

*IBM Global Sign-On for Multiplatforms, Version 2.0
Installation and Server Management Guide*

GC32-0284-00

July 7, 1998



IBM Global Sign-On for Multiplatforms, Version 2.0

Installation and Server Management Guide



IBM Global Sign-On for Multiplatforms, Version 2.0

Installation and Server Management Guide

Note

Before using this information and the product it supports, be sure to read the general information under "Appendix E. Notices" on page 159.

First Edition (July 1998)

This edition applies to version 2.0 of IBM Global Sign-On for Multiplatforms and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 1997, 1998. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

About this Book	vii
Prerequisite and Related Documents	vii
Conventions	vii
Chapter 1. Overview and Planning	1
GSO Concepts	2
GSO Cells and Managed Resources	3
GSO Components	4
Supported Platforms	5
GSO Requirements	6
Hardware Requirements	6
Software Requirements	7
Special Considerations.	8
Chapter 2. Installing GSO from the Desktop	15
Installing the TME 10 GSO User Administration on the TMR Server and Managed Nodes	17
Installing GSO Plus on the TMR Server, TEC Server, and Managed Nodes	18
Installing from the Command Line	19
Starting a Tivoli/Plus Module	20
Tivoli/Plus Icons	23
Chapter 3. Software Distribution for GSO	25
Configuring TME 10 Software Distribution File Packages	25
File Packages for the GSO Server	26
File Packages for the GSO Client	28
File Packages for the GSO Database Server	30
File Packages for the GSO Database Client.	32
Installing GSO Servers and Clients.	34
Removing GSO Software	35
Chapter 4. Configuration Tasks for GSO	37
Time Synchronization Issues	37
Configure GSO Master Server	37
Configure GSO Replica Server	38
Configure GSO Database Server	39
Configure GSO Clients.	40
Creating GSO Users and Targets	42
Chapter 5. Management Tasks for GSO	43
Start Server	43
Stop Server	43
Backup Cell	44
Restore Cell	45
Remove Machine From Cell	46
Set Password Policy	47

Reset Password	48
Synchronize Replicas	49
Move Master Server	50
Recover Replica	52
Enable Integrated Login	53
Disable Integrated Login	53
Enable Litronic Smart Card	53
Disable Litronic Smart Card	54
Enable Event Adapter	54
Disable Event Adapter	55
Chapter 6. Resource Monitoring	57
Using GSO Plus Monitors	57
Viewing the Status of Monitored Resources	58
Monitored Resources	59
GSO Monitor Probes	60
GSO Server Monitors Monitoring Profile	63
GSO Database Server Monitors Monitoring Profile	70
GSO UNIX Monitors Monitoring Profile	76
GSO Automated Actions	76
Chapter 7. Enterprise Event Management.	81
Configuration Activity	81
Setting Up the Tivoli Enterprise Console	82
Creating a New Rule Base	83
Adding to an Existing Rule Base	83
Configure the GSO Event Adapter	84
Events and Rules	85
GSO Server Monitor Events and Rules	85
GSO DCE Serviceability Events and Rules	91
Summary of GSO Monitor Event Classes	93
SVC Event Class	93
Unconfigure GSO Event Adapter	94
Appendix A. Installing Smart Card Administration.	95
Appendix B. Installing the Client Machine Without Software Distribution	97
Installing the GSO Client 2.0 on Windows NT/95	97
Installing the GSO Client 1.5 on OS/2 Warp	98
Configuring the GSO Client 2.0 on Windows NT/95	99
cfgclient -config	100
cfgclient -login	101
cfgclient -logindev	102
cfgclient -view	103
cfgclient -? -h	104
DCE for OS/2 Warp Client Information	105
Online Information	105
Printable Documentation	105

Appendix C. GSO Database-Specific Configuration	107
Configuring ODBC	107
Configuring ODBC on AIX and Solaris Servers	108
Configuring ODBC on Windows NT Servers	117
Implementing Server Security	118
Configuring a Client Data Source	122
ODBC Server Configuration Parameters	122
Resolving ODBC Issues and Known Problems	125
Supported ODBC Functions	125
Configuring OCI	125
Configuring OCI on AIX and Solaris Servers	126
Configuring OCI on Windows NT Servers	130
Implementing Server Security	132
Configuring a Client Data Source	134
OCI Server Configuration Parameters	136
Resolving Oracle Issues and Known Problems	139
Configuring CT-LIB	139
Setting CT-LIB Environment Variables on AIX and Solaris Servers	139
Associating a Sybase SQL Server with a CT-LIB Server	140
Setting Server Configuration Parameters	140
Creating a Special Sybase Database Account	143
Implementing Server Security	144
Configuring a Client Data Source	146
CT-LIB Server Configuration Parameters	148
Resolving CT-LIB Issues and Known Problems	151
Supported CT-LIB Functions	152
Appendix D. Product Packages on the GSO CDs	155
Server Packages	155
Client Packages	156
GSO Information	157
Printed Information	157
Online Information	157
Readme Files	157
GSO Code Page Compatibility	158
Appendix E. Notices	159
Trademarks	160
Index	163

About this Book

Welcome to IBM Global Sign-On (TM) for Multiplatforms, Version 2.0 (hereinafter called GSO). This book *Installation and Server Management Guide* describes the installation process and includes procedures for using the GSO Tivoli/Plus module. This guide is intended for system administrators who use GSO to manage their enterprise operations. A working knowledge of the TME 10 environment is important in understanding the functionality of this GSO Plus module. Readers of this guide should also be familiar with the operating systems running on their machines.

Prerequisite and Related Documents

The following books are part of the GSO product and are provided online on each GSO client. You can access each book through the **Start** menu on the taskbar.

- *Global Sign-On Administration Help*
- *Global Sign-On Command Reference*
- *Global Sign-On Programmer's Guide*

The *IBM Global Sign-On User Administration Guide* is provided in printed format.

The information in this book, *Installation and Server Management Guide*, complements information presented in the following:

- *TME 10 Framework Platform User's Guide*
- *TME 10 Framework Planning and Installation Guide*
- *TME 10 Framework Reference Manual*
- *TME 10 Software Distribution User's Guide*
- *TME 10 Software Distribution Reference Manual*
- *TME 10 Distributed Monitoring User's Guide*
- *TME 10 Enterprise Console User's Guide*

Conventions

Knowing the conventions used in this book will help you use it more efficiently.

Boldface type

Indicates the name of an item you select, the name of a command, and the name of a field you fill in.

Italics type

Indicates new terms, book titles, and variable information that must be replaced by an actual value.

Monospace type

Indicates an example, text you type, and text that is displayed on the screen.

Chapter 1. Overview and Planning

IBM Global Sign-On for Multiplatforms, Version 2.0 (hereinafter called GSO) provides enhancements to Version 1.5 and is integrated with the Tivoli Management Environment 10 (TME 10) Framework to provide:

- Automated installation and maintenance of GSO using Tivoli Software Distribution.
- Tivoli tasks and jobs available for configuring GSO environment.
- Management of GSO users and targets from one centralized console.
- Role-based administration of GSO users and logon targets using Tivoli User Administration.
- Notification of logon attempts, password resets, and other GSO events using Tivoli Event Management.

GSO provides a secure, single point of entry to computing resources that not only enables organizations to connect disparate networked systems but also results in significant benefits, such as:

Increased security

GSO supports the use of password, or smart card authentication to confirm authorized users.

Easier administration

GSO makes it easier for users to set up and manage their passwords and IDs.

Increased productivity

GSO reduces the time required to complete logons and to manage users and the overall system.

GSO strengthens existing security by preventing security exposures; such as, having multiple passwords and IDs that users must memorize, maintaining multiple passwords, having trivialized passwords (simple words that are easy to decode). GSO provides the capability to coordinate multiple user IDs and passwords securely in heterogeneous environments so that users can access files, applications, printers and databases (that they are authorized to use) anywhere in the enterprise. GSO provides a highly secure solution for users that allows seamless access to the resources they need, no matter where the resources are located.

GSO integrates with existing operating systems and is consistent with (and across) the leading operating system platforms for truly global sign-on capabilities. It is easily extended to allow maximum flexibility for adding new applications and minimizes the programming effort needed to support them. GSO supports login access to 3270 mainframe applications, AS/400 applications, LAN Server, OS/2 Warp Server, Novell NetWare, Windows NT Server, Lotus Notes, and databases.

By using GSO's location-independent logon, a user can work from any machine equipped with GSO. When a GSO user logs in to the local operating system, GSO authenticates the user to the authentication server. Successful authentication triggers

the retrieval of user information, such as target systems and applications, that the user is authorized to use. These user resources are then displayed in the GSO graphical user interface (GUI).

When the user selects the target systems or applications to be used, application-specific identification and authentication information is securely retrieved from the GSO server. Logon proceeds automatically and asynchronously using the application-specific mechanisms. GSO provides logon status information throughout the logon process.

GSO Concepts

The following provides a brief overview of GSO concepts.

- GSO securely coordinates password and passticket access to multiple systems and applications, called *targets*. The information that describes GSO users and their targets to GSO, such as user IDs, passwords, hosts, and domains, is stored on a GSO server and is administered through TME 10 User Administration.
- GSO uses encryption services to encrypt passwords before they are transmitted between the GSO client and the GSO server.
- In GSO, the communication applications used to connect from the client computer to the user's targets are called *programs*. For example, the Novell NetWare program connects the client machine to a Novell NetWare server. Programs and the information that describes these programs to GSO are stored on the individual client machines and are administered through GSO administration.
- *Program template files* contain the information that defines a specific program's interfaces and behavior to GSO. Stored in each GSO client, are a set of program template files for each supported platform. To create your own program template file, follow the instructions in the *Global Sign-On Programmer's Guide*.
- Because the user's information is stored on the GSO server, GSO users can gain access to their authorized targets from any GSO client machine. This is called *free seating*. Free seating can happen as long as the appropriate program and program-related information is installed and configured on the GSO client machine.
- GSO protects access to target and program configuration information by implementing various levels of authority among users and administrators. This allows administrators to maintain GSO security features, such as *passticket* capability, while providing GSO users with an uncomplicated user interface.
- Passtickets are an alternative to transmitting passwords across the network. A passticket is based on information understood only by GSO and is typically used in resource access control facility (RACF) host systems (TSO or VM). Passtickets provide greater security because they are used once in place of an actual password and then discarded.
- A GSO cell is a collection of clients and servers from your enterprise which are configured to share common GSO resources. The servers consist of a GSO master server and possibly one or more GSO replica servers and GSO database servers. One or more GSO cells can be managed within a single Tivoli Management Region (TMR). A GSO client is configured into a single GSO cell.

