C:\WINCE420\WTC\WINCE420\Geode\oak\files
4. Open your WBT project in Platform Builder.
5. Select the **ParameterView** tab from the **Workspace** window.
6. Expand the **Your BSP** item. For example, "Geode"
7. Expand the Project Specific Files item.
8. Open the **project.bib** file.
9. Add the following line to your **project.bib** file
#include "\$(_FLATRELEASEDIR)\ggw.bib"
10. Open the **project.reg** file.
11. Add the following line to your **project.reg** file
#include "\$(_FLATRELEASEDIR)\ggw.reg"
12. **Build** your WBT project and **Make** the device image.

Running the Windows CE Client on a WBT Device

Users can launch iGoldMine from a WBT device that already has iGoldMine installed on it.

To setup up an iGoldMine connection

1. Select the Configure tab from the Terminal Connection Manager.
2. Click the **Add** button
3. Select **iGoldMine Client** from the drop-down list
4. Click **OK**.
5. Type a connection name in the **Connection Name** box.
6. Optionally enter any command-line options for this connection in the **Command-Line Option** box.
7. Click **Next**.
8. If your connection name is valid, the following message is displayed: "A connection has been created with the name." Click **Finish**. The new connection will be displayed in the **Terminal Connection Manager**.

The connection name cannot be longer than 32 characters, cannot begin with a space, and cannot contain the following characters: / \ : * ? " < > | , . [] () Also, the connection name cannot match the name of an existing iGoldMine connection.

To edit the name or command-line options of a connection

1. In the **Configure** tab of the **Terminal Connection Manager** select the desired connection to modify.
2. Click **Edit**.
3. Optionally make changes to the name and command-line options for this connection.
4. Click **OK**.

To delete a connection

1. In the **Configure** tab of the **Terminal Connection Manager** select the desired connection to delete.
2. Click **Delete**.

To run an iGoldMine connection

1. Click the **Connections** tab of the **Terminal Connection Manager**.
2. Select the desired connection to run.
3. Click the **Connect** button.
4. Type your server address in the **Connection** dialog.
5. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Uninstalling the Windows CE Client

To uninstall the Windows CE Client, delete the installation files from the directory on the client device to which you copied them. These files include:

ggw.exe
clipc.dll
cs.dll
dc.dll
filec.dll
pbru.dll
sc.dll
scres.dll
sndc.dll
printc.dll
upc.dll

Pocket PC Client

iGoldMine's **Pocket PC Client** is available for Pocket PC 2003 and Windows Mobile 5 for Pocket PC.

Installing the Pocket PC Client

Once the Pocket PC Client has been installed, users can log on to an iGoldMine Server from the Start menu or directly from the iGoldMine executable. The Pocket PC Client can be installed on devices with or without .CAB file support.

To install the Pocket PC Client on devices with .CAB file support

1. Open a Web browser.
2. In the Address box, type http:// followed by the server name and iGoldMine logon page. For example, **http://server/logon.html**
3. Click the **Pocket PC Client** link.
4. Determine which version of Pocket PC is running on your device.
5. Download the appropriate .CAB file (Pocket PC 2003 or Windows Mobile 5 for Pocket PC).
6. Double-click the .CAB file.

You can manually install the Pocket PC Client by launching **iGoldMine.CAB** from the corresponding Pocket PC version on the client device. For example, Clients\CE\PocketPC5\iGoldMine.CAB

To install the Pocket PC Client on devices without .CAB file support

1. Locate the following files from the appropriate CPU folder in Clients\CE\CPU\Programs (for example, Clients\CE\PocketPC5\Programs*.*):
ggw.exe
clipc.dll
cs.dll
dc.dll
filec.dll
pbru.dll
sc.dll
scres.dll
sndc.dll
2. Copy these files to a common directory on the client device. (For example, copy Clients\CE\PocketPC5\Programs*. * to YourCEDevice\iGoldMine\.)
3. In the directory created in step 2, create a subdirectory named **kbd**. Copy any desired keyboard mapping file(s) from Clients\CE\kbd to this new directory. (For example, copy Clients\CE\X86\Programs\fr_FR.kbm to YourCEDevice\iGoldMine\kbd\.)

Running the Pocket PC Client from the Start Menu

Users can run the **Pocket PC Client** from the taskbar's Start menu.

To run iGoldMine from the Start menu

1. Click the **Start** button on the Windows taskbar.
2. Select **iGoldMine Client**.
3. Type your server address in the **Connection** dialog.
4. Select the desired screen size and click **Connect**.
5. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

Running the Pocket PC Client from the iGoldMine Executable

Users with pocket devices can run iGoldMine directly from the iGoldMine client executable.

To run the Pocket PC Client

1. Run **ggw.exe** on the client device.
2. Type the server address in the **Connection** dialog.
3. Select the desired **screen size** and click **Connect**.
4. When the **Logon** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.



Using the Pocket PC Client

The Pocket PC has several buttons and scrollbars based upon the screen size selected in the **Connection** dialog. If the screen size selected is larger than the actual screen of the Pocket PC device, horizontal and vertical scroll bars will appear on the right and bottom of the iGoldMine window. You can manually move these scroll bars to view different portions of the iGoldMine screen.

There are 5 pan buttons located at the bottom of the Pocket PC screen. These buttons allow you to quickly scroll to the four corners and center of the iGoldMine screen. There are also 4 zoom buttons located at the bottom of the device's screen. These buttons allow you to zoom-in, zoom-out, fit to screen, and view 100%.

Uninstalling the Pocket PC Client

To uninstall the **Pocket PC Client**, delete the installation files from the directory on the client device to which you copied them. These files include:

- ggw.exe
- clipc.dll
- cs.dll
- dc.dll
- filec.dll
- pbru.dll
- sc.dll
- scres.dll
- sndc.dll

Load Balancing

Load balancing allows iGoldMine sessions to be distributed across multiple application servers. Load balancing is required when the server resource requirements for a deployment exceed the capacity of a single server computer. Load balancing is done automatically and is transparent to the user. iGoldMine can also be used with any third party TCP/IP based load-balancing service.

Load Balancing Requirements

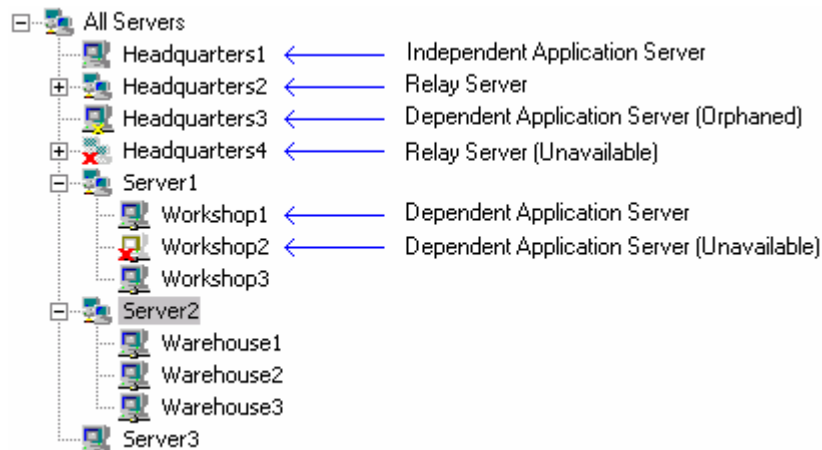
- A iGoldMine Server must be installed on each of the servers in the cluster.
- For Web deployment, each of the iGoldMine Servers in the cluster must have a Web server running and the Web server home directory should contain the iGoldMine Web files.
- If an application saves any user specific settings in the registry, (e.g., Corel WordPerfect, Microsoft Word, etc.) we strongly recommend that users operate with roaming profiles rather than local profiles. Since there is no way of predicting which server the user will actually be logged onto in a balanced server farm, working with roaming profiles is the only way to ensure that user specific settings are available to the user at all times.

A iGoldMine Server can be configured to operate as an independent application server, a relay server, or as a dependent application server.

Independent Application Servers

Independent application servers are iGoldMine Servers that do not interact with other iGoldMine Servers running on the network. Independent application servers appear in the Cluster Manager on the first level of the iGoldMine Servers tree view as an independent node. The iGoldMine setup program configures iGoldMine Servers to operate as independent application servers. iGoldMine clients can connect to independent application servers directly by specifying the name or IP address of the server in the **Connection** dialog or the location box of a Web browser. Clients can also connect to independent application servers through a third party network load balancer that distributes client connections among several servers. However, session reconnect is not supported in the latter configuration and must be disabled.

iGoldMine Servers

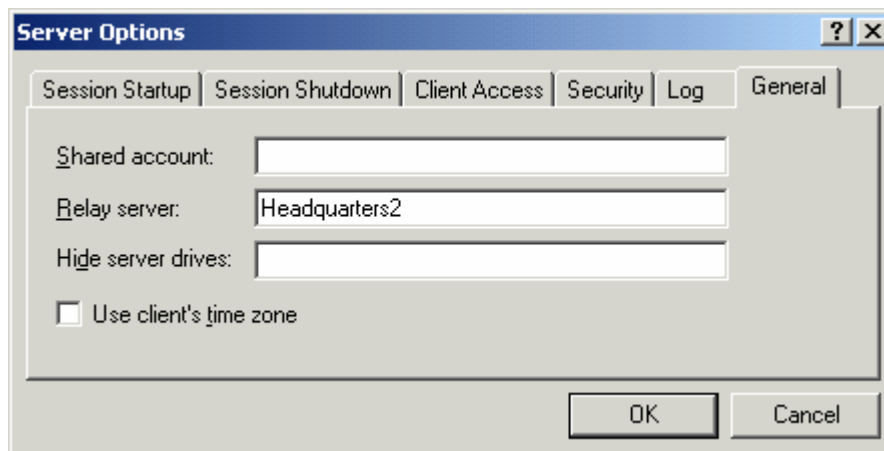


Relay Servers

A relay server is an iGoldMine Server that provides centralized control over one or more iGoldMine Servers. Relay servers maintain client connections and distribute iGoldMine sessions across a set of load-balanced application servers. Relay servers appear in the Cluster Manager on the first level of the list of **All Servers** as nodes with one or more dependent application servers.

To configure an iGoldMine Server to operate as a relay server

1. Select the desired server from the list of **All Servers**.
2. Click Tools | Server Options.
3. Click the **General** tab.
4. Type the name or IP address of the computer in the **Relay server** box.
5. Click **OK**.
6. A message box is displayed indicating that the change will not take effect until the **iGoldMine Application Publishing Service** on the relay server has been restarted. Click **OK**.
7. Stop and restart the **iGoldMine Application Publishing Service** from the Services option in the Control Panel.

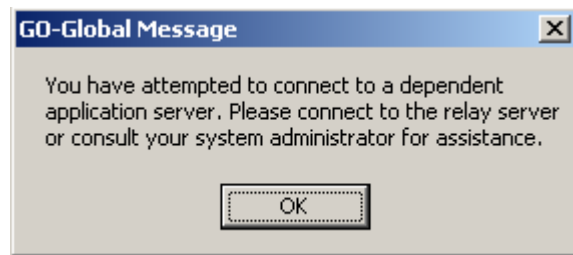


After configuring a server to run as a relay server with one or more dependent application servers, iGoldMine load-balances client connections and ensures that sessions start successfully. If a session fails to start on the selected server, the relay server selects another server and tries again until it finds one that can support the session.