- The GSO database support provides a secure single sign-on connection between your client application and the database server. GSO connects the client database application to the database without the need for entering individual user information. GSO can also be configured to securely transmit the data sent between the client and server through the use of GSO's encryption capabilities.

GSO users do not need to work with the Tivoli desktop. Users use GSO to log on and off targets, browse the GSO log, change their passwords, and update their own target user preferences. However, GSO users cannot create new targets.

Administrators will use the Tivoli desktop to manage all of the administrative processes associated with GSO. When managing GSO user accounts there are two security roles in TME that are relevant to GSO. These types are **admin** and **senior admin**. These roles are used to protect access to target configuration information and maintain GSO security features, such as passticket capability.

The **admin** role can create users, edit users, delete users, create targets and manage target-related information for other users. The **admin** role can also authorize access to GSO and GSO targets, but may require Windows NT client administration authority to configure the programs installed on a client machine.

The **senior** role can do everything that the **admin** role can do and in addition they can manage passticket information, and manage target groups.

GSO Cells and Managed Resources

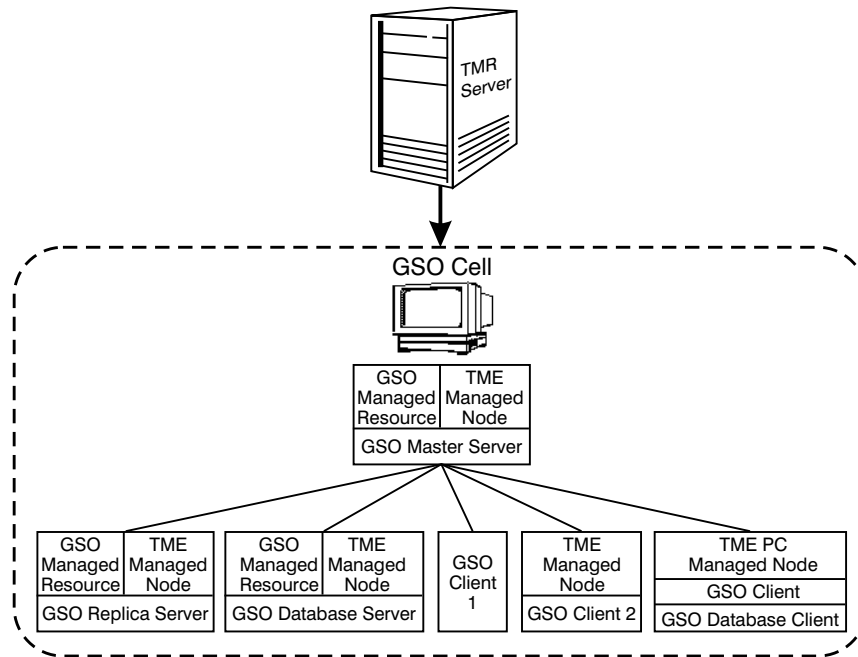
The ME 10 Framework provides the ability to subdivide an enterprise network into multiple TMRs. You can now manage the GSO cell as a managed resource type under TME 10. Managed resources are objects that administrators work with in a policy region, such as managed nodes and profiles. Some examples of TME 10 resources are workstations, software, administrators, and GSO cells.

You manage resources using rules called *policies*. For many environments, policies are a set of conventions that may or may not always be followed. A policy region is a collection of managed resource types governed by a common set of policies. A policy region is often created to represent a management domain or area of influence for one or more system administrators. A policy region is a Tivoli feature that lets you model the management and organization of your specific environment. It can be thought of as a special collection of resources that share common policies.

If an administrator has been assigned access to a user (the user resides in the administrator's policy region), the administrator has access to all of the user's data, not just the GSO data. For example, the administrator can access the user's UNIX, Windows NT, NetWare, or RACF data.

In TME 10, a managed node represents a workstation (or a particular port on a workstation). When a workstation is a managed node, you can use TME 10 to manage the resources on that system. In the following example, you have a GSO cell that is

installed on a TME managed node.



When you are managing user accounts from a TME 10 user profile, the user account changes are not reflected on the system until you distribute the user profile. In the case of GSO user accounts, the changes are not made until you distribute the user account information to the GSO cell.

For general information about configuring TMRs, see *TME 10 Framework Planning and Installation Guide*.

GSO Components

When you install GSO you install the following components:

- TME 10 GSO User Administration
- Tivoli/Plus GSO module
- One or more GSO server applications
- One or more GSO client applications
- One or more GSO database server (optional)
- One or more GSO database client (optional)

Supported Platforms

You can install the GSO User Administration, GSO Plus module, GSO Server, and the GSO Database Server on any of the following operating systems:

- IBM AIX
- Sun Solaris
- Microsoft Windows NT

Note: To view the specific levels of the operating systems, see the appropriate README file listed in “Readme Files” on page 157.

You can install the GSO Client, and the GSO Database Client on any of the following operating systems:

- Microsoft Windows 95
- Microsoft Windows NT

You can install the GSO 1.5 Client on IBM OS/2 Warp.

Note: To view the specific levels of the operating systems, see the appropriate README file listed in “Readme Files” on page 157.

GSO supports the following targets:

- Novell NetWare Server
- IBM OS/2 LAN Server
- IBM OS/2 Warp Server
- IBM Client Access for AS/400 for Windows 95/NT
- Microsoft Windows NT
- Lotus Notes
- 3270 host systems, including those protected by RACF and those that recognize passtickets when used with these emulators:
 - IBM Personal Communications 3270 Emulator, for all GSO client operating systems: OS/2 Warp, Microsoft Windows NT and Windows 95
 - Attachmate EXTRA! for Windows 95, Windows NT
 - Wall Data RUMBA 95/NT for the Mainframe
- 5250 host systems when used with these emulators:
 - IBM Personal Communications 5250 Emulator, for all GSO client operating systems: OS/2 Warp, Microsoft Windows NT and Windows 95.
 - Attachmate EXTRA! for Windows 95, Windows NT
- SnareWorks

Note: To view the specific product levels, see the appropriate README file listed in “Readme Files” on page 157.

GSO supports the following databases:

- DB2\6000
- Oracle
- Sybase
- Informix
- Microsoft SQL Server

Note: For more information, see “Appendix C. GSO Database-Specific Configuration” on page 107.

GSO Requirements

Before attempting to install GSO through TME, make certain you review the requirements in this section.

Hardware Requirements

The GSO client requires, at a minimum, a computer with an Intel (R) or equivalent 80486 33MHz microprocessor. Memory usage, buffer and cache management, and control structures are scalable. However, the underlying requirements of your base operating system, and the requirements of your client applications dictate the minimum requirements for disk space and memory.

RAM and Disk Space Requirements

The following list identifies the requirements for installing GSO servers and GSO clients using TME 10. The permanent disk space requirement identifies the amount of space where GSO will reside. The temporary disk space requirement identifies the amount of space needed during the installation process, this space is made available once the installation process completes. To install, at a minimum you need:

For an AIX server:

- 64MB of total memory on the server machine to run GSO servers
- 35MB of permanent disk space
- 130MB of temporary disk space

For a Solaris server:

- 64MB of total memory on the server machine to run GSO servers, including DCE servers
- 100MB of permanent disk space under the */opt* directory
- 110MB of temporary disk space under the */opt* directory

For a Windows NT server:

- 48MB of total memory on the server machine to run GSO servers, including DCE servers
- 60MB of permanent disk space
- 140MB of temporary disk space

For a Windows NT client:

- 24MB of total memory on the client machine to run GSO clients
- 20MB of permanent disk space

For a Windows 95 client:

- 16MB of total memory on the client machine to run GSO clients
- 20MB of permanent disk space

The following list identifies the requirements for installing GSO database servers and GSO database clients.

For an AIX server:

- 45MB of permanent disk space
- 50MB of temporary disk space

For a Solaris server:

- 120MB of permanent disk space
- 15MB of temporary disk space

For a Windows NT server:

- 70MB of permanent disk space
- 40MB of temporary disk space

For a Windows NT client:

- 5MB of permanent disk space
- 6MB of temporary disk space

For a Windows 95 client:

- 5MB of permanent disk space
- 6MB of temporary disk space

Note: The above numbers do not include the specific database requirements. For information about the database requirements, see the appropriate database documentation.

Software Requirements

Before you install GSO you must install:

- TME 10 Framework
- TME 10 User Administration

To take advantage of the functions provided in the following TME 10 software components, GSO requires the following:

- Software Distribution:
 - TME 10 Software Distribution
- Distributed Monitoring:
 - TME 10 Distributed Monitoring
 - Distributed Monitoring
 - TME 10 Distributed Monitoring Universal Monitors
 - TME 10 Distributed Monitoring UNIX Monitors
 - DM UNIX Monitors
- Enterprise Console:
 - TME 10 Enterprise Console

GSO Server Prerequisites

The GSO User Administration, GSO Plus module, GSO Server, and the GSO Database Server are supported on the following operating systems:

- IBM AIX
- Sun Solaris
- Microsoft Windows NT

GSO Client Prerequisites

The GSO Client, and the GSO Database Client are supported on the following operating systems:

- Microsoft Windows NT
- Microsoft Windows 95

The GSO Client Version 1.5 supports the IBM OS/2 Warp operating system. For instructions on installing IBM OS/2 Warp, see “Installing the GSO Client 1.5 on OS/2 Warp” on page 98.

Special Considerations

This section describes some special considerations you must be aware of to ensure you can successfully install GSO and use the TME Software Distribution file packages to distribute it.

Solaris Managed Nodes

Before you distribute a file package to a Solaris managed node you need to be aware of the following:

- The machine must have an */opt* directory. If an */opt* directory does not exist, create it as a subdirectory from the machine's root file system, a symbolic link to another directory in a file system on the machine, or a mount point for a partition on the machine.

- The root user must be able to write to the following directories on the machine:
 - /
 - /etc
 - /opt
 - /usr/bin
 - /usr/lib
 - /usr/sbin
- The machine must have a working network interface on which broadcasting is correctly configured. Check a machine's network interface and broadcast configuration with the **ifconfig le0** command (where **le0** is the standard device name for the Ethernet network interface of a SPARCstation)

```
le0: flags=number<string>
inet IP_address netmask mask broadcast
broadcast_address
```

Where *number* and *string* provide information about the machine's network interface. If the machine's network interface is functional, *string* includes the word UP; if the network interface is not functional, UP is absent from *string*.

IP_address and *mask* are the IP address of the local machine and the mask that defines how much of the address is used to divide networks into subnetworks.

broadcast_address specifies the address to use to represent broadcasts to the network. The correct broadcast address depends on the level of subnetting in use in the network. In general, each bit that pertains to the local host portion of the IP address should be set to 1 in the broadcast address. For example, in a class B network that uses 8 bits for the subnetwork, the last 8 bits (those for the local host) of the broadcast address should all be set to 1, which equates to decimal number 255. (See the documentation provided with your machine for more information about network configuration.)

- An appropriate entry must exist for Kerberos 5 in the Internet services database. If your environment uses */etc/services* files, the */etc/services* file on the local machine must contain the necessary entry. If your environment uses a Network Information Services (NIS) services map, the services map file on the NIS master must contain the necessary entry. In either case, the entry must have the following form:


```
kerberos5 88/udp kdc
```
- The kernel of the machine must have shared memory enabled, and it must use semaphores. To check whether these facilities are enabled, make sure that the following files exist:

```
/kernel/sys/semsys
/kernel/sys/shmsys
```

You must also make sure that the following entries exist in the */etc/name_to_sysnum* file:

```
semsys number
shmsys number
```

where *number* is a system call number. Use the following **egrep** command to check for the entries in the *name_to_sysnum* file:

```
$ /bin/egrep 'semsys|shmsys' /etc/name_to_sysnum
```

- The */etc/group* file on the machine must include an entry for the group bin. Check for the entry with the following **grep** command:

```
$ /bin/grep bin /etc/group
```

If the group bin has an entry in the file, the command displays output that includes a line similar to the following:

```
bin:additional_information
```

AIX Managed Nodes

Before you distribute a file package to an AIX managed node, add the following line to the beginning of the */etc/Tivoli/oserv.rc* file:

```
ulimit -d unlimited
```

The */etc/Tivoli/oserv.rc* file is called during installation of the system to start the Tivoli **oserv** daemon. Adding this line allows the data segment for this process to be unlimited. After you make this change you must restart your AIX system to make this change take effect.

Windows NT Managed Nodes

Before you distribute a GSO server on Windows NT you must ensure that TME 10 is using the correct *msvcrt40.dll* file and that NETBIOS is enabled.

To ensure TME 10 is using the correct *msvcrt40.dll* file, at a Windows NT command prompt type:

```
x:\winnt\system32\drivers\etc\Tivoli\setup_env.cmd
copy %BINDIR%\mslib\msvcrt40.dll %DBDIR%
copy %BINDIR%\mslib\msvcrt40.dll %DBDIR%\bin
copy %BINDIR%\mslib\msvcrt40.dll %DBDIR%\tools
cacle %DBDIR%\msvcrt40.dll /e /g everyone:r
```

Where x: is the directory where you have TME 10 installed. For more information, contact your TME 10 support.

During the installation process GSO needs to obtain the system's hardware address; therefore, NETBIOS must be enabled. To ensure NETBIOS is enabled, from the **Control Panel** double-click on the **Network** icon and view the setting on the **Protocols** tab.

PC Managed Nodes

Before you distribute a file package to a PC managed node (Windows 95 and Windows NT systems), you need to be aware of the following:

- GSO clients and GSO database clients can be distributed to PC managed nodes or managed nodes. GSO servers and GSO database servers can be distributed only to managed nodes.
- After distributing GSO, you must restart your Windows 95 or Windows NT.

Note: You will not be able to perform configuration tasks until a user signs on to the workstation which completes the restart process.

- Unlike managed nodes, PC managed nodes are not capable of returning messages to the distribution log file. Therefore when a distribution fails, your only indication will be a non-zero return code (see "Distribution Return Codes") and an indication that distribution failed in the log file. However, the GSO distribution process creates a log file named `gsocinst.log` on the PC managed node. The location of this file varies depending on how the TME PC applicaton was configured. Use the Windows Explorer in Windows 95 or Windows NT to find the log file.

On Windows 95, the file is located in:

`x:\Tivoli\meagent\win95`

On Windows NT, the file is located in one of the following:

`x:\Tivoli\meagent\win32`

`x:\var\spool\tmp\`

`%SystemRoot%\system32`

Where x: is the directory where you have TME 10 installed.

- When installing the TCP/IP Agent on Windows NT, select **Windows NT (SERULE)**.
- On Windows 95, it is necessary to increase the program environment space for the Command Processor. Add the following line to your `config.sys` file:

`shell=c:\command.com /P /E:16384`

Distribution Return Codes: The following return codes can be generated when you distribute a GSO file package to a PC managed node. The file package log file contains the generated return codes. The `gsocinst.log` file on the target workstation contains additional information.

Return Code	Explanation
2	All the required files for the file package were not transferred successfully.
3	Installation failed. Setup returned a non-zero return code.
4	Installation failed. The setup log file could not be found.

Return Code	Explanation
5	Installation failed. Setup exited abnormally. The most likely causes of this error are: <ul style="list-style-type: none"> • You are attempting to install after a previous removal of a file package and the workstation needs to be restarted. • You are attempting to reinstall or upgrade GSO but a GSO application is active. Users must end all GSO applications before you can redistribute a file package to that workstation. • The TME PC Agent is not running with Windows NT System Administrator privileges.
6	Removal of the file package failed. The most likely cause of this error is that the Tivoli Agent is not running with Windows NT System Administrator privileges.
7	GSO Prerequisite not installed. The GSO client Version 2.0 must be installed before you can install this file package.
8	The staging drive or the installation drive does not contain enough space to install the file package.
9	Installation of the database client failed because the database type could not be determined. The most likely cause of this error is that the workstation does not contain enough environment space.
a	The file package cannot be installed. The file package was distributed to the wrong operating system type.

Replica Servers

If you create a master server on an AIX machine in a heterogeneous operating system environment, you must create your replica on an AIX machine. If you create a master server on a Solaris or Windows NT machine, you can create your replica on an AIX, Solaris, or Windows NT machine.

Client and Server Time Synchronization

Disable the time synchronization features in target applications that synchronize client-machine time with their servers.

Some target applications, such as NetWare and LAN Server, allow the client machine's time to be synchronized with their servers. When the time set on GSO clients differs significantly (greater than the 15 minute default range) from the time set on GSO servers, the clients and servers cannot communicate properly.

GSO client time must be synchronized with GSO server time. The default client configuration (15 minute maximum) ensures that client-server synchronization is within an acceptable range.

Encryption Algorithms

When you purchased GSO you selected Commercial Data Masking Facility (CDMF) or Data Encryption Standard (DES) as your encryption package. Read the following information to ensure you selected the appropriate encryption algorithm for your business.

CDMF Data can be exported outside the United States.

If you selected GSO with CDMF, the IBM program number on your package must be 5697-GS1.

Note: If all the GSO clients are CDMF, then the servers can be either DES or CDMF.

DES Data cannot be exported outside the United States without appropriate DES export licenses.

If you selected GSO with DES, the IBM program number on your package must be 5697-GS2.

Notes:

1. If any GSO client is DES, then all the servers must be DES.
2. GSO supports only DES encryption on Solaris. Therefore, all GSO clients connecting to a Solaris GSO server must be DES.

Chapter 2. Installing GSO from the Desktop

Installation of GSO on the servers and clients is done through the TME desktop. The following table identifies all the steps you must follow to install and configure GSO, and make GSO fully operational.

Action	Reference
1. Check the TME 10 Framework prerequisites.	For instructions, see the appropriate TME 10 documentation.
2. Check the GSO operating system requirements.	For a list, see "Supported Platforms" on page 5 .
3. Review the GSO software and hardware prerequisites.	For a list, see "Software Requirements" on page 7 , and "Hardware Requirements" on page 6 .
4. Back up your TMR server.	For instructions, see TME 10 Framework Planning and Installation Guide.
5. Install the TME 10 GSO User Administration on the TMR server.	For instructions, see "Installing the TME 10 GSO User Administration on the TMR Server and Managed Nodes" on page 17.
6. Install GSO Plus on a TMR server.	For instructions, see "Installing GSO Plus on the TMR Server, TEC Server, and Managed Nodes" on page 18.
7. Back up your TMR server again.	For instructions, see the <i>TME 10 Framework Planning and Installation Guide</i> .
8. Install GSO Plus on the Tivoli Enterprise Consoleserver.	For instructions, see "Installing GSO Plus on the TMR Server, TEC Server, and Managed Nodes" on page 18.
9. Install GSO User Administration on all managed nodes that you want to be GSO servers or GSO database servers.	For instructions, see "Installing the TME 10 GSO User Administration on the TMR Server and Managed Nodes" on page 17.
10. Install GSO Plus on all managed nodes that you want to be GSO servers or GSO database servers.	For instructions, see "Installing GSO Plus on the TMR Server, TEC Server, and Managed Nodes" on page 18.
11. Set up the Tivoli Enterprise Console.	For instructions, see "Setting Up the Tivoli Enterprise Console" on page 82.
12. Configure the file package for the GSO server.	For instructions, see "File Packages for the GSO Server" on page 26.
13. Configure the file package for the GSO client.	For instructions, see "File Packages for the GSO Client" on page 28.

Action	Reference
14. Optional: Configure the file package for the database server.	For instructions, see "File Packages for the GSO Database Server" on page 30.
15. Optional: Configure the file package for the GSO database client.	For instructions, see "File Packages for the GSO Database Client" on page 32.
16. Distribute and install the configured file packages.	For instructions, see "Installing GSO Servers and Clients" on page 34.
17. Configure the GSO master server	For instructions, see "Configure GSO Master Server" on page 37.
18. Optional: Configure a GSO replica server.	For instructions, see "Configure GSO Replica Server" on page 38.
19. Configure the GSO clients.	For instructions, see "Configure GSO Clients" on page 40.
20. Optional: Configure a GSO Database Server.	For instructions, see "Configure GSO Database Server" on page 39.
21. Set up a target type list.	For instructions, see "Chapter 3. Managing the IBM GSO Cell" in the <i>IBM Global Sign-On, User Administration Guide</i> .
22. Create GSO user IDs.	For instructions, see "Chapter 4. Configuring IBM GSO User Information" in the <i>IBM Global Sign-On, User Administration Guide</i> .
23. Configure the GSO targets.	For instructions, see "Chapter 6. Managing GSO Targets and Target Groups" in the <i>IBM Global Sign-On, User Administration Guide</i> .
24. Define GSO cell as a managed resource.	For instructions, see the <i>TME 10 Framework Platform User's Guide</i> .
25. Subscribe the GSO cell to a user profile.	For instructions, see "Chapter 3. Managing the IBM GSO Cell" in the <i>IBM Global Sign-On, User Administration Guide</i> .
26. Distribute user profiles.	For instructions, see "Chapter 2. Administration and Subadministration" in the <i>IBM Global Sign-On, User Administration Guide</i> .
27. Configure GSO programs.	For instructions, see "Chapter 5. Configuring GSO Programs" in the <i>IBM Global Sign-On, User Administration Guide</i> .

Action	Reference
28. Launch GSO targets.	For instructions, see the <i>IBM Global Sign-On Launcher Help</i> online book which is accessible through the Start menu on the taskbar.