Dependent Application Servers

A dependent application server is an iGoldMine Server that is connected to a relay server. iGoldMine clients cannot connect directly to dependent application servers. Instead, they connect to the associated relay server, and the relay server selects one of the connected servers to host the session.

If a user attempts to connect to a dependent application server, the following error message is displayed:



To configure an iGoldMine Server to operate as a dependent application server

1. Select the desired server from the list of **All Servers**.
2. Click Tools | Server Options.
3. Click the **General** tab.
4. Type the name or IP address of the relay server in **Relay server** edit box.
5. Click **OK**.
6. A message box is displayed indicating that the change will not take effect until the **Application Publishing Service** has been restarted. Click **OK**.
7. Stop and restart the **iGoldMine Application Publishing Service** from the Services option in the Control Panel.

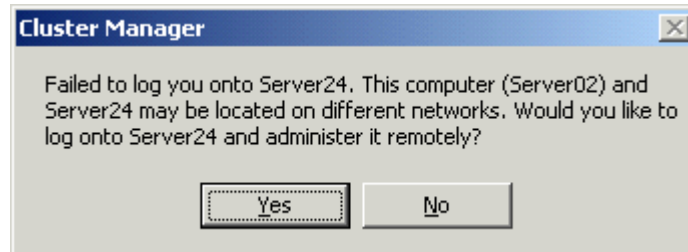
When the Application Publishing Service is restarted, the dependent application server will appear beneath the relay server in the Cluster Manager's list of iGoldMine Servers. A dependent application server with a yellow x indicates that the server has been "orphaned;" in other words, that its relay server has gone down. If a server's icon has a red x, the administrator does not have administrative rights on the server. If the server's icon has a red x and is grayed out, the server is no longer running the Application Publishing Service or it has been turned off. In either case, the administrator is unable to access that server from the Cluster Manager.

Users are authenticated on dependent application servers, not on relay servers. As a result, dependent application servers can be located on a different network than their associated relay server. For example, dependent application servers can be located behind a firewall on an internal, Active Directory network, and the associated relay server can be located in a demilitarized zone (DMZ) that is outside the firewall. If Integrated Windows authentication is used, clients and dependent application servers must be located on the same domain, but the relay server can be located on a different domain.

Note: We recommend installing the same set of applications on each dependent application server, using the same installation path on each server.

Administering Relay and Dependent Application Servers on Different Networks

When a user starts the Cluster Manager on a relay server or a dependent application server, the Cluster Manager connects to the relay server and attempts to authenticate the user using Integrated Windows authentication. If the Cluster Manager is running on a dependent application server and the associated relay server is located on a different network, a message such as the following is displayed:



Clicking **No** will return you to the **All Servers** node of the Cluster Manager. Clicking **Yes** will initiate a special remote administration session on the relay server as follows:

1. The Cluster Manager on the dependent application server starts the iGoldMine Client.
2. The client connects to the relay server and starts a session. The **Logon** dialog is displayed to the user.
3. The user logs on, specifying the user name and password of an account that is a member of the Administrators group on the relay server.
4. The Cluster Manager starts on the relay server. The user can now administer the relay server and all of its dependent application servers.
5. A maximum of two administration sessions can run on the relay server at any given time, regardless of the **Maximum sessions on this server** setting in the Cluster Manager and regardless of license restrictions.

Dependent application servers inherit their list of published applications, server settings, and user settings from the relay server. Applications *must* be installed in the same directory on all dependent application servers. Applications do not need to be installed on the relay server. When an iGoldMine Server is connected to a relay server all of its server settings are synchronized with those of the relay server. When any changes are made to the relay server's settings, they are also made to all servers connected to that relay server. The only settings that are allowed to vary are the maximum number of sessions, the printer driver sources, and the name of the relay server. All other settings in the **Server Options** and **Application Properties** dialogs are grayed out and cannot be modified.

When setting up a relay server, if an application is *installed* but not *published* on the dependent application server, you will need to publish the application on the relay server through the Cluster Manager. For example, if Adobe Reader 7.0 is installed on the dependent application server at C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe, open the Cluster Manager on the relay server and type this path location in the **Executable Path** box in the **Add Application** dialog.

Note: Before publishing an item on a mapped drive, verify that the drive is mapped to the same drive letter and location on the dependent application servers as it is on the relay server.

Client Printers in a Multi-Server Environment

In a multi-server environment, you can manage printer drivers from a central location by specifying a Driver server. The Driver server acts as a repository for all printer drivers that are available to iGoldMine clients. Printer drivers that are installed on the Driver server are replicated on each application server when a user requiring them logs on to iGoldMine.

When a user configures a printer with a driver that is not already available on the Driver server, that driver is replicated on the Driver server and is available to all application servers with access to that Driver server. If the Driver server and the relay server are the same machine, no additional setup is required. If they are separate machines, the Driver server must be accessible from the application servers. In this case, the Driver server needs to have a "print\$" share that points to the printer driver directory (WINNT\system32\spool\drivers). Users need read access to this share in order to install drivers from the Driver server. Users need write access to this share in order to install drivers to the Driver server.

Note: iGoldMine does not need to be installed on a Driver server.

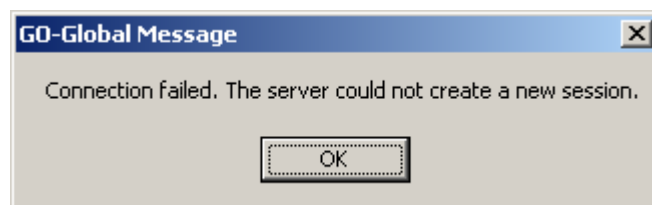
Server Selection

When a client connects to a relay server, the relay server attempts to start a session on the dependent application server that has the lowest number of running sessions as a percentage of the maximum number of sessions allowed for the server.

If the session fails to start on the selected server, the relay server successively attempts to start the session on other available servers until it finds a server that can support the session. If there are no available servers (i.e., if the number of running sessions on all servers equals the maximum number allowed), the following message is displayed to the user:



Otherwise, if the session cannot be started on any of the available servers, the following message is displayed to the user:



Relay Server Failure Recovery

On Windows Server 2003 and Windows XP Professional, the Application Publishing Service can be configured to automatically restart if the service fails. If a relay server fails, clients are disconnected but sessions continue to run on the iGoldMine Servers that were connected to the relay server. These servers will attempt to reconnect to the relay server every 15 seconds. When a dependent application server reconnects to the relay server, it re-adds its sessions to the relay server and restores any state information associated with the disconnected sessions. Clients are then able to log back on and resume their sessions. Clients do not automatically attempt to reconnect to the relay server.

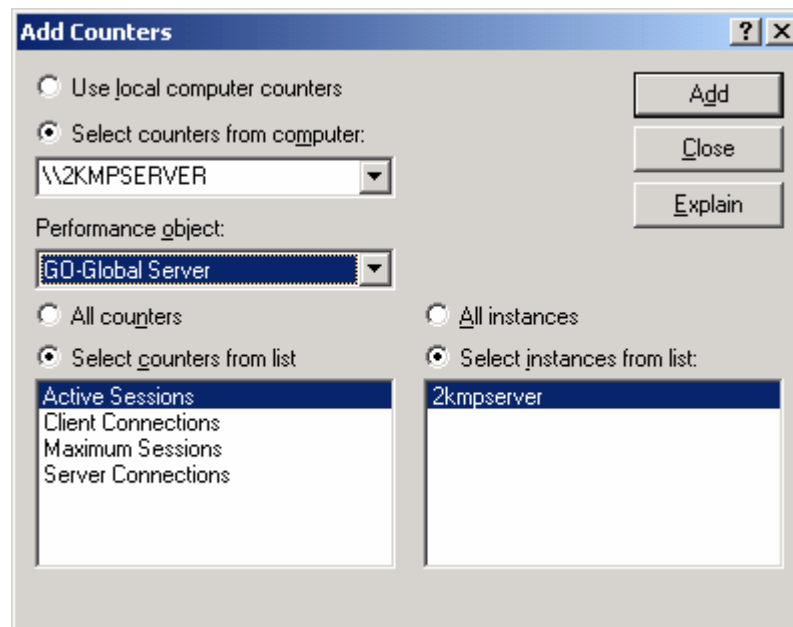
In order to provide higher service availability, a failover server can be configured for the iGoldMine relay server using the Microsoft Cluster Service. In this configuration, if the relay server fails for any reason, the failover server immediately takes the place of the failed server. Application servers automatically reconnect to the failover server, and users will generally be able to log on and reconnect to their disconnected sessions within 1-2 minutes of the relay server failure.

iGoldMine Server Performance Counters

iGoldMine Server performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a server. Performance counters can also be added to track the number of servers connected to a relay server and to identify the maximum number of sessions allowed on a server. iGoldMine Server performance counters allow administrators to monitor server activity from any machine with network access to an iGoldMine Server. The Remote Registry Service (Regsvc.exe) must be enabled for remote performance monitoring to work.

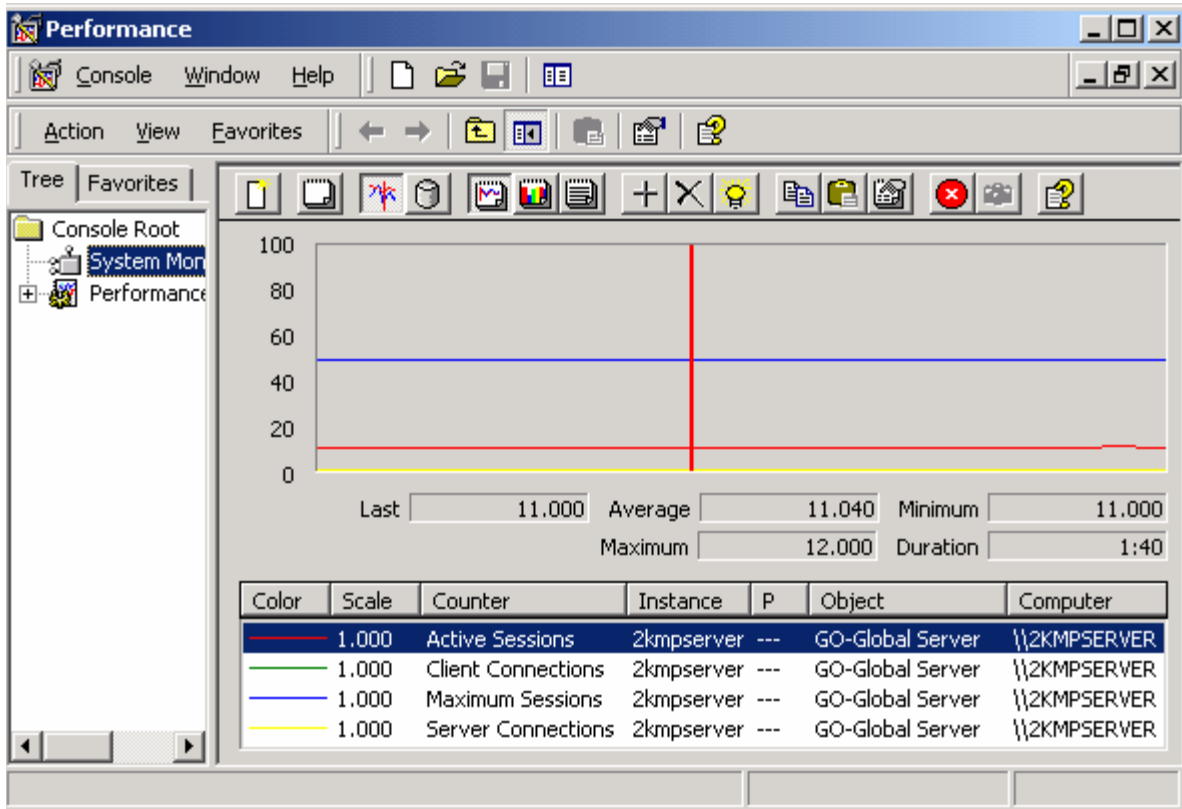
To add iGoldMine Server Performance Counters to the Performance Monitor

1. Click Start | Programs | Administrative Tools | Performance.
2. Click the **+** button to add counter(s).
3. From the **Object** field, locate and click **iGoldMine Server**.
4. From the **Counter** field, click the desired counters (Active Sessions, Client Connections, Maximum Sessions, Server Connections) and click **Add**.



iGoldMine Server Performance Counters include:

- **Client Connections.** The total number of client connections on independent application servers or relay servers. This value is always zero for dependent application servers.
- **Server Connections.** The total number of dependent application servers connected to a relay server. This value is always zero for independent or dependent application servers.
- **Active Sessions.** For independent or dependent application servers this is the number of sessions hosted on that server. For a relay server this is the total number of sessions hosted on all connected dependent application servers.
- **Maximum Sessions.** This displays the Maximum Session Count set in the Cluster Manager's **Server Options** dialog.