Note: The TME 10 Software Distribution, TME 10 Distributed Monitoring, and TME 10 Enterprise Console applications must be installed and configured before their corresponding Tivoli/Plus features are available.

Installing the TME 10 GSO User Administration on the TMR Server and Managed Nodes

TME 10 GSO User Administration adds GSO user accounts to your current TME 10 Framework. The GSO server CD contains the software for TME 10 GSO User Administration. The TME filepack can be installed from any managed node in the Tivoli Management Region (TMR).

Use the following steps to install the TME 10 GSO User Administration:

1. Make sure you are logged on the TME 10 desktop as an administrator with the *install_product* authorization role capability and that you have the server CD inserted in the CD-ROM.
2. From the **Desktop** menu, select the **Install-->Install Product...** option to display the **Install Product** dialog.

If **TME 10 GSO User Administration** is not listed in the **Select Product to Install** scrolling list, proceed to step 3. If **TME 10 GSO User Administration** is listed, skip to step 4.
3. Press the **Select Media...** button to display the **File Browser** dialog. The **File Browser** dialog allows you to define the path to the installation CD image. Do one of the following:
 - If you already know the path to the CD image:
 - a. Enter the full path in the **Path Name** field.
 - b. Press the **Set Path** button to change directories using the specified path.
 - c. Press the **Set Media & Close** button to save the new path and return to the **Install Product** dialog. The **Select Product to Install** scrolling list is updated with the list of products that are available for installation.
 - If you do not know the path to the CD image:
 - a. From the **Hosts** scrolling list, select the host on which the install media is mounted. Selecting a host updates the **Directories** scrolling list to display the directories of that host.
 - b. From the **Directories** scrolling list, select the directory containing the install medium.

- c. Press the **Set Media & Close** button to save the new path and return to the **Install Product** dialog. The **Select Product to Install** scrolling list is updated with a list of products that are available for installation.

Note: If **TME 10 GSO User Administration** does not show up in the **Select Product to Install** scrolling list, verify the path to your installation medium.

4. Select **TME 10 GSO User Administration** from the **Select Product to Install** scrolling list.
5. To specify the clients where you want to install this product, use the arrow buttons to move clients between the **Clients to Install On** and the **Available Clients** scrolling lists.
6. Press the **Install & Close** button to begin the installation process. The **Product Install** dialog is displayed. This dialog displays the progress of the installation process and warns you of any problems that you might have to correct before the installation can be completed.
7. Do one of the following:
 - If an error message displays requiring that you make changes before the installation process can continue, press the **Cancel** button, correct the problem and start the installation process again.
 - If no errors are found, press the **Continue Install** button to continue with the installation process. The **Product Install** dialog continues displaying the status of the installation process as it proceeds.
8. When the "Finished product installation" message displays, press the **Close** button to close the dialog.

TME 10 GSO User Administration is now installed on the managed nodes you selected.

Installing GSO Plus on the TMR Server, TEC Server, and Managed Nodes

You can use this task to install GSO Plus on a TMR server as well as to install GSO Plus on a managed node, the procedure is the same. The example that follows outlines the steps for installing GSO Plus on a TMR server.

Use the following steps to install GSO Plus on the TMR server:

1. Make sure you are logged on the TME 10 desktop as an administrator with the *install_product* authorization role capability and that you have the server CD inserted in the CD-ROM.
2. From the **Desktop** menu, select the **Install->Install Product...** option to display the **Install Product** dialog.
3. Press the **Select Media...** button to display the **File Browser** dialog. The **File Browser** dialog allows you to define the path to the installation CD image. Do one of the following:
 - If you already know the path to the CD image:
 - a. Enter the full path in the **Path Name** field. (GSO Plus is located in the `/tme/gso/plus` directory.)

- b. Press the **Set Path** button to change directories using the specified path.
 - c. Press the **Set Media & Close** button to save the new path and return to the **Install Product** dialog. The **Select Product to Install** scrolling list is updated with the list of products that are available for installation.
- If you do not know the path to the CD image:
 - a. From the **Hosts** scrolling list, select the host on which the install media is mounted. Selecting a host updates the **Directories** scrolling list to display the directories of that host.
 - b. From the **Directories** scrolling list, select the directory containing the install media. (GSO Plus is located in the `/tme/gso/plus` directory.)
 - c. Press the **Set Media & Close** button to save the new media path and return to the **Install Product** dialog. The **Select Product to Install** scrolling list is updated with a list of products that are available
4. Select **GSO Plus** from the **Select Product to Install** scrolling list.
 5. To specify the TME clients on which this product will be installed, use the arrow buttons to move TME clients between the **Clients to Install On** and the **Available Clients** scrolling lists.
By default, all TME clients in the current TMR are listed in the **Clients to Install On** scrolling list. If you do not want to install the **GSO Plus** on a TME client, select that TME client from the **Clients to Install On** scrolling list and press the right arrow button. The selected TME client is moved to the **Available Clients** scrolling list.
 6. Press the **Install & Close** button to begin the installation process. The **Product Install** dialog is displayed. This dialog displays the progress of the installation process and warns you of any problems that you might have to correct before the installation can be completed.
 7. Do one of the following:
 - If an error message displays requiring that you make changes before the installation process can continue, press the **Cancel** button, correct the problem and start the installation process again.
 - If no errors are found, press the **Continue Install** button to continue with the installation process. The **Product Install** dialog continues displaying the status of the installation process as it proceeds.
 8. When the "Finished product installation" message displays, press the **Close** button to close the dialog.

The **GSO Plus** icon is added to the **TivoliPlus** window.

Installing from the Command Line

Use the **winstall** command to install TME 10 GSO User Administration and GSO Plus from the command line. The following is an example of the **winstall** command and its parameters:

```
winstall -c cdrom_path -s installation_server \i index_file
```

- c *cdrom_path*
Specifies the path to the CD image.
- s *installation*
Specifies the server on which the product is to be installed.
- i *index_file*
Specifies the index file from which the product is to be installed.

TME 10 GSO User Administration is located in the `/tme/gso/user` directory. GSO Plus is located in the `/tme/gso/plus` directory. For more information on the **winstall** command, see in the *Tivoli Management Platform Reference* manual.

Starting a Tivoli/Plus Module

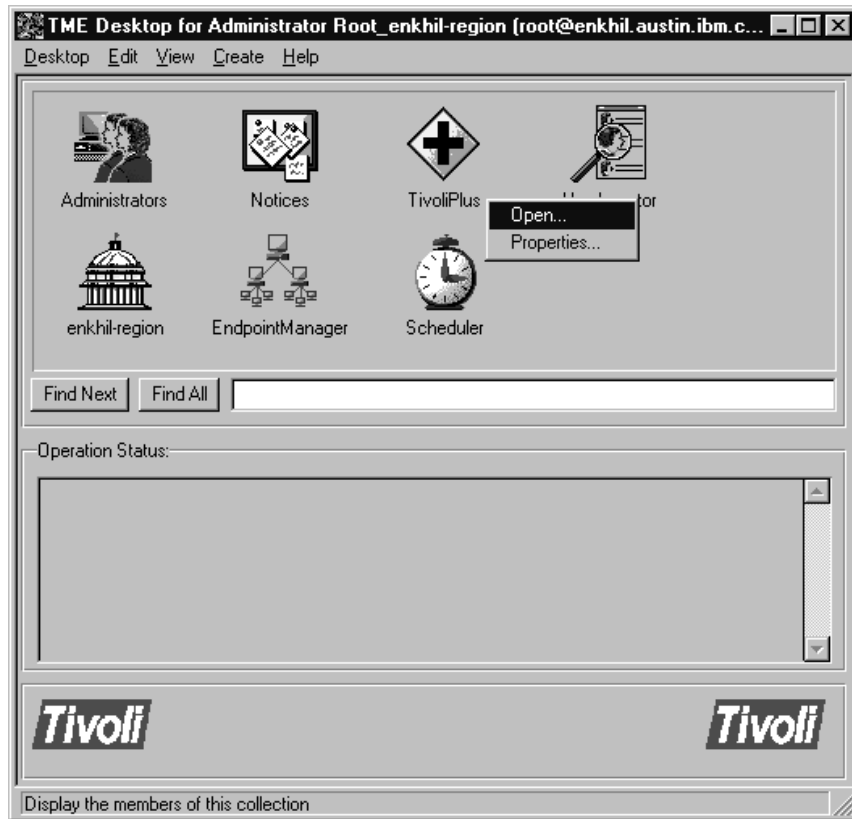
All Tivoli/Plus modules are kept in a collection under the **TivoliPlus** window. The module's icon is added to this collection after installation. The following icon represents the Tivoli/Plus collection:



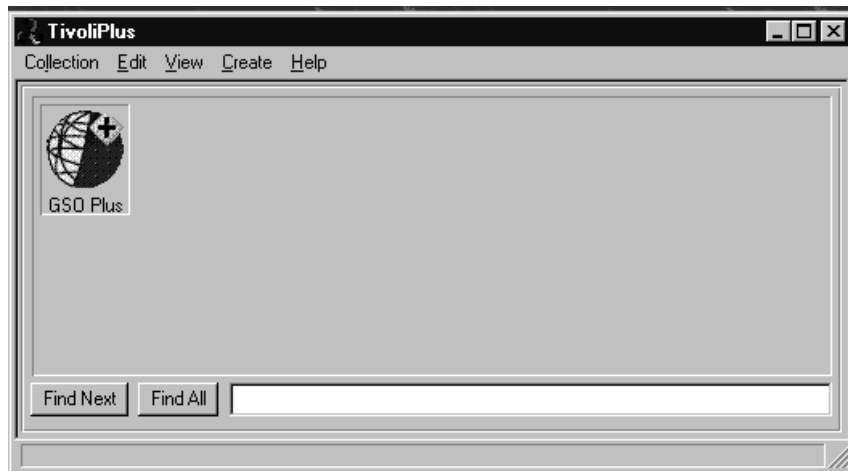
TivoliPlus

Use the following steps to see the modules included in your Tivoli/Plus collection:

1. From the main TME desktop, double-click on the **TivoliPlus** icon or select the **Open...** option from the **TivoliPlus** icon's pop-up menu

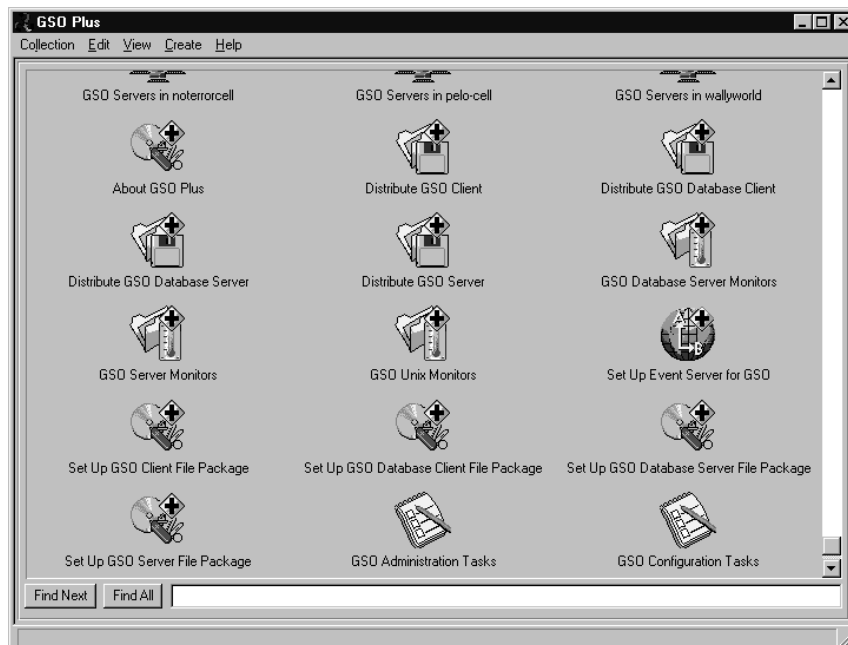


to display the **TivoliPlus** window.



The **TivoliPlus** window displays an icon for each Tivoli/Plus module installed. In the case above, only the GSO Plus module is installed.

2. Double-click on the **GSO Plus** icon to display the icons representing the tasks and tools for managing GSO.



Tivoli/Plus Icons

Although the Tivoli/Plus icons look like (traditional) TME icons, their functionality has been altered slightly to provide a faster, more intuitive approach to navigating and deploying the module's features. In some cases, like Tivoli Courier file package profile, menu items have been removed from the icon's pop-up menu to create a more "point and click" environment.

You can activate the Tivoli/Plus icon in either of two ways:

- Opening the icon by double-clicking on it with the left mouse button. In many cases, double-clicking runs an activity (such as a task) without opening another dialog layer.
- Displaying the icon's pop-up menu by pressing and holding the right mouse button.

Generally, you can use either method to access a particular function. There are cases where a particular function can be accessed only by one of these methods.

The following icon represents GSO Plus:



GSO Plus

Chapter 3. Software Distribution for GSO



GSO Plus supports the creation of file packages for distributing and installing GSO on servers and clients. To perform these tasks you must have senior admin role authority. Much of the configuration has been done for you. Using GSO Plus and TME 10 Software Distribution, you can distribute GSO applications across a multiplatform network. For example, you can distribute the GSO client application to both a Windows 95 and Windows NT platform.



Distributing GSO is a two stage process. First, you must configure a TME 10 Software Distribution file package for each type of operating system on which you are installing a GSO server or client. Second, you must distribute the configured file packages by running the distribute task. The distribute task uses the file packages to distribute the GSO binaries and initiate the GSO installation process. By running the distribute task, you can install GSO on the selected subscribers.

Note: Installing the GSO Plus module does not copy the installation images to a hard disk. Therefore, you have to make the CD available to a managed node that has the GSO Plus module. The CD must be physically in a CD-ROM drive on a managed node or the CD image must be copied from the CD to a hard disk on a managed node.

Configuring TME 10 Software Distribution File Packages

The following table identifies the GSO Plus set up icons for configuring the various GSO file packages.

Function	Icon
Configures a file package for distributing a GSO server.	 Set Up GSO Server File Package
Configures a file package for distributing a GSO client.	 Set Up GSO Client File Package

Function	Icon
Configures a file package for distributing a GSO database server.	 <p data-bbox="821 344 1235 369">Set Up GSO Database Server File Package</p>
Configures a file package for distributing a GSO database client.	 <p data-bbox="826 543 1230 569">Set Up GSO Database Client File Package</p>

The following sections explain how to configure these file packages.

Notes:

1. You will need to configure a file package for each platform where you plan to install GSO servers and clients. The steps for completing the set up window are similar for each platform; therefore, when naming the file packages make sure you select a name that helps you identify the platform.
2. You can install GSO servers only on managed nodes. You can install GSO clients on PC managed nodes or managed nodes.

File Packages for the GSO Server

Create a file package for each platform (AIX, Solaris or NT) where you plan to install a GSO server. Use the following steps:

1. From the **GSO Plus** window, double-click on the **Set Up GSO Server File Package** icon to display the **Set Up GSO Server File Package** dialog.

The screenshot shows the 'Set Up GSO Server File Package' dialog box. It features a title bar with the text 'Set Up GSO Server File Package' and standard window controls. The dialog is organized into several sections:

- File Package Name:** A text input field.
- Source Files Information:** A section containing two text input fields: 'Source Host Name' and 'Source Path'.
- Distribution Options:** A section containing a dropdown menu for 'Target Platform Operating System' set to 'AIX'.
- UNIX Specific Options:** A section containing a text input field for 'Distribute to Staging Path' with the value '/tmp'.
- NT Specific Options:** A section containing a text input field for 'Distribute to Staging Path' with the value 'C:\TEMP', a dropdown menu for 'Install to Drive' set to 'C:', and a checked checkbox labeled 'Restart Windows NT after distribution or removal'.

At the bottom of the dialog are three buttons: 'Set and Close', 'Cancel', and 'Help'.

2. In the **File Package Name** field, enter a name (that is unique within the entire region) for the file package you are creating. The same name is used to name the error log file. During the distribution of the file package, TME 10 Software Distribution creates a local log file (*File Package Name.log*) in the TME temp directory.
3. In the **Source Files Information** block:
 - a. In the **Source Host Name** field, enter the name of the machine that identifies the location of the server CD installation image.
 - b. In the **Source Path** field, enter the directory path of the server CD installation image.
4. In the **Distribution Options** block:

- a. Press the **Target Platform Operating System** arrow to select the platform you want to install on.
 - b. Do one of the following:
 - If you select AIX or Solaris as the target platform, enter in the **Distribute to Staging Path** field the temporary location where you want the installation image to reside. This path is erased after the installation is completed.
 - If you select Windows NT as the target platform, in the **NT Specific Options** block:
 - 1) In the **Distribute to Staging Path** field, enter the temporary location where the installation image will reside. This path is erased after the installation process is completed.
 - 2) In the **Install to Drive** field, enter the letter that identifies the drive you want the GSO server to reside on.
 - 3) Select the **Restart Windows 95/NT after distribution or removal** button to restart Windows 95/NT after the file package is distributed to the server machine.
- Note:** You must restart Windows NT to activate GSO.
5. Press the **Set and Close** button. This task creates an icon for the file package in the **Distribute GSO Server** collection window.
 6. Repeat steps 1-5 for each operating system.

File Packages for the GSO Client

Create a file package for each platform (Windows NT or Windows 95) where you plan to install the GSO client. For information about special considerations you should be aware of in this environment, see "Special Considerations" on page 8. Use the following steps:

1. From the **GSO Plus** window, double-click on the **Set Up GSO Client File Package** icon to display the **Set Up GSO Client File Package** dialog.

The screenshot shows a Windows-style dialog box titled "Set Up GSO Client File Package". It features a standard title bar with minimize, maximize, and close buttons. The dialog is divided into several sections:

- File Package Name:** A text input field.
- Source Files Information:** A section containing three fields: "Source Host Name" (text input), "Source Path" (text input), and "Language" (dropdown menu currently set to "U.S. English").
- Distribution Options:** A section containing four items: "Target Platform Operating System" (dropdown menu set to "Win 95"), "Distribute to Staging Path" (text input set to "C:\TEMP"), "Install to Drive" (dropdown menu set to "C:"), and a checked checkbox labeled "Restart Windows 95/NT after distribution or removal".
- Buttons:** Three buttons at the bottom: "Set and Close", "Cancel", and "Help".

2. In the **File Package Name** field, enter a name (that is unique within the entire region) for the file package you are creating. The same name is used to name the error log file. During the distribution of the file package, TME 10 Software Distribution creates a local log file (*File Package Name.log*) in the TME temp directory. GSO also creates a log file (*gsocinst.log*) on each machine.
3. In the **Source Files Information** block:
 - a. Enter in the **Source Host Name** field, the name of the machine that identifies the location of the Windows client CD installation image.
 - b. Enter in the **Source Path** field, the directory path of the Windows client CD installation image.
 - c. Press the **Language** arrow to select the language of the software you are installing.
4. In the **Distribution Options** block:
 - a. Press the **Target Platform Operating System** arrow to select the platform you want to install on.

- b. Enter in the **Distribute to Staging Path** field, the temporary location where the installation image will reside. This path is erased after the installation process is completed.
- c. Enter in the **Install to Drive** field, the letter that identifies the drive you want the GSO client to reside on.
- d. Select the **Restart Windows 95/NT after distribution or removal** button to restart Windows 95/NT after the file package is distributed to the client machine.

Note: You must restart Windows 95/NT to activate GSO.

5. Press the **Set and Close** button. This task creates an icon for the file package in the **Distribute GSO Client** collection window.
6. Repeat steps 1-5 for each operating system.

File Packages for the GSO Database Server

Create a file package for each platform (AIX, Solaris, or NT) where you plan to install a GSO database server. Use the following steps:

1. From the **GSO Plus** window, double-click on the **Set Up GSO Database Server File Package** icon to display the **Set Up GSO Database Server File Package**

dialog.

Set Up GSO Database Server File Package

File Package Name

Source Files Information

Database Type

Source Host Name

Source Path

Distribution Options

Target Platform Operating System

UNIX Specific Options

Distribute to Staging Path

NT Specific Options

Distribute to Staging Path

Install to Drive

Restart Windows NT after distribution or removal

2. In the **File Package Name** field, enter a name (that is unique within the entire region) for the file package you are creating. The same name is used to name the error log file. During the distribution of the file package, TME 10 Software Distribution creates a local log file (*File Package Name.log*) in the TME temp directory.
3. In the **Source Files Information** block:
 - a. Press the **Database Type** arrow to select the type of database you want to install. For information on database types, see “Appendix C. GSO Database-Specific Configuration” on page 107.
 - b. Enter in the **Source Host Name** field, the name of the machine that identifies the location of the server CD installation image.