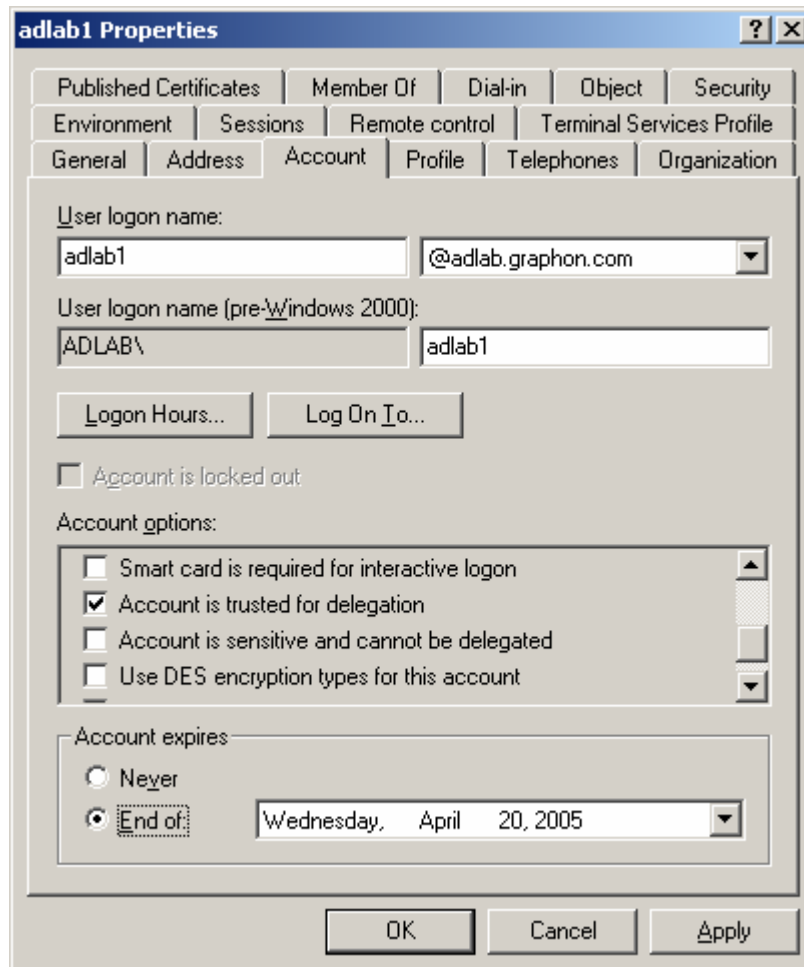


Configuration Requirements for Delegation Support

Server-side password caching, as described in Chapter 4, and network resource access require Windows delegation. The configuration requirements for delegation support are as follows:

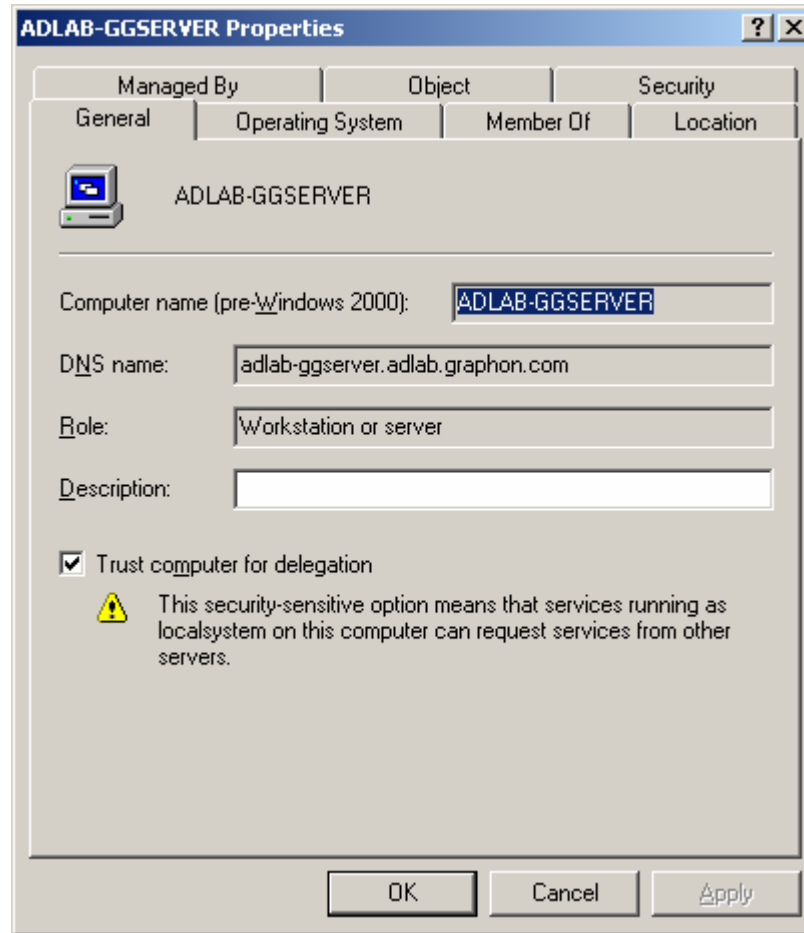
- Delegation requires the Kerberos authentication protocol and an Active Directory Domain, both of which were introduced with Windows 2000. As such, server-side password caching and accessing shared folders using Integrated Windows authentication are not supported from Windows NT 4.0 or Windows 98 client computers.
- The Domain Name System (DNS) servers must support Service Location (SRV) resource records. It is also recommended that DNS servers provide support for DNS dynamic updates. Without the DNS dynamic update protocol, administrators must manually configure the records created by domain controllers and stored by DNS servers. The DNS service provided with Windows 2000 or later supports both of these requirements.

- The computers hosting the iGoldMine client, the iGoldMine Server, and any backend services, such as email or a database, must support Kerberos. Kerberos is supported by systems running Windows 2000 or later in a Windows 2000 or later Active Directory domain. iGoldMine Server is only supported on Windows XP or later.
- The client's user account must support being delegated by the iGoldMine Application Publishing Service. In the **Active Directory Users and Computers** Management Console, select the user and click **Action | Properties**. Click the **Account** tab. In the Account options list box, scroll down and ensure the **Account is sensitive and cannot be delegated** option is disabled. Enable the **Account is trusted for delegation** option.



- The iGoldMine Server must have the right to delegate the user's account to other computers. In the **Active Directory Users and Computers** Management Console, select the computer and click **Action | Properties**. Enable **Trust computer for delegation**. The iGoldMine Application Publishing Service must be configured to run in the Local System account for these delegation rights to apply.

Note: After enabling **Trust Computer for delegation** in the Active Directory, the iGoldMine Server must be restarted in order for delegation to take effect.



- The **iGoldMine Application Publishing Service** must be able to register its Service Principle Name (SPN) with the Active Directory. It attempts to do this every time the service is restarted. The **setspn.exe** utility (available in the Microsoft Resource Kit and as a separate download from Microsoft) can be used to verify the SPN is properly set. The following Command Window shows output obtained from setspn.exe when run on the iGoldMine Server.

```

C:\WINNT\system32\cmd.exe

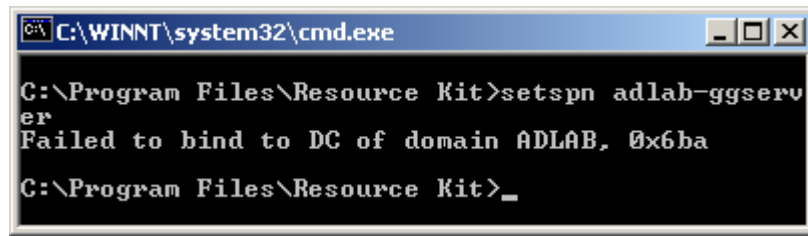
C:\Program Files\Resource Kit>setspn adlab-ggserver
Registered ServicePrincipalNames for CN=ADLAB-GGSERVER,CN=Computers,DC=adlab,DC=graphon,DC=com:
{54094C05-F977-4987-BFC9-E8B90E088973}/adlab-ggserver.adlab.graphon.com
HOST/ADLAB-GGSERVER
HOST/adlab-ggserver.adlab.graphon.com

C:\Program Files\Resource Kit>_

```

Replace adlab-ggserver with the computer name of your iGoldMine Server. The {54094C05-F977-4987-BFC9-E8B90E088973} Globally Unique Identifier (GUID) is specifically used by the iGoldMine Application Publishing Service to create the {54094C05-F977-4987-BFC9-E8B90E088973}/adlab-ggserver.adlab.graphon.com SPN.

The following Command Window shows output obtained by running **setspn.exe** on the iGoldMine Server and indicates a network configuration error. If all the above requirements are met this should not occur.



```

C:\WINNT\system32\cmd.exe

C:\Program Files\Resource Kit>setspn adlab-ggserver
Failed to bind to DC of domain ADLAB, 0x6ba

C:\Program Files\Resource Kit>_

```

Client Printing

iGoldMine supports client-side printing on all clients except the Pocket PC Client and the unsigned version of the Java Client. By default, iGoldMine automatically detects the client's default printer information once the user has logged on to the iGoldMine Server. This includes the default printer's port and printer driver. If the printer driver is not installed on the iGoldMine Server, iGoldMine will attempt to locate the driver and automatically install it. Due to a Java Virtual Machine limitation, users running the signed version of the Java Client will need to configure their printers manually using the Program Window's **Client Printer Wizard**.

Administrators are able to control which, if any, client printers are automatically detected at startup. The fewer printers that are initialized at startup, the quicker the Program Window will open. Printers not initialized at startup must be configured by the user through the Program Window's **Client Printer Wizard**.

Parameters can be used to indicate whether *all* printers, *no* printers, or *only the default* printer is automatically configured at startup. By default, iGoldMine automatically configures the user's default printer only. For the Microsoft ActiveX Control, Netscape Plug-in, and Browser Plug-in for Mac OS X, modify the HTML pages with the following values:

Value	Description
autoconfigprinters="all"	iGoldMine will attempt to automatically configure all client printers at startup.
autoconfigprinters="none"	iGoldMine will not attempt to automatically configure client printers at startup.
autoconfigprinters="default"	iGoldMine will only attempt to automatically configure the default printer at startup.