- c. Enter in the **Source Path** field, the directory path of the server CD installation image.
4. In the **Distribution Options** block:
 - a. Press the **Target Platform Operating System** arrow to select the platform you want to install on.
 - b. Do one of the following:
 - If you select AIX or Solaris as the target platform, in the **Distribute to Staging Path** field enter the temporary location where you want the installation image to reside. This path is erased after the installation process is completed.
 - If you select Windows NT as the target platform, in the **NT Specific Options** block:
 - 1) In the **Distribute to Staging Path** field, enter the temporary location where the installation image will reside. This path is erased after the installation process is completed.
 - 2) In the **Install to Drive** field, enter the letter that identifies the drive you want the GSO database server to reside on.
 - 3) Select the **Restart Windows 95/NT after distribution or removal** button to restart Windows 95/NT after the file package is distributed to the server machine.
- Note:** You must restart Windows 95/NT to activate GSO.
5. Press the **Set and Close** button. This task creates an icon for the file package in the **Distribute GSO Database Server** collection window.
6. Repeat steps 1-5 for each operating system.

File Packages for the GSO Database Client

Create a file package for each platform (Windows NT or Windows 95) where you plan to install a GSO database client. Use the following steps:

1. From the **GSO Plus** window, double-click on the **Set Up GSO Database Client File Package** icon to display the **Set Up GSO Database Client File Package** dialog.

The screenshot shows a Windows-style dialog box titled "Set Up GSO Database Client File Package". It features a standard title bar with minimize, maximize, and close buttons. The dialog is organized into several sections:

- File Package Name:** A text input field at the top.
- Source Files Information:** A section containing:
 - Database Type:** A dropdown menu currently set to "ODBC".
 - Source Host Name:** A text input field.
 - Source Path:** A text input field.
 - Language:** A dropdown menu currently set to "U.S. English".
- Distribution Options:** A section containing:
 - Target Platform Operating System:** A dropdown menu currently set to "Win 95".
 - Distribute to Staging Path:** A text input field containing "C:\TEMP".
 - Restart Windows 95/NT after distribution or removal**

At the bottom of the dialog are three buttons: "Set and Close", "Cancel", and "Help".

2. In the **File Package Name** field, enter a name (that is unique within the entire region) for the file package you are creating. The same name is used to name the error log file. During the distribution of the file package, TME 10 Software Distribution creates a local log file (*File Package Name.log*) in the TME temp directory. Also, GSO creates a log file (*gsocinst.log*) on each target machine in the TME PC Agent directory.
3. In the **Source Files Information** block:
 - a. Press the **Database Type** arrow to select the type of database you want to install. For information on database types, see "Appendix C. GSO Database-Specific Configuration" on page 107.
 - b. Enter in the **Source Host Name** field, the name of the machine that identifies the location of the Windows client CD installation image.
 - c. Enter in the **Source Path** field, the directory path of the Windows client CD installation image.

- d. Press the **Language** arrow to select the language of the software you are installing.
4. In the **Distribution Options** block:
 - a. Press the **Target Platform Operating System** arrow to select the platform you want to install on.
 - b. In the **Distribute to Staging Path** field, enter the temporary location where the installation image will reside. This path is erased after the installation process is completed.
 - c. Enter the letter that identifies the drive you want the GSO database client to reside on, in the **Install to Drive** field.
 - d. Select the **Restart Windows 95/NT after distribution or removal** button to restart Windows 95/NT after the file package is distributed to the server machine.

Note: You must restart Windows 95/NT to activate GSO.

5. Press the **Set and Close** button. This task creates an icon for the file package in the **Distribute GOS Database Client** collection window.
6. Repeat steps 1-5 for each operating system.

Installing GSO Servers and Clients

After you configure the TME 10 Software Distribution file packages, you are ready to install them. Before you start the installation process, make sure you read the discussion on “Special Considerations” on page 8.

If you want to view the TME 10 Software Distribution file packages that you created, select the **Open...** option from the distribute icon’s pop-up menu.

Note: You can install GSO servers only on managed nodes. You can install GSO clients on PC managed nodes or managed nodes.

Use the following steps to install GSO using the file packages you configured:

1. From the **GSO Plus** window, select the **Subscribers...** option from the **Distribute** icon’s pop-up menu that contains the file package you want to install. The **Subscribers** dialog is displayed.
2. Specify the subscription list you want to use to install the GSO servers or clients by using the right and left arrow buttons to create the desired list in the **Current Subscribers** field.
3. Press the **Set Subscriptions & Close** button. The **GSO Plus** window is displayed.
4. Select the **Open ...** option from the file package icon’s pop-up menu. The appropriate **Distribute** dialog is displayed containing the list of file packages you created.

Note: After installing GSO servers and clients, you must configure them. For more information, “Chapter 4. Configuration Tasks for GSO” on page 37. A GSO database server cannot reside on the same machine as the GSO master server. Make sure that you do not install a GSO database server on the machine which you intend to configure the GSO master server.

5. Select the **Open ...** option from the distribute icon’s pop-up menu. The **File Package Properties** dialog is displayed.
6. Ensure the **Host** and **Path** fields are what you want to use. If you make a change to either field, press the **Save** button.

During the installation process GSO performs pre-installation checks, such as verifying available disk space. The output of the check process is sent to the host machine you named in the **Host** field in the file named in the **Path** field. If you use the default path the log file is sent to:

```
/tmp/filepackagename.log
```

where *filepackagename.log* is the name specified in the **Path** field.

After you distribute each file package, consult the file package log file to see the results of the installation.

7. From the **File Package** menu, select the **Distribute...** option. The **Distribute File Package** dialog is displayed.
8. In the **Available Subscribers** field, select the servers you want to receive the file package by using the left and right arrow buttons to move the name of the server into the **Distribute File Package To** field.
9. Press the **Distribute & Close** button.

Removing GSO Software

If you want to remove (uninstall and unconfigure) GSO software from a machine make sure you first remove the replica servers before you remove the GSO master server.

Use the following steps to unconfigure and uninstall GSO software:

1. Insert the GSO CD into the CD-ROM drive.
2. From the **GSO Plus** window, select the **Open...** option from the **Distribute** icon’s pop-up menu that you want to uninstall. The **Distribute Collection** window is displayed.
3. Select the **Open...** option from the file package you want to uninstall.
4. From the **File Package** menu, select the **Remove From Hosts...** option. The **Remove File Package** dialog is displayed.
5. In the **Available Subscribers** field, select the managed nodes you want to remove by using the left and right arrow buttons to move the name of the managed node into the **Remove File Package From** field.
6. Press the **Remove & Close** button.

Chapter 4. Configuration Tasks for GSO

This chapter describes the configuration tasks that are available from the **GSO Configuration Tasks** window. To perform these tasks you must have senior admin role authority.

You must configure the GSO master server before you can do any other configuration.

Time Synchronization Issues

GSO requires that all machines, within a GSO cell, have synchronized clocks. GSO replica servers and database servers must have their time synchronized within 5 minutes of the GSO master server. GSO clients must have their time synchronized within 15 minutes of the GSO replica server or master server where they are connected.

After the GSO servers and database servers are configured, GSO maintains their time synchronized. GSO does not maintain the time synchronization for client machines. GSO coexists with other time services as long as all the GSO clients and servers in a GSO cell are within the scope of the same time service.

Configure GSO Master Server

A master server is the first instance of a GSO server in a GSO cell. Only one master server can exist within a GSO cell at one time. Installation of the servers and clients can be done in any order; however, configuration of the master server must be done before any other configuration tasks.

Note: If you create a master server on an AIX machine in a heterogeneous operating system environment, you must create your replica on an AIX machine. If you create a master server on a Solaris or Windows NT machine, you can create your replica on an AIX, Solaris, or Windows NT machine.

Use the following steps to configure and automatically start a GSO master server:

1. From the **GSO Plus** window, double-click on the **GSO Configuration Tasks** icon to display the **Task Library: GSO Configuration Task** window.
2. Double-click on the **Configure GSO Master Server** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.

5. In the **Execution Targets** block, select the managed node you want to use as your master server by using the left and right arrow buttons to move the name of the managed node into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to display the **Configure GSO Master Server** dialog.



7. In the **New Cell Name** field, enter the name you want to assign to the GSO cell.
8. In the **New Cell Password** field, enter the password you want to assign to the GSO cell.
9. Press the **Set and Close** button to complete this task.

Configure GSO Replica Server

A replica server is a duplicate copy (read-only) of the master server. There is no limit on the number of replica servers that can exist in a GSO cell. You cannot directly modify a replica server; GSO attempts to update the replica server immediately after a change was made to the master server.

You will want to create a replica server for the following reasons:

- To distribute information throughout a network.
- To make information more accessible to users and applications within a network environment.
- To improve response time.
- To preserve a backup of the information contained in the master server.

Note: If you create a master server on an AIX machine in a heterogeneous operating system environment, you must create your replica on an AIX machine. If you create a master server on a Solaris or Windows NT machine, you can create your replica on an AIX, Solaris, or Windows NT machine.

Use the following steps to configure a GSO replica server:

1. From the **GSO Plus** window, double-click on the **GSO Configuration Tasks** icon to display the **Task Library: GSO Configuration Task** window.
2. Double-click on the **Configure GSO Replica Server** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the replica server you want to configure by using the left and right arrow buttons to move the name of the replica server into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to display the **Configure GSO Replica Server** dialog.



7. In the **Cell Name** field, enter the name of the GSO cell.
8. In the **Cell Master Server** field, enter the name of the master server for this cell .
9. Press the **Set and Close** button to complete this task.

Configure GSO Database Server

There is no limit on the number of database servers that can exist in a GSO cell. Use the following steps to configure a GSO database server:

1. From the **GSO Plus** window, double-click on the **GSO Configuration Tasks** icon to display the **Task Library: GSO Configuration Task** window.
2. Double-click on the **Configure GSO Database Server** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.

5. In the **Execution Targets** block, select the database server you want to configure by using the left and right arrow buttons to move the name of the database server into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to display the **Configure GSO Database Server** dialog.



7. In the **Cell Name** field, enter the name of the GSO cell.
8. In the **Cell Master Server** field, enter the name of the master server for this cell.
9. Press the **Set and Close** button to complete this task.

For more information on databases, see "Appendix C. GSO Database-Specific Configuration" on page 107.

Configure GSO Clients

Each client must be "connected" to a GSO server. The following steps assume that the GSO client was successfully installed on the target machine. Use the following steps to configure a GSO client:

1. From the **GSO Plus** window, double-click on the **GSO Configuration Tasks** icon to display the **Task Library: GSO Configuration Task** window.
2. Double-click on the **Configure GSO Client** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the GSO client you want to configure by using the left and right arrow buttons to move the name of the GSO client into the **Selected Task Endpoints** field.

6. Press the **Execute & Dismiss** button to display the **Configure GSO Client** dialog.

The screenshot shows a dialog box titled "Configure GSO Client". It features a standard Windows-style title bar with minimize, maximize, and close buttons. The main area contains four text input fields labeled "Cell Name", "Master Server", "Primary Replica (optional)", and "Secondary Replica (optional)". Below these fields are two checkboxes: "Integrated Login" (checked) and "Litronic Smart Card" (unchecked). At the bottom of the dialog are three buttons: "Set and Close", "Cancel", and "Help".