Examples:

Netscape Plug-in

```

<EMBED TYPE="application/x-ggw-plugin" width="1" height="1"
autoconfigprinters="all">
</EMBED>

```

Microsoft ActiveX Control

```

<OBJECT ID="Control1" WIDTH=0 HEIGHT=0
CLASSID="CLSID:76850F2A-FCAA-454F-82D3-BD46CB186EF5"
CODEBASE="ggw-activex.cab#Version=2,0,0,0" >
<PARAM NAME="autoconfigprinters" VALUE="all">
</OBJECT>

```

Browser Plug-in for Mac OS X

```
<EMBED TYPE="application/x-ggw-plugin" WIDTH="1000" height="630"
user="" password="" host="" application="" args="" isembeddedwin="true"
compression="true" hostport="" autoclosebrowser="false"
inbrowserprocess="true" autoconfigprinters="all">
</EMBED>
```

Note: Keep in mind that if you configure shortcuts or HTML pages that launch applications directly, the user will bypass the Program Window, and will be unable to add or modify client printers.

For the Windows Client, the Linux Client, and the Mac OS X Client, the argument **-ac** followed by the values **none**, **all**, and **default** can be added to the shortcut's command-line. For example, **ggw -ac all**

Regardless of which value is designated, users can still configure and print to any client printer by accessing the Program Window's **Client Printer Wizard**. Once a printer is configured through the Client Printer Wizard, it will be automatically configured at startup the next time the user logs on to iGoldMine. Users can prevent iGoldMine from automatically configuring a printer by accessing the Program Window's **Client Printer Properties** dialog and deleting the printer.

Printers that have been fully configured either at startup or via the Client Printer Wizard are listed in the Printers menu of the Program Window. A check mark appears next to the printer that has been designated as the default printer.

To view the list of client printers

From the Program Window, click File | Printers.

-or-

Right-click on the Program Window desktop and select Printers from the shortcut menu.

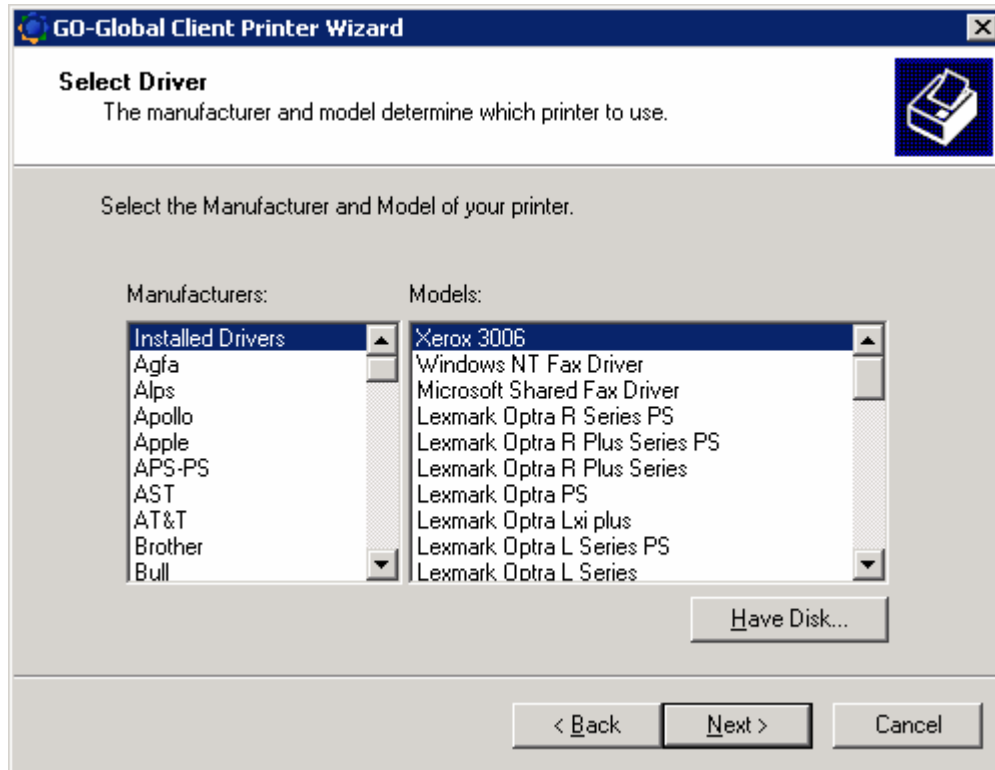
Note: The **Print Spooler** service must be running on the iGoldMine Server in order to configure client printers.

Configuring a Client Printer

If the iGoldMine Server is unable to locate the client printer driver, users can manually install a printer driver using the Program Window's **Client Printer Wizard**. The Client Printer Wizard displays a list of available printer drivers. The user selects the appropriate printer driver from the list. Administrators are able to install the driver from disk if Custom (Have Disk) is enabled on the Cluster Manager.

To configure a client printer

1. From the Program Window, click File | Printers | Configure Client Printer.
2. Click the name of the printer or type the name in the **Printer name** field.
3. Click the manufacturer and model of the printer. If available, administrators can click **Have Disk** if the printer came with an installation disk.
4. Click the check box next to the desired port. (If the port is known, the Client Printer Wizard will bypass this screen.)
5. Print a test page. (This step is optional, but recommended.)



Information entered through the **Client Printer Wizard** is stored in a printer configuration file (*print.ini* or *print.rc*) on the client computer and can be modified manually by the user. This file is used to perform client printer initialization for subsequent connections to iGoldMine Servers. The *print.ini* file is stored in the user's profile. For example, C:\Documents and Settings\username\Local Settings\Application Data. On clients running Windows 98, the file is stored in the user's TEMP path, in the directory that the environment variable %TEMP% points to. For example, C:\Windows\temp.

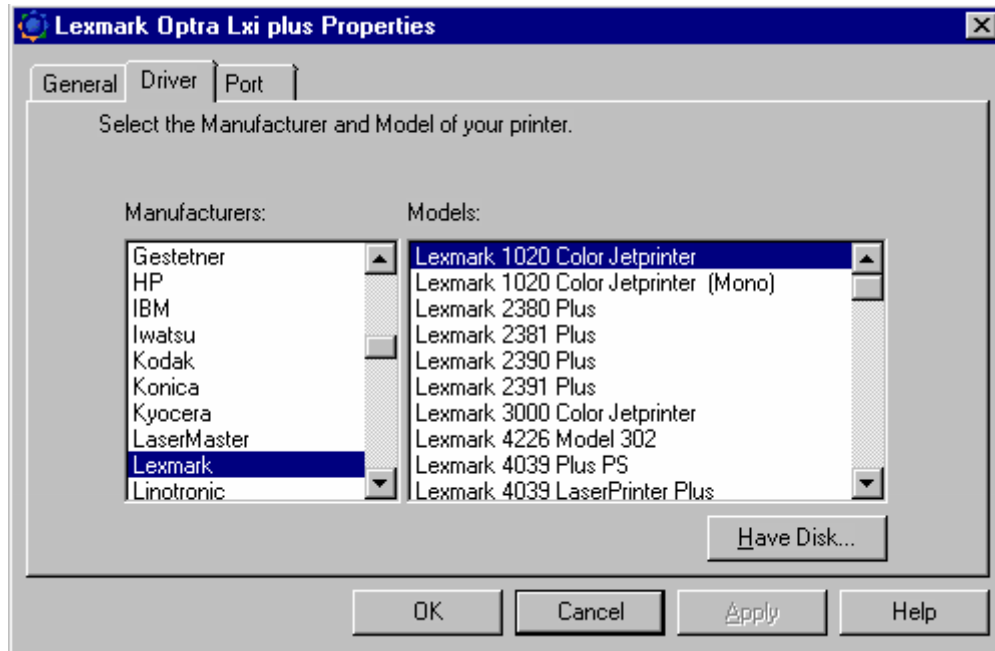
Once a printer has been successfully configured, users can modify the printer's properties by accessing the **Client Printer Properties** dialog. Through the Properties dialog, users can select the port for the client printer, select their default printer, delete a printer, or print a test page. By clicking the **Preferences** button, users can select the paper orientation, the page order, and the paper source.

Note: Setting the default printer via the Program Window will modify the default printer on the client.

Once all client-side printers have been properly configured, the Client Printer Wizard is no longer available. Users can edit the printers' properties, but they cannot configure a new printer. Any additional printers must first be installed on the client machine before they can be configured to run through iGoldMine.

To access the Client Printer Properties dialog

1. From the Program Window, click File| Printers.
2. Select the desired printer.



Users can print to TCP/IP-based printers by typing the printer's IP address in the port edit box of the Client Printer Wizard or the Properties dialog—for example, 192.168.100.21. Additionally, a specific port can also be added in the port edit box—for example, 192.168.100.21:9100. If no TCP/IP port is defined, the default of 9100 is used.

Enabling Support for Client Printers

Client-side printing is disabled by default. Administrators enable client-side printing through the Cluster Manager's **Server Options** dialog.

To enable support for client printers

1. In the Cluster Manager, select the desired server from the list of **All Servers**.
2. Click Tools | Server Options.
3. Click the **Client Access** tab.
4. Click the **Printers** check box.
5. Click **OK**.

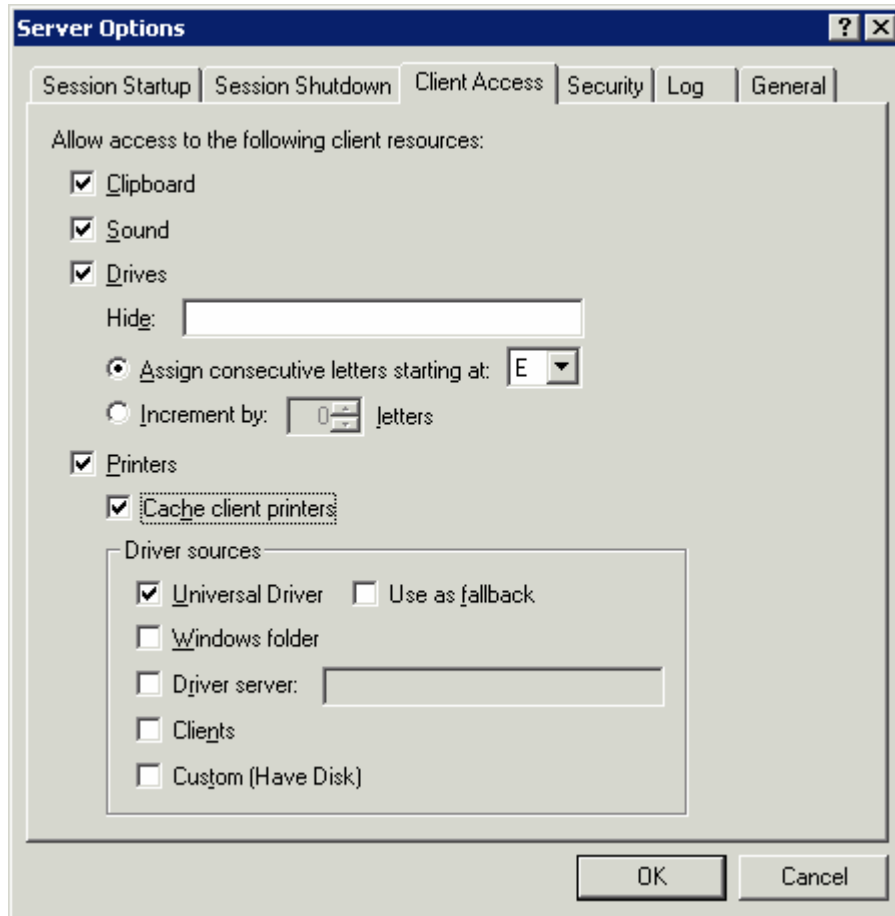
Enabling Client Printer Caching

When client printing is enabled, iGoldMine creates printers on the iGoldMine Server that act as proxies for the client's printers. If **Cache client printers** is enabled, proxy printers are not deleted when sessions close, but remain on the server. When a user starts a new session from the same client computer, iGoldMine synchronizes the list of client's printers with the proxy printers on the server. If there have been no printer additions or deletions on the client computer since the last time an iGoldMine connection was made, no printer changes are required on the server.

Enabling **Cache client printers** prevents the deletion of client printers when a session closes and provides faster session initialization for subsequent sessions started from the same client machine.

To enable client printer caching

1. In the Cluster Manager, select the desired server from the list of **All Servers**.
2. Click Tools | Server Options.
3. Click the **Client Access** tab.
4. Click the **Printers** check box.
5. Click the **Cache client printers** box.
6. Click **OK**.



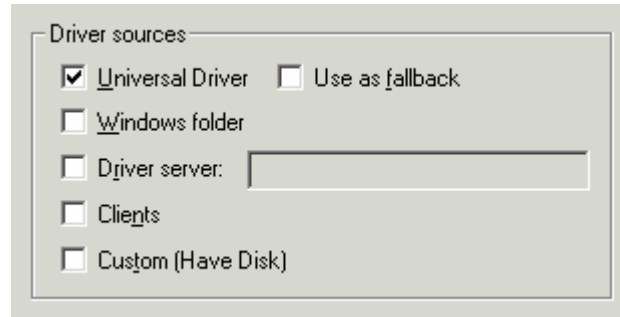
Designating Access to Printer Drivers

iGoldMine can obtain printer drivers from the following sources:

- **Universal Driver:** iGoldMine includes a Universal Printer Driver that can print to any client computer with a Portable Document Format (PDF) viewer (e.g., Adobe Reader) installed. Enable the **Universal Driver** option to designate the Universal Printer Driver as the printer driver for all client printers. Users running the Windows CE Client can only use the Universal Driver in order to print to client printers.
- **Use as fallback:** Enable the **Use as fallback option** to designate the Universal Printer Driver as backup printer driver for all client printers.
- **Windows folder:** The **Windows folder** contains printer drivers that are distributed with Microsoft Windows. Enable the **Windows folder** option to permit specification of this folder and browse for the location of the operating system's driver files (i386 directory).
- **Driver server:** The **Driver server** option allows administrator to create a repository of printer drivers that is accessible to all servers. Enable the **Driver server** option to permit specification of the name or IP address of the server used to store printer drivers. If the

Driver server is a computer other than the relay server, users must minimally have read access to the print share (system32\spool\drivers) on the Driver server. If a user is a Power User, any drivers that are uploaded from the client will also be installed on the Driver server so that they will be available to all servers in the cluster. If the Driver server is a relay server, all users will automatically have both read and write access to the Driver server.

- **Clients:** Enabling the **Clients** option allows users to upload drivers from their client machine. The client machine must be running the same operating system as the iGoldMine Server.
- **Custom (Have Disk):** Allows administrators to install a printer driver with the **Have Disk** button.



The Universal Printer Driver can print to any client computer with a PDF viewer (e.g., Adobe Acrobat) installed, and is available to the following iGoldMine clients: Windows Client, Linux Client, ActiveX Control, Netscape Plug-in, and Mac OS X Client. Users running the Windows CE Client can only use the Universal Driver in order to print to client printers.

If **Universal Driver** is enabled without the **Use as Fallback** option enabled, iGoldMine will use the Universal Printer Driver as long as a PDF viewer is installed on the client computer. iGoldMine will not use the Universal Printer Driver in this scenario if the client printer has already been configured to use a different printer driver.

If both **Universal Driver** and **Use as Fallback** options are enabled, iGoldMine will give priority to the standard drivers and will only use the Universal Printer Driver when a standard driver is not available.

In order to use the Universal Printer Driver with the Linux Client, the locate database must be updated after installing Adobe Reader. The Linux Client uses the locate program to find the path to Adobe Reader. To do this, issue the command **updatedb** or **locate -u** in a terminal window. Alternatively, the path to Adobe Reader can be added to the user's PATH environment variable.

To automatically configure all client printers so that users are not required to perform any printer configuration tasks, select **Universal Driver** as the driver source in the **Server Options** dialog, add **-ac all** to the command-line, and verify that Adobe Reader is installed on the client computer.

Notes:

Most printers will be auto-configured when **Universal Driver** and **Windows Folder** are enabled in the Cluster Manager. In this case, printers will be configured using the Universal Printer Driver unless the native printer driver is already installed on the server. This is the recommended setting for most installations. The **Use as Fallback** option can be enabled to allow other driver sources to take precedence over the Universal Driver.

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

Administrators set access to printer driver sources through the **Server Options** dialog.

To designate access to printer drivers

1. In the Cluster Manager, select the desired server from the list of All Servers.
2. Click Tools | Server Options.
3. Click the **Client Access** tab.
4. Click the **Printers** check box.
5. Click the box beside the desired driver source or sources.
6. If enabling the Driver server, type the name or IP address of the driver server in the driver server box.
7. Click **OK**.

Notes:

iGoldMine supports USB printers in all clients, except the Java Client.

Client printers are temporarily installed on the iGoldMine Server 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 iGoldMine Server.

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

iGoldMine installs a printer on the server 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 using iGoldMine. Since multiple users connect to an iGoldMine Server, 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 MAC address	001122334455
%C	The client machine name	HRWorkstation
%S	The server machine name	Server1

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:
[SOFTWARE\GraphOn\Bridges\1.0.0\ 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 -%U@%C by default. Using the above examples, printer names would appear as: PrinterName-Wilson@HRWorkstation

Note that the hyphen (-) and the at sign (@) 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.

The client computer's MAC address will be used to construct a unique identifier for each client printer. This identifier is stored in an .ini file in the iGoldMine Programs directory and will be associated with the printer's custom name. In cases where two separate sessions are assigned the same client printer string, the second session will be named using this unique identifier (e.g., PrinterName-MAC_Address) in place of the custom printer name.

Note: If the **Cache client printers** option is enabled on an iGoldMine Server that has upgraded to the newest version of iGoldMine, previously configured client printers might remain installed on the server. These printers can be deleted with no consequence to the user.

Client Sounds

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

To enable support for client sound

1. In the Cluster Manager, select the desired server from the list of **All Servers**.
2. Click Tools | Server Options.
3. Click the **Client Access** tab.
4. Click the **Sound** check box.
5. Click **OK**.

Note: waveOut is not supported on Linux or Mac OS X.

Clipboard Support

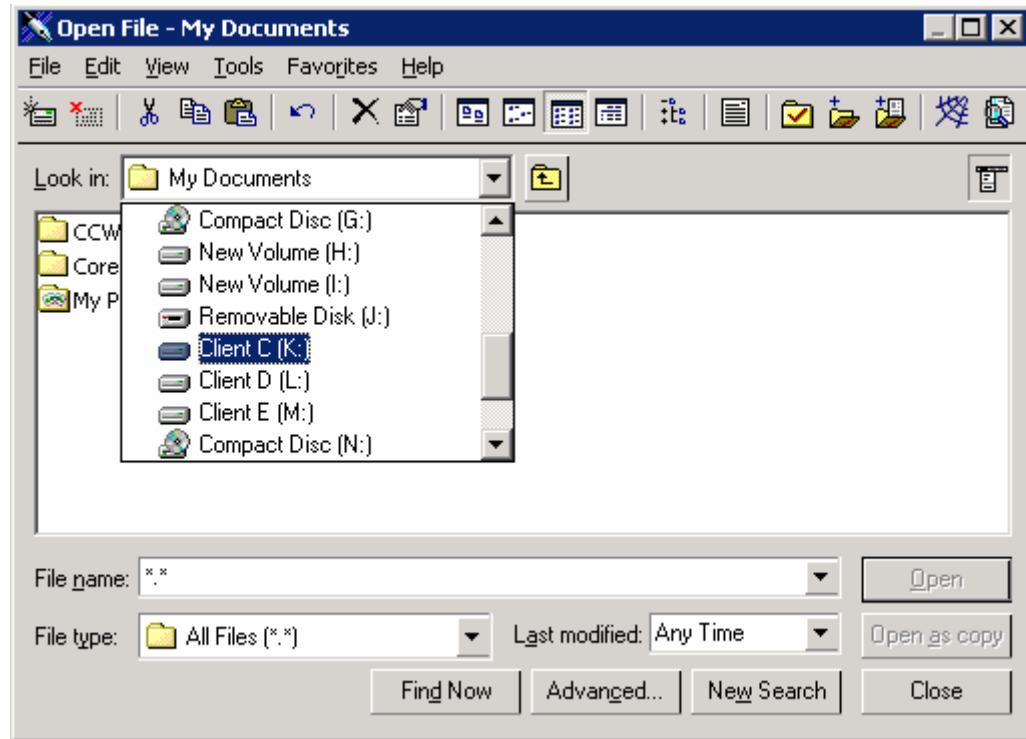
iGoldMine allows client and server-based applications to exchange information using the clipboard. Users can cut and copy information from applications running on the client and paste it into applications running on an iGoldMine Server, and vice versa. Clipboard support is disabled by default.

To enable clipboard support

1. In the Cluster Manager, select the desired server from the list of **All Servers**.
2. Click Tools | Server Options.
3. Click the **Client Access** tab.
4. Click the **Clipboard** check box.
5. Click **OK**.

Client File Access

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



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

To enable support for client drives

1. In the Cluster Manager, select the desired server from the list of **All Servers**.
2. Click Tools | Server Options.
3. Click the **Client Access** tab.
4. Click the **Drives** check box.
5. Click **OK**.