7. In the **Cell Name** field, enter the name of the GSO cell.
8. In the **Master Server** field, enter the name of the GSO master server.
9. Optional: In the **Primary Replica** field, enter the name of the first replica server you want to associate with this client.
10. Optional: In the **Secondary Replica** field, enter the name of the second replica server you want to associate with this client. The client contacts the secondary replica server only when the primary replica server is not available. When both replicas servers are not available the master server is contacted.
11. If you want to configure this client machine to automatically sign-on to GSO when the user signs on to the desktop select **Integrated Login**.
12. If you want to configure this client machine to use a Litronic Smart Card for GSO authentication select **Litronic Smart Card**.

Note: Before you select **Litronic Smart Card**, the smart card hardware must already be installed and configured. For more information, see "Appendix A. Installing Smart Card Administration" on page 95.

13. Press the **Set and Close** button to complete this task.

Creating GSO Users and Targets

After you successfully installed and configured GSO on the servers and clients you must perform additional tasks to make GSO fully operational. The following list outlines the additional tasks you must complete.

1. Set up a target type list.
2. Create GSO user IDs.
3. Configure the GSO targets.
4. Define GSO cell as a managed resource.
5. Subscribe the GSO cell to a user profile.
6. Distribute user profiles.
7. Configure GSO programs.
8. Launch GSO targets.

Steps 1 - 7 must be completed before the GSO user can launch GSO targets. For instructions on how to complete the above tasks, see the *IBM Global Sign-On for Multiplatforms User Administration Guide*. For instructions on how a GSO user can launch GSO targets, see the *Global Sign-On Launcher Help* online book which is accessible through the **Start** menu on the taskbar.

Chapter 5. Management Tasks for GSO

This chapter describes the tasks that are available from the **GSO Administration Tasks** window. A task is a set of instructions that you execute routinely on GSO servers and clients. To perform these tasks you must have senior admin role authority.

Start Server

Use the following steps to start the GSO server processes on a managed node:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Start Server** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the name of the server you want to start by using the left and right arrow buttons to move the desired server into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to complete this task.

Stop Server

Use the following steps to stop all associated GSO server processes on a managed node:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Stop Server** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the server you want to stop by using the left and right arrow buttons to move the desired server into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to complete this task.

Backup Cell

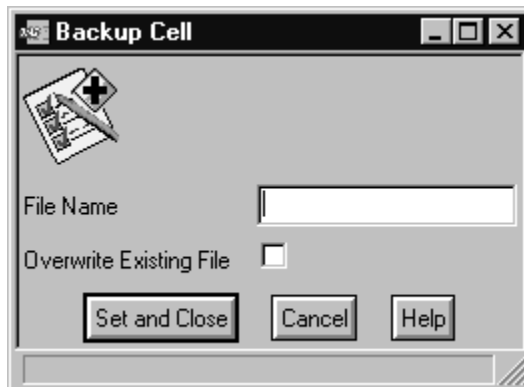
Use this task to back up the data on the GSO master server (cell). By backing up regularly, you can always restore the GSO master server in order to recover from accidental record deletions or from catastrophic system failures. (For information on restoring a cell, see “Restore Cell” on page 45.)

Create a backup every time you successfully add GSO servers, or whenever a significant number of updates have been applied to the GSO data. You can use the TME scheduler to create regular backups during off-peak hours.

Note: Always restore the backup image to the same master server.

Use the following steps to backup the cell:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Backup Cell** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the server you want to backup by using the left and right arrow buttons to move the name of the desired server into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to display the **Backup Cell** dialog.



7. In the **File Name** field, enter the path and filename where you want the backup to be stored.
8. Select **Overwrite Existing File** if you want to overwrite an existing backup file in the specified path.
9. Press the **Set and Close** button to complete this task.

Restore Cell

You can return the GSO master server to a previous state by restoring it from a backup copy. When you restore a backup copy of the cell to the master server the following occurs:

- The master server is tested to ensure it is in a steady state before beginning the restore cell process.
- All the GSO services are stopped.
- The backup copy is restored on the master server.
- All the GSO services are started again.

Note: Make sure you always restore the backup image to the same master server. All server replicas will be updated with the backup image on the master server.

Use the following steps to return a GSO master server to a previous state:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Restore Cell** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the server you want to restore by using the left and right arrow buttons to move the name of the server into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to display the **Restore Cell** dialog.



7. In the **File Name** field, enter the name of the backup file you want to use to restore the GSO cell.
8. Press the **Set and Close** button to complete the task.

Remove Machine From Cell

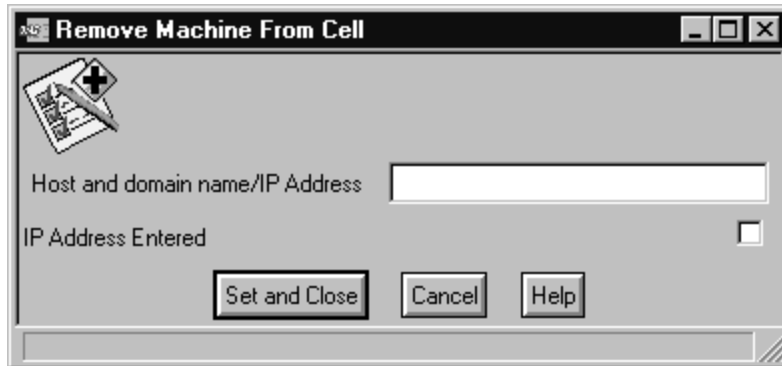
If any GSO server becomes permanently unavailable, you will want to communicate this to the master server so that all references to that server can be removed. This task can be run only on the GSO master server.

You will want to remove a machine from a cell for the following reasons:

- To change its network configuration.
- To disable references to a machine that is unreachable because of a hardware or software crash.

Use the following steps to remove a machine from a cell:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Remove Machine From Cell** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the server you want to remove from a cell by using the left and right arrow buttons to move the name of the server into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to display the **Remove Machine From Cell** dialog.



7. In the **Host and domain name/IP Address** field, enter the name of the machine or the IP address of the machine you want to remove.
8. If you entered an IP address in the above field, select **IP Address Entered**.
9. Press the **Set and Close** button.

Set Password Policy

Use this task to change the password policies of the GSO master server. (You can run this task only on the GSO master server.) You might want to change a password policy for the following reasons:

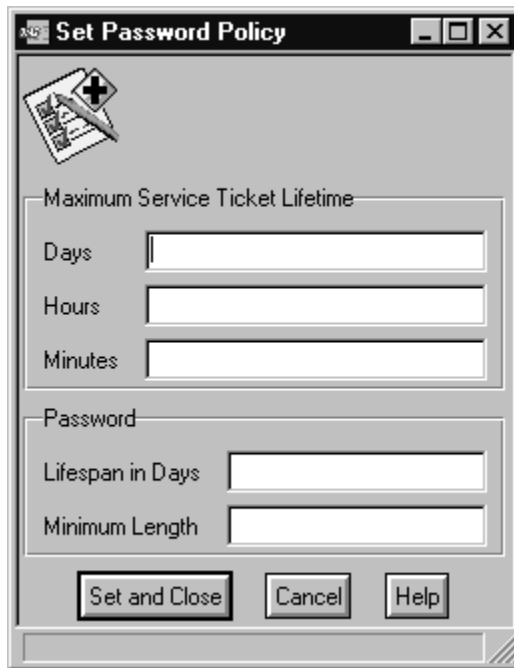
- To set the amount of time a user can be logged on without having to refresh their credentials.
- To set how long a user's password remains valid.
- To set the minimum length of a user's password.

Note: If you need to change a password policy, you must also change all of the fields at the same time.

Use the following steps to change the password policy on the master server:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Set Password Policy** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the GSO master server whose password policy you want to change by using the left and right arrow buttons to move the name of the master server into the **Selected Task Endpoints** field.

6. Press the **Execute & Dismiss** button to display the **Set Password Policy** dialog.



The screenshot shows a dialog box titled "Set Password Policy". It features a standard Windows-style title bar with minimize, maximize, and close buttons. The dialog is divided into two main sections. The first section, "Maximum Service Ticket Lifetime", contains three input fields labeled "Days", "Hours", and "Minutes". The second section, "Password", contains two input fields labeled "Lifespan in Days" and "Minimum Length". At the bottom of the dialog, there are three buttons: "Set and Close", "Cancel", and "Help".

7. In the **Maximum Service Ticket Lifetime** block:
 - a. In the **Days** field, enter the number of days the user can remain logged on without having to refresh their credentials. The default is 1 day.
 - b. In the **Hours** field, enter the number of hours the user can remain logged on without having to refresh their credentials. The default is 24 hours.
 - c. In the **Minutes** field, enter the number of minutes the user can remain logged on without having to refresh their credentials.
8. In the **Password** block:
 - a. In the **Lifespan in Days** field, enter how long a user's password will remain valid before it expires. The default is forever.
 - b. In the **Minimum Length** field, enter the minimum length of the password. The valid range is 1 to 512 alphanumeric characters. The default is 1.
9. Press the **Set and Close** button.

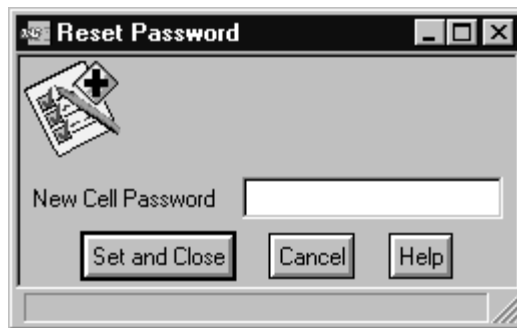
Reset Password

If security has been compromised, you can reset the GSO password. You must run this task on each one of the GSO servers in the cell (GSO master server, GSO replica servers, and GSO database servers). If you forget to run the reset password task on a server, that server will not continue to function within the GSO cell.

Note: This task invalidates all previous backups. Therefore, make sure you back up the master server after you reset the password.

Use the following steps to reset the password on each server:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Reset Password** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select all the servers in the cell by using the left and right arrow buttons to move the name of the servers into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to display the **Reset Password** dialog.



7. In the **New Cell Password** field, enter the new password you want to use.
8. Press the **Set and Close** button to reset the password on the servers you selected. Make sure you do the next step.
9. Perform the Backup Cell task. For instructions, see "Backup Cell" on page 44.

Note: Use this new backup to restore the master server. Do not use an old backup that was created when the previous password was active. If you attempt to use an old backup the machine will not be able to communicate.

Synchronize Replicas

You should synchronize the replica servers at the following times:

- When a replica server has been irrevocably damaged and updates are pending on that replica.
- Every time you successfully add GSO servers.