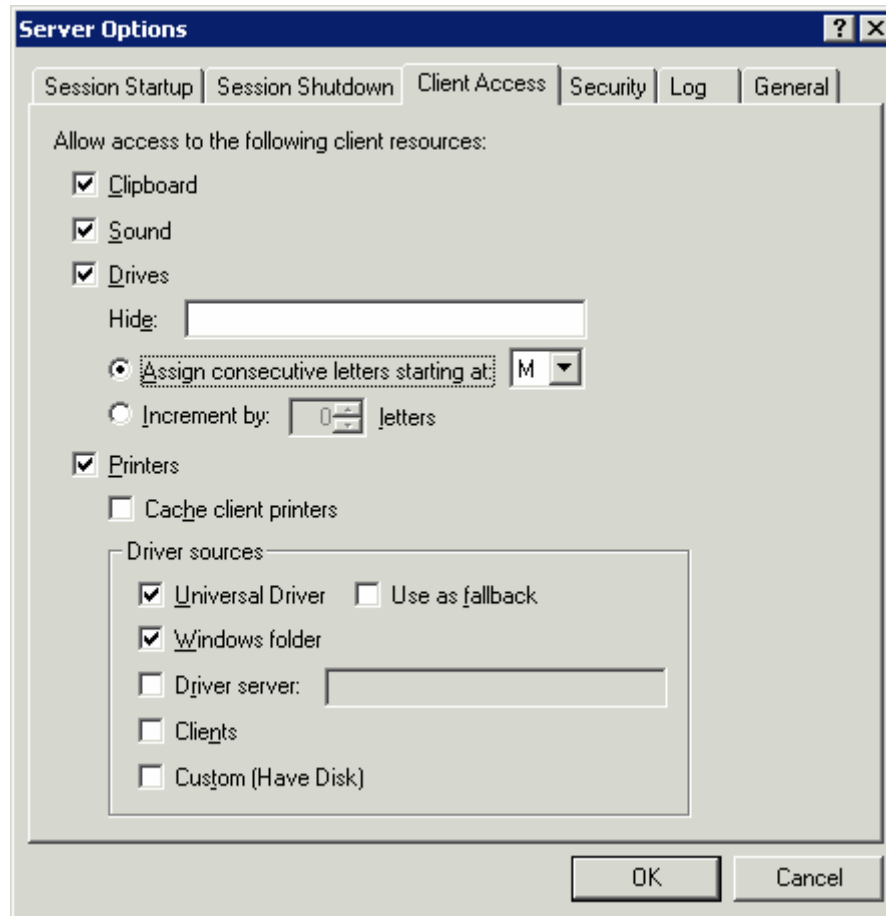
Remapping Client Drives

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

To list client drives sequentially starting at a given drive letter

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

For example, if a client computer has 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. From the Cluster Manager, click Tools | Server Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. Click **Increment by: ___ letters**.
5. In the edit field, type a number greater than or equal to 1 that will yield the desired offset.
6. Click **OK**.

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.

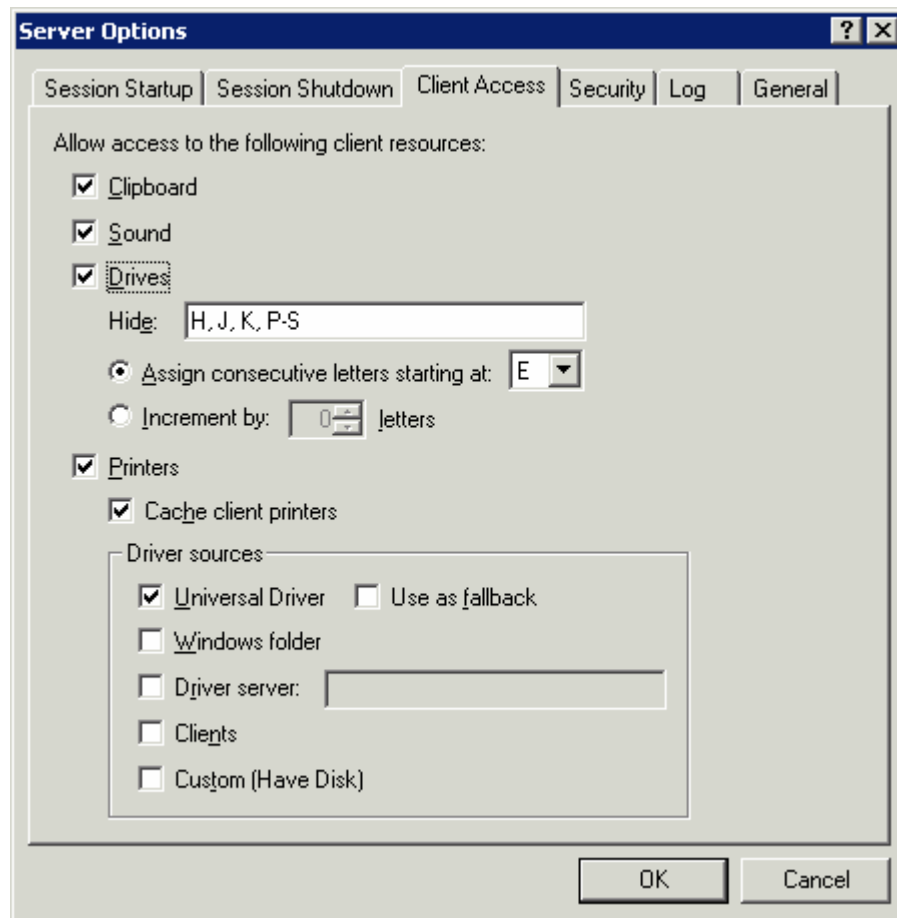
Hiding Client Drives

Through the Cluster Manager, administrators can hide client drives such as the client's operating system drive, floppy drive, and CD ROM drive, making them inaccessible to the user through iGoldMine.

To hide one or more client drives

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

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



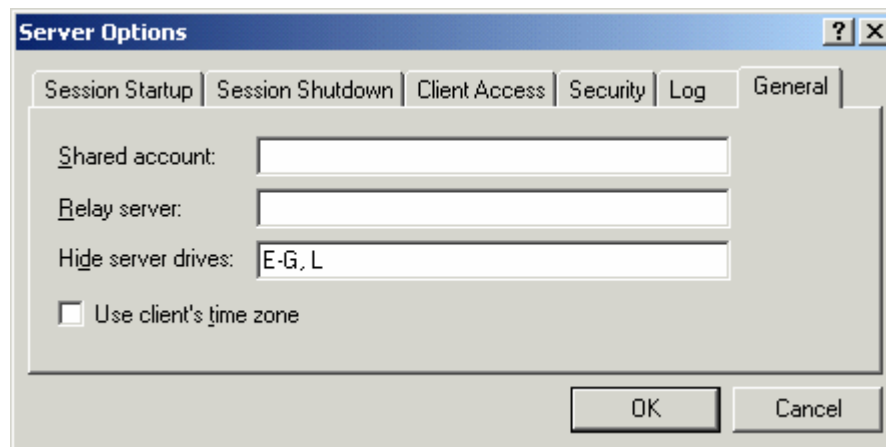
Hiding Server Drives

Through the Cluster Manager, administrators can hide one or more server drives so that they are not listed as local drives on the client computer, and therefore not accessible to users.

To hide one or more server drives

1. From the Cluster Manager, click Tools | Server Options.
2. Click the **General** tab.
3. In the **Hide server drives** box, type the server drive letters you want to hide.
4. Click **OK**.

All server drives are mapped by default. Drives listed in the **Hide server drives** box can be listed in any order. You cannot hide the server drive on which Windows is installed (C, in most cases) or the server drive on which iGoldMine is installed. You cannot hide drives referenced by applications installed on the iGoldMine Server. For example, drives referenced in the application's registry settings or the application's initialization file cannot be hidden.



Mapped Drives

Drive mappings are private within each iGoldMine session Windows Server 2003. For example, if there are two sessions running on an iGoldMine Server, a drive letter (H, for example) can be mapped to one network share in session 1 (e.g., \\servername\session1), and the same drive letter can be mapped to a different network share in session 2 (e.g., \\servername\session2).

Define drive letter mappings using logon scripts. You can also allow users to define their own drive letter mappings by publishing applications that provide this functionality.

Drive mappings defined within the interactive session on the iGoldMine Server are not available to remote users. If all users require access to the same network share through a drive mapping, the drive mapping will generally need to be defined in a logon script.

Obtaining the Name of the Client Computer

For applications that require the client's computer name rather than the iGoldMine Server's, administrators can add the name of that executable under the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\Bridges\1.0.0\Compatibility\GetComputerName** as a DWORD with a data value of **0x00000001**. Any time an executable matching any of the names listed under this registry key with a data value of **0x00000001** calls the Windows **GetComputerName** API, the given buffer will be filled in with the client's name rather than the server's.

Additionally, there is an environment variable named **CLIENTCOMPUTERNAME** that exists as part of the running environment of a published application. This environment variable contains the client's computer name. The standard Windows environment variable **COMPUTERNAME** remains unchanged; its value is the server's computer name.

To obtain the name of the client computer

1. Run the Registry Editor (regedit.exe).
2. From the Registry Editor, expand the **HKEY_LOCAL_MACHINE** key.
3. Locate the **GetComputerName** key:
[SOFTWARE\GraphOn\Bridges\1.0.0\Compatibility\GetComputerName]
4. Create a **DWORD** entry for the executable. (For example, pw.exe).
5. Set the value of the new entry to **0x00000001**.
6. Close the Registry Editor.

Application Script Support

Many Win32 applications were designed for installation on a client PC and run by only one user. When an application is deployed from an iGoldMine Server, multiple users need to be able to run the application simultaneously, and a number of problems may be encountered if the application is not "multi-user ready."

The best way to solve multi-user deployment problems with an application is to modify the application so it properly supports multiple users as specified in the *iGoldMine for Windows Developer Guide*. When it is not possible to modify the application, an application script may be used to perform the pre-launch configuration and post-shutdown cleanup that is required to allow the application to run in a multi-user environment. The process for creating and deploying an application script is as follows:

1. Write a batch file that:
 - Performs the tasks necessary to prepare the application environment for a user.
 - Launches the application.
 - Performs any cleanup tasks required after the application shuts down. The batch file should end with an EXIT command. Otherwise the CMD.EXE process will not shut down.
2. Publish the application script
 - a. Open the Cluster Manager.
 - b. Click Tools | Applications | Add.
 - c. Type the path to CMD.EXE in the **Application Path** field.
 - d. In the **Command Line Options** field, specify "/K filename", where filename is the full path of the batch file to be run.
 - e. Type the application display name and specify an icon.
 - f. Click **OK**.
3. Test the application script
 - a. Launch one of the iGoldMine clients and connect to the iGoldMine Server.
 - b. Double-click the icon for the application script. The user interface of the application should appear on the client display, and the application should be running in the environment configured by the application script.

Note: When an application script is launched using iGoldMine, the CMD.EXE window is not displayed. As such, the application script cannot contain any prompts for user input.

Process Loader Options

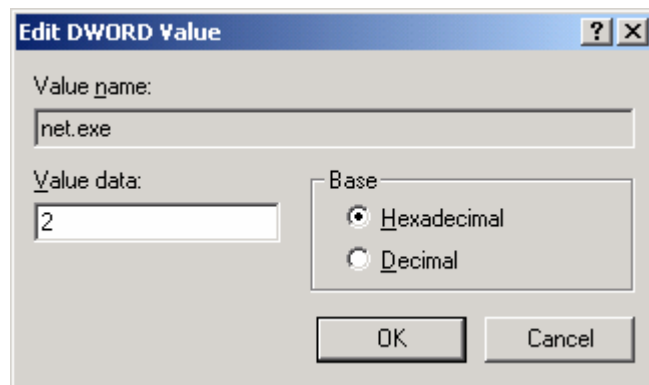
All applications that run within iGoldMine sessions are redirected and initialized for display on the client computer. The time required to perform these operations is generally a small percentage of the time required to launch typical Windows applications, but it can be a large percentage of the time 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. iGoldMine's **Process Loader** options allow administrators to bypass redirection of a process. Applications execute faster since the client access components are not loaded and initialized.

To bypass redirection of a process

1. Click Start | Run | Regedit.
2. Browse to the registry key
\\HKLM\GraphOn\Bridges\1.0.0\Loader\Processes.
3. Click Edit | New | DWORD value.
4. Type the name of the executable file that should not be redirected. The name of the DWORD entry should be the file name of the particular application. It may be specified as either a fully qualified path or as the file's base name and extension.
5. Select the new registry value and click Edit | Modify. Type one of the following values:
 - **0:** Specify this option to disable redirection of non-GUI processes in order to allow them to start faster. With this option specified, sounds are not redirected to the client and access to client files, printers, and COM/LPT ports is disabled. Applications may not display properly with this setting, so this option should only be used for processes that do not display a graphical user interface.
 - **2:** Specify this option to disable the client sound, file, printer, and COM/LPT port features for the process. Applications will paint properly with this setting. This option may be used for processes that display a graphical user interface.
 - **3:** Specify this option to enable the default behavior.

Note: Any other value besides 0, 2, or 3 is unsupported and may cause applications to fail.

6. Click **OK**.



Proxy Tunneling

Proxy tunneling via the **HTTP CONNECT** method allows a user who accesses the Internet via a proxy server to connect to iGoldMine Servers on the Internet when the following conditions are met:

- The user runs the native Windows Client, ActiveX Control, or Netscape Plug-in for Windows;
- The address and port of the proxy server are stored under the client computer's Internet Options; and
- The proxy server is configured to allow HTTP CONNECT method tunnels to the port on which the iGoldMine Server is configured to accept RapidX Protocol (RXP) connections.

Proxy Tunneling via the HTTP CONNECT Method

When the Windows Client, ActiveX Control, or Netscape Plug-in for Windows are unable to establish a direct connection to an iGoldMine Server, and when the client computer is configured through its Internet Options to use a proxy server, the client attempts to establish an HTTP CONNECT method tunnel to the iGoldMine Server.

Specifically, the client:

1. Connects to the proxy server using the address and port specified in the client computer's **Internet Options**.
2. Sends a CONNECT request to the proxy server: i.e., `CONNECT address:port HTTP/1.0`, where *address* and *port* are respectively the IP address of the iGoldMine Server and the port on which the server accepts RXP connections (e.g., 491 by default).
3. Reads the reply from the proxy server.
4. Responds to the proxy server's reply as follows:
 - a. If Basic authentication is required, iGoldMine prompts users for their user name and password and then repeats Step 2, this time providing the user's credentials.
 - b. If the request failed, iGoldMine displays the following message:
"Failed to connect to serverAddress via the proxy server at proxyAddress : [reason for failure]."
 - c. If the request succeeded, iGoldMine initializes the RXP connection and starts the session.

To allow HTTP CONNECT method tunnels using port 443

1. Configure the iGoldMine Server to accept connections on port 443.
2. Specify port 443 in the Web pages that will be used to access the server.
3. If necessary, configure the proxy server to allow connections to the iGoldMine Server on ports 80 (HTTP) and 443 (HTTPS).

Once you have configured the iGoldMine Server and its Web pages, users that meet the three requirements above will be able to connect to the server. Users running the Windows Client will need to append the `-hp` argument, followed by 443, to the command-line. For example, `"..\ggw.exe" -h server -hp 443`. Otherwise, these users will be unable to log on to iGoldMine.

Note: iGoldMine clients are unable to connect to iGoldMine Servers via proxy servers that are configured to verify that the traffic on port 443 is HTTPS.

Enabling Support for PAE

On Windows Server 2003 and Windows XP Professional, iGoldMine supports memory in excess of 4 GB by way of the Physical Addressing Extension (PAE).

To enable PAE

1. Click Start | Run.
2. Type **C:\boot.ini**, where X is the drive letter of the location of the boot files, tldr, Boot.ini, and so forth.
3. Modify the line that corresponds to your operating system by appending the switch **/PAE**.
4. Save the file, and restart the computer.

Automatic Windows Update and Hotfix Compatibility

iGoldMine supports High Priority Windows Updates, Windows Hotfixes, and Windows Service Packs. GraphOn tests iGoldMine for compatibility with High Priority Windows Updates and Windows Service Packs. Certification testing begins as soon as the High Priority Windows Update or Service Pack is released and is usually completed within one day. The results of these tests are e-mailed to customers and posted at <http://www.graphon.com/support/updates.shtml>

If GraphOn certifies that the Windows Update or Service Pack is compatible with the currently released version of iGoldMine, Updates or Service Packs can safely be installed on iGoldMine Servers. If testing shows an incompatibility, customers will receive email notification when a compatibility update is available.

Microsoft does not release Windows Hotfixes from its Microsoft Update site and typically only provides Hotfixes to customers on an as-needed basis. Since Hotfixes are not universally available, GraphOn does not run compatibility tests on Windows Hotfixes.

iGoldMine 3.2 is expected to be compatible with nearly all future Windows Updates and Hotfixes. Windows Service Packs, however, contain more significant changes and may not be compatible with iGoldMine. If a Windows Update, Hotfix, or Service Pack is incompatible with iGoldMine, the Application Publishing Service will record an error in its log file and close. If this occurs, contact Customer Support. GraphOn will typically provide support for incompatible updates within one week.

GraphOn recommends that users install only Windows Updates and Service Packs on iGoldMine Servers that have been certified to be compatible with iGoldMine. As such, GraphOn recommends that iGoldMine Servers be configured so they do not automatically install Windows Updates.

To disable the automatic installation of Windows Updates

1. Click Start | Control Panel.
2. Click Automatic Updates.
3. In the **Automatic Updates** dialog, click one of the following options:
 - **Download updates for me, but let me choose when to install them.**
 - **Notify me but don't automatically download or install them.**
 - **Turn off Automatic Updates.**
4. Click **OK**.

Log Files

The iGoldMine Server creates log files in which it records information about its own performance and that of certain iGoldMine processes. GraphOn Technical Support uses the data to diagnose and correct problems that may arise. This can be especially helpful for errors that are only reproducible on specific machines or with a specific application.

All log files, whether they pertain to the client or server machine, are located in the **Log** folder on the iGoldMine Server. For example, D:\Program Files\GraphOn\iGoldMine Server\Log. In the Log folder are three subfolders: **Backup**, **Codes**, and **Templates**. Be careful not to delete these folders. iGoldMine 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_2007-04-04_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 iGoldMine 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.

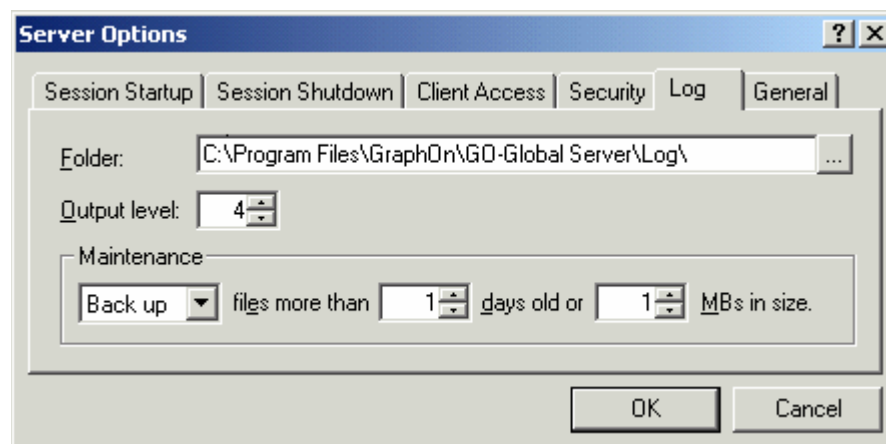
Selecting a New Location for the Log Files

By default, log files are created and stored at \Program Files\GraphOn\iGoldMine Server\Log. You can select a new location for the log files through the Cluster Manager's **Server Options** dialog.

To select a new location for the Log files

1. From the Cluster Manager, click Tools | Server Options.
2. Click **Log**.
3. Type the path to the new directory in the **Folder** edit box or browse to its location.

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

iGoldMine offers six log output levels, as follows:

- 0: No output
- 1: Errors
- 2: Errors and Events
- 3: Errors, Events, and Warnings
- 4: Errors, Events, Warnings, and Diagnostic Messages
- 5, 6: Errors, Events, Warnings, Diagnostic Messages, and Trace Messages

To set the output level

1. From the Cluster Manager, click Tools | Server Options.
2. Click **Log**.
3. Type one of the above numeric values in the **Output level** box.
4. Click **OK**.

CAUTION!

Setting the log output value to 5 or 6 will cause the server 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 iGoldMine Server.

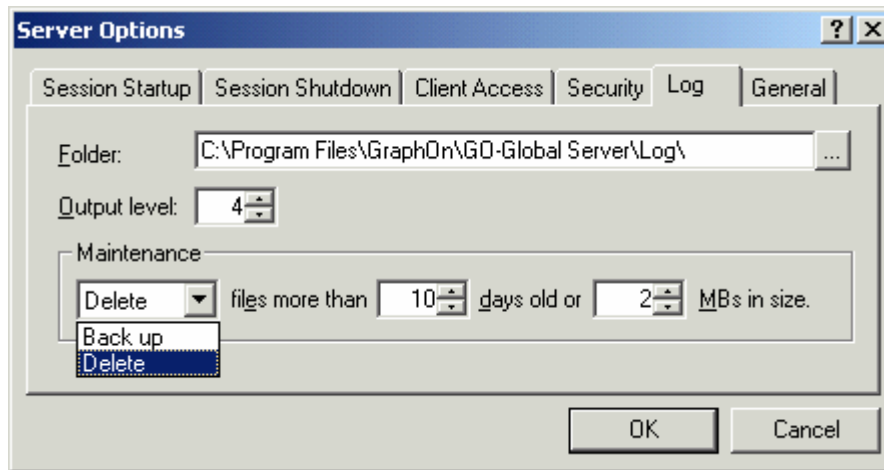
The default value for the Output level is 1.

Maintaining Log Files

iGoldMine 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, iGoldMine lets you delete or backup log files and set file size or age limits.

To delete log files

1. From the Cluster Manager, click Tools | Server Options.
2. Click **Log**.
3. Under **Maintenance**, select **Delete**.
4. Specify how old (in days) log files can become before being deleted.
5. Specify at what size (in megabytes) log files are to be deleted.
6. Click **OK**.
7. Restart the **iGoldMine Application Publishing Service**.



To backup log files

1. From the Cluster Manager, click Tools | Server Options.
2. Click **Log**.
3. Under **Maintenance**, select **Back up**.
4. Specify how old (in days) log files can become before being moved to the Backup subdirectory of the Log folder.
5. Specify at what size (in megabytes) log files are to be moved to the Backup subdirectory of the Log folder.
6. Click **OK**.
7. Restart the **iGoldMine Application Publishing Service**.

Once every half hour, and each time it is started, the Application Publishing Service searches the **Log** folder for files that have reached the specified age or size limit. It then either deletes the files or moves them to the **Backup** subdirectory of the Log folder. If while sweeping the log files, the Application Publishing Service finds that the age or size limit has been met in the current log file, it closes the file and installs a newly created file in its place.

By default, log files are backed up after 7 days or when the file size has reached 20 MB.

Serial and Parallel Port Redirection

iGoldMine supports serial and parallel port redirection when the application accesses the serial or parallel port directly, i.e., if the application calls the Win32 ReadFile and WriteFile APIs to respectively read from and write to the device. Client **Drives** must be enabled on the iGoldMine Server in order for calls to be redirected to the client.

When iGoldMine detects that an application has successfully accessed a serial or parallel port, a message is recorded in the Log file (at Output Level 4 and above). For example:

Wilson on Server4, cs (1208) An application has attempted to connect to a client device on LPT1.

Note: Serial port printers are not enumerated in the Program Window's printer list.

INDEX

&

";, 65, 74

A

-a, 45, 68, 70, 71, 76
-ac, 45, 68, 70, 71, 91
Active Directory, 3, 38, 83, 89
Active Directory Domain, 87
Active Directory Domain Controller, 38
Active Sessions, 87
ActiveX Control, 4, 58, 59, 65, 90
Adobe Reader, 94, 95
All Servers, 22, 48, 93, 94, 96, 97
Always in front, 50
Application Publishing Service, 6, 20, 22, 36, 82, 83, 86, 106, 107, 108
Application Script Support, 102
Application Users/Groups, 25
Applications, 46
 adding, 23, 24
 duplicating, 25
 editing properties, 25
 installing, 23
 removing, 27
 renaming, 26
aps, 106
ARGS, 62, 64, 65, 73
Audio support, 97
Authentication, 38
autoclosebrowser, 64, 66, 73
autoconfigprinters, 64, 66, 73, 90

B

Backup, 108
Backup folder, 106
Basic authentication, 104
Broadcast Interval, 48
Browser Logons, 7
Browser Plug-in, 73
Browser Plug-in for Mac OS X, 5

C

-c, 68, 70, 71, 76
CA, 34
CA certificate, 31, 32
CA key, 31, 32
ca.cfg, 32
ca.crt, 33, 34
Cache client printers, 93, 97
Cache passwords, 39
Cached password, 40
Central license server, 7, 10
Certificate Authority, 29
Certificate Signing Request, 29, 32, 33, 34
Certificate Wizard, 34
Change Icon, 24, 25
Change Password, 43
Client clipboard, 97
Client Connections, 87
Client drive letters, 99
Client drives, 98, 100
Client file access, 2, 98
Client keyboards, 11
Client printer name, 96
Client Printer Naming, 96
Client Printer Properties dialog, 91
Client Printer Wizard, 1, 90, 91, 92
Client printers, 64, 66, 73
Client printing, 1, 68, 70, 71, 90
Client sounds, 1, 97
Client-side password caching, 39
Clipboard support, 97
Cluster Manager, 22, 24, 26, 44, 81, 84
 accessing, 22
 accessing from a client machine, 56
 refreshing, 47
cm.exe, 56
Codes, 106
COM/LPT ports, 103
Command-line arguments, 45, 68, 70, 71, 76
Command-line options, 24, 25, 26
Common Name, 29, 32, 34
Compression, 62, 64, 65, 68, 70, 71, 73, 76
Connected Clients, 28, 46
Connection dialog, 37, 68, 76, 81
Consecutive letters, 98
Copy and paste, 97
CPU, 48
CPU requirements, 4

CPU utilization, 48
Cross-platform compatibility, 1

D

Default printer, 96
Delegation, 38, 88
Delegation Support, 87
Demilitarized zone, 3, 83
demo license, 6
Dependent application server, 81, 83, 84, 85
DES encryption, 35
Desktopcolor, 62
Diagnostic Messages, 107
Disconnect, 44
Disconnecting a session, 44
Display name, 24, 68, 70, 71, 76
DNS servers, 87
Domain Controller Security Policy, 20
Domain name, 20
Domain Name System, 87
Domain Security Policy, 20
DPAPI, 39
Drive Letter Mapping, 2
Drive letters, 98
Drive mappings, 101
Driver server, 85, 94

E

Embedded windows, 59, 63
embeddedactivexlogon.html, 60
embeddedlinuxpluginlogon.html, 60
embeddedwindowspluginlogon.html, 60
Encryption, 35
Encryption algorithm, 35
Errors, 107
Events, 107
Executable Path, 24, 25

F

-f, 70, 71
failover server, 86
Failure recovery, 86
fallback, 35
Fallback layout text, 17
FAT file system, 23, 26
File Permissions, 21
Firewall, 3, 36, 83

G

geometry, 70, 72
GGII, 14
ggw.exe, 76, 79
ggw.rpm, 63, 69
Global logon script, 51
Global scripts, 50
iGoldMine Application Publishing Service, 6, 48, 88, 89, 106
iGoldMine Client, 68, 76
iGoldMine Clients, 58
iGoldMine Input Identifiers, 14

iGoldMine License Manager, 10
iGoldMine Server, 7, 20, 21, 27, 44, 59, 102, 107
iGoldMine Server Performance Counters, 87
iGoldMine shortcut, 68
iGoldMine.dmg, 71, 72
iGoldMine.pkg, 72
Grace period, 55
Group Policy, 49
Group Policy Support, 2

H

-h, 68, 70, 71, 76
Have Disk, 95
Hiding client drives, 100
Hiding server drives, 101
Host Port, 36, 37
hostport, 36
HTTP, 104
HTTP CONNECT method, 104
HTTPS, 104

I

i386 directory, 94
Idle limit, 54
Idle time, 54
IME, 11, 17
Inactivity Timeout, 2
inbrowserprocess, 64, 66
Increment, 99
Independent application server, 81
Input Method Editors, 11
Installing the iGoldMine Server, 6
installnativelinux.html, 60
installnativemacx.html, 60
installnativewindows.html, 60
Integrated Windows authentication, 38, 44, 83, 84, 87
Integrated Windows Authentication, 43
INTERACTIVE group, 37, 38, 39
Internet Explorer, 63
Internet Options, 31, 104
IP address, 46, 93
isembeddedwin, 64, 66, 73

J

Java Client, 5, 60, 61
Signed, 61, 90
Startup parameters, 61
Unsigned, 61
javalogonsigned.html, 60
javalogonunsigned.html, 60

K

-kb, 14
Kerberos authentication protocol, 87
Keyboard layout, 14, 17
Keyboard Mapping Files, 15

L

- Launch Parameters, 26
- Layout text, 16
- Layout text substitutions, 16
- License Retrieval Wizard, 6, 7
- License server, 10
- License-file list, 8
- License-file list redundancy, 9
- Linux Client, 4, 37, 69, 96
- Linux Clients, 59
- Live collaboration, 27
- LM_LICENSE_FILE, 8
- LM_LICENSE_FILE, 9, 10
- Imtools, 9
- Load balancing, 2
- Local logon rights, 20
- Local Security Policy, 20
- Locality, 29
- Locality Name, 32, 33
- Log Files, 106, 107
- Log folder, 107, 108
- Logon dialog, 68, 69, 76
- Logon Manager, 50
- logon scripts, 101
- Logon scripts, 50
- logon.html, 7, 60
- Loose windows, 59, 63
- looseactivexlogon.html, 60
- looselinuxpluginlogon.html, 60
- loosewindowspluginlogon.html, 60
- LPT ports, 103

M

- Mac OS X, 72
- Mac OS X Client, 4, 71
- Mac X11 Client, 58, 59
- Maintenance, 107
- Mapped drive, 25
- Mapped drives, 101
- Maximum number of sessions, 53, 86
- Maximum Sessions, 87
- Maximum sessions count, 53
- MEM, 48
- Mem usage, 48
- Memory, 105
- Memory requirements, 4
- Messages, 106
- Microsoft ActiveX Control, 4, 58, 59, 65, 96
- Microsoft Cluster Service, 86
- Microsoft Management Console, 34
- Modifying the Host Port Setting, 36
- Multi-server environment, 21
- Multi-user deployment, 23, 102

N

- Native Linux Client, 69
- Native Windows Client, 59, 67
- Netscape Plug-in, 4, 59, 63, 90, 96
- Netscape Plug-in for Linux, 63
- Netscape Plug-in for Windows, 63
- netscapeplugininstaller.html, 60
- NETWORK group, 38

- Network Printer, 21
- network share, 101
- New Password, 42
- NTFS, 21, 23, 26

O

- ODBC data sources, 24
- OpenSSL toolkit, 29, 31
- Options dialog, 57
- Organization Name, 32, 33
- Organizational Unit, 29
- Organizational Unit Name, 32, 33
- Output Level, 107, 108

P

- p, 68, 70, 71, 76, 90
- PAE, 105
- Pan buttons, 80
- Parallel port, 108
- Password Caching, 39
- Password Change, 41, 43
- Passwords, 69, 70, 71, 77
- PEM format, 34
- Performance counters, 2, 86
- Performance problems, 52
- Physical Addressing Extension, 105
- Physical memory, 53
- Platform Builder, 77
- PlaySound, 1, 97
- Plug-in, 63
- Pocket PC Client, 78
- Port, 36, 37, 93
- Print Spooler service, 91
- print.ini, 92
- print.rc, 92
- Printer drivers, 90, 96
- PrinterNameFormat, 96
- Process
 - ending, 27
- Process ID, 47, 106
- Process information, 47
- Process Loader Options, 103
- Processes, 48
- Procs, 48
- Product Code, 6
- Program Window, 25, 26, 44, 90, 91
- Progress message, 49
- Proxy printer names, 96
- Proxy printers, 93
- Proxy server, 104
- Proxy tunneling, 2
- Proxy Tunneling, 104

R

- r, 45, 68, 70, 71, 76
- RapidX Protocol, 104
- Red x, 22, 83
- Redundant license servers, 8
- Refresh rate, 47
- Relay server, 81, 82, 83, 84, 85, 86
- Remapping client drives, 98

Remote Registry Service, 86
Resource limits, 49, 52
Roaming user profiles, 21, 81
RSA private key, 32

S

Secure Socket Layer, 29
Security, 20, 35
Security Alert, 35
Serial port, 108
Server, 6, 20
Server activity, 46
Server Connections, 87
Server drives, 101
Server keys, 33
Server monitoring, 2
Server Options dialog, 44, 93
Server Performance Counters, 87
server.cfg, 33
server.crt, 31, 34
server.key, 31, 34
Server-side password caching, 39, 87
Service Principle Name, 89
Session
 encrypting, 35
 terminating, 27
Session information, 46
Session limit, 53
Session Name, 46
Session reconnect, 2, 44, 81
Session shadowing, 2, 27
Session Startup, 51
Session termination, 44
Session timeout, 44
Sessions, 48
Sessions tab, 44
setup.exe, 6
Shadowing a session, 27
Shared account, 45, 46
Shortcuts, 68
Signed Java Client, 60
sndPlaySound, 1, 97
Sound card, 97
Spaces, 69, 70, 71, 77
Speakers, 97
SSL, 29
SSL Certificate, 29, 30, 31, 34, 35
SSL Security, 2
SSL transport, 35
Standard authentication, 37, 38
Start Directory, 24, 25, 26
Start menu, 67, 75
Startup parameters, 61, 64, 65, 68, 70, 71, 73, 76
Startup State, 24, 25, 26
Startup Time, 46
Status bar, 48, 57
System requirements, 4

T

TCP, 29
TCP/IP, 4, 81
TCP/IP printing, 93
Templates, 106
Terminal Connection Manager, 78
Trace Messages, 107
Transmission Control Protocol, 29
True Color, 61

U

-u, 68, 70, 71, 76
UNC, 25
Universal Driver, 94
Universal Printer Driver, 2, 94
Unsigned Java Client, 60
User, 46
User Accounts, 20
User Profiles, 21
User roaming, 2
User-specific scripts, 50

V

Virtual memory, 53

W

Warning period, 55
Warnings, 107
waveOut, 1, 97
WBT CE Image, 77
WBT Device, 77
Web access, 59
Web files, 7, 81
Web proxy server, 104
Web server, 7
Windows Based Terminal, 77
Windows CE Client, 4, 58, 59, 76
Windows Client, 4, 59, 67, 68, 76, 96
Windows Explorer, 21
Windows folder, 94
Windows Mobile, 59, 78
Windows Performance Monitor, 86
Windows shortcut, 68, 76

Y

Yellow x, 83

Z

Zoom buttons, 80