- When a significant number of updates have been applied to the GSO data.
- Before taking down the master server for routine maintenance.

When you synchronize the servers, the following occurs as part of the process:

- The master server is tested to ensure it is in a steady state before beginning the synchronize process.
- The replica servers are synchronized.

You can use the TME scheduler to synchronize the servers on a regular basis during off-peak hours.

Use the following steps to synchronize the replica server:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Synchronize Replicas** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the replica servers you want to synchronize by using the left and right arrow buttons to move the name of the servers into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button.

Move Master Server

This task converts a GSO replica server into the GSO master server. You might want to use this task at one of the following times:

- When the GSO master server needs to be taken offline for maintenance purposes.
- When the GSO master server is permanently out of service.

The GSO Move Master Server task accomplishes the following as part of the process:

- Stops all GSO services.
- Synchronizes the master and the replica server. GSO attempts to synchronize all the replica servers in the GSO cell.
- Swaps the master server with the replica server.
- Starts all GSO services.

Note: When you move the master server to a replica server, the replica server becomes the new master server. The old master server becomes a replica server.

Use the following steps to move a master server:

1. Create or select a replica server.

2. Ensure that no updates are pending on either the master or the replica server.
3. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
4. Double-click on the **Move Master Server** icon to display the **Execute Task** window.
5. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
6. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
7. In the **Execution Targets** block, select the replica server you want to become the master server by using the left and right arrow buttons to move the name of the master server into the **Selected Task Endpoints** field.
8. Press the **Execute & Dismiss** button to display the **Move Master Server** dialog.



9. In the **Cell Password** field, enter the password for the GSO master server you want to move.
10. You can choose to remove any unavailable servers from the cell. However, before selecting the **Remove unavailable GSO servers from GSO cell** option keep the following in mind:
 - If you do not select this option and there is a GSO server in the GSO cell that is unavailable, this task will fail.
 - If you select this option and a GSO server is removed from the GSO cell, that server can not be used until you run the Recover Replica task to restore the machine to the cell.
 - If you select this option and the master server is out of service, you can still convert a replica server into a master server, but data could be lost if the replica has not been recently updated from the master server.
11. Press the **Set and Close** button to complete this task.

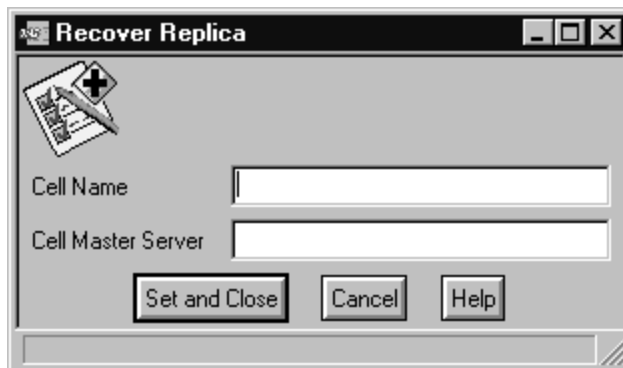
Recover Replica

You might want to recover a replica server at one of the following times:

- When the replica server data is damaged or not valid.
- When the replica server was down and now must be updated with new data.
- When a replica server was removed from the GSO cell during the Move Master Server task.

Use the following steps to recover the replica server:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Recover Replica** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Output Destination** block, select **Display on Desktop** if you want to display the task output on the desktop.
5. In the **Execution Targets** block, select the replica server you want to recover by using the left and right arrow buttons to move the name of the server into the **Selected Task Endpoints** field.
6. Press the **Execute & Dismiss** button to display the **Recover Replica** dialog.



7. In the **Cell Name** field, enter the name of the GSO cell you want to recover this replica.
8. In the **Cell Master Server** field, enter the name of the GSO master server for this cell.
9. Press the **Set and Close** button to complete this task.

Enable Integrated Login

Integrated login enables you to automatically sign on to GSO when you sign on to your desktop. You can run this task only on GSO clients.

Note:

- Before you run this task, make sure that your desktop password matches your GSO password.
- If you are using Smart Cards for GSO, the desktop password must match the Smart Card PIN.

Use the following steps to enable integrated logon:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Enable Integrated Login** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Execution Targets** block, select the client where you want to enable integrated login by using the left and right arrow buttons to move the name of the client into the **Selected Task Endpoints** field.
5. Press the **Execute & Dismiss** button to complete this task.

Disable Integrated Login

Use the following steps to disable integrated login:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Disable Integrated Login** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Execution Targets** block, select the client where you want to disable integrated login by using the left and right arrow buttons to move the name of the client into the **Selected Task Endpoints** field.
5. Press the **Execute & Dismiss** button to complete this task.

Enable Litronic Smart Card

If you are using Litronic Smart Cards to sign on to GSO, you must enable the Litronic Smart Card on each configured client. You can run this task only on GSO clients.

Use the following steps to enable Litronic Smart Cards:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Enable Litronic Smart Card** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Execution Targets** block, select the client where you want to enable Litronic smart Card support by using the left and right arrow buttons to move the name of the client into the **Selected Task Endpoints** field.
5. Press the **Execute & Dismiss** button to complete this task.

Disable Litronic Smart Card

Use the following steps to disable Litronic Smart Cards:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Disable Litronic Smart Card** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Execution Targets** block, select the client where you want to disable Litronic Smart Card support by using the left and right arrow buttons to move the name of the client into the **Selected Task Endpoints** field.
5. Press the **Execute & Dismiss** button to complete this task.

Enable Event Adapter

Use this task to enable the GSO event adapter to resume sending GSO messages to the Tivoli Enterprise Console. This task applies only to GSO servers and GSO database servers.

Use the following steps to enable event adapter:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Enable Event Adapter** icon to display the **Execute Task** window.
3. Press the **Execute & Dismiss** button to complete this task.

Disable Event Adapter

Use this task to disable the GSO event adapter from sending GSO messages to the Tivoli Enterprise Console. This task applies only to GSO servers and GSO database servers. Use the following steps to disable the event adapter:

1. From the **GSO Plus** window, double-click on the **GSO Administration Tasks** icon to display the **Task Library: GSO Administration Task** window.
2. Double-click on the **Enable Event Adapter** icon to display the **Execute Task** window.
3. Press the **Execute & Dismiss** button to complete this task.




Chapter 6. Resource Monitoring

GSO Plus provides the ability to monitor resources with TME 10 Distributed Monitoring. The GSO monitor profiles for TME 10 Distributed Monitoring are predefined to enable you to manage different aspects of the operating system, such as processes that are critical to the continued availability of the GSO application. These monitors allow you to quickly identify and respond to potential problems so that system downtime is avoided.

The GSO administrator must know about events that affect the availability of GSO for the users in that domain. For example, the administrator needs to know if a machine or a server is down, if disk space is low on a machine, or if a service has been affected by a particular event. The GSO monitor profiles help monitor the availability of GSO components with several availability management features.

Using GSO Plus Monitors

GSO comes with three types of monitor profiles:

Monitor	Icon
GSO Server Monitors	 GSO Server Monitors
GSO Database Server Monitors	 GSO Database Server Monitors
GSO UNIX Monitors	 GSO Unix Monitors

Use the following steps to modify the default subscription list of a particular monitor:

1. Select the **Subscribers...** option from the monitor profile's pop-up menu to display the **Subscribers** dialog.
2. In the **Available to become Subscribers** field, select the servers you want to receive the monitor profile by using the left and right arrow buttons to move the name of the server into the **Current Subscribers** field. (During the configuration process the appropriate subscribers are added to the subscription list.)
3. Press the **Set Subscription & Close** button.

To make the GSO monitors operational, you must distribute them using the subscription list you created. Use the following steps to distribute a monitor profile:

1. Select the **Distribute...** option from the monitor profile's pop-up menu to display the **Distribute Profiles** dialog.
2. Press the **Distribute Now** button. The monitor profiles are distributed to their default subscription lists.

Although the GSO monitor profiles come already defined to monitor resources specific to GSO, you can add monitors from other TME 10 Distributed Monitoring collections or delete monitors. You can also edit existing monitors to perform actions under different conditions. To edit the monitors in a monitor profile select **Properties...** from the monitor profile's pop-up menu.

Selecting the options on a particular monitor's pop-up menu displays the usual TME 10 Distributed Monitoring windows. For more information about these windows, see the TME 10 Distributed Monitoring documentation.

Viewing the Status of Monitored Resources

To view the status of the monitored resources, from the **Global Sign-On Plus for Tivoli** window, double-click on the **GSO Indicator Collection** icon.



The indicator on the thermometer rises as the status of a monitored resource becomes more urgent.

Open the **GSO Database Server Monitors**, **GSO Server Monitors**, or the **GSO UNIX Monitors** icon to view the status of the GSO resources. The monitored resource reports

only the most urgent status received within a recent time frame. The monitor reports are organized so that the most urgent status levels appear at the top of the report.

For more information on viewing the status of a monitored resource, see the TME 10 Distributed Monitoring documentation.

Monitored Resources

The following table indicates the resources that GSO monitors.

Monitored Resource	Reference
GSO Server Monitor Monitoring Profile	See "GSO Server Monitors Monitoring Profile" on page 63.
GSO Server Up	See "GSO Server Up" on page 63.
GSO Server Disk Space Used <code>-/var/gso</code>	See "GSO Server Disk Space Used - /var/gso" on page 64.
GSO Server Disk Space Used <code>-/opt/dcelocal/var</code>	See "GSO Server Disk Space Used - /opt/dcelocal/var" on page 64.
GSO Server File Size <code>-fatal.log</code>	See "GSO Server File Size - fatal.log" on page 65 .
GSO Server File Size <code>-error.log</code>	See "GSO Server File Size - error.log" on page 65 .
GSO Server File Size <code>-warning.log</code>	See "GSO Server File Size - warning.log" on page 66 .
GSO Server File Size <code>-notice.log</code>	See "GSO Server File Size - notice.log" on page 66 .
GSO Server File Size <code>-notice_verbose.log</code>	See "GSO Server File Size - notice_verbose.log" on page 67.
GSO Server File Size <code>-bin.log</code>	See "GSO Server File Size - bin.log" on page 68 .
GSO Server Audit Files Size <code>-gsod Audit Files</code>	See "GSO Server Audit Files Size - gsod Audit files" on page 68.
GSO Server Audit Files Size <code>-secd Audit Files</code>	See "GSO Server Audit Files Size - secd Audit files" on page 69.
GSO Server Checkpoint Space Available	See "GSO Server Checkpoint Space Available" on page 69.
Available Swap Space	See "Swap Space Available" on page 70.

Monitored Resource	Reference
GSO Database Server Monitors Monitoring Profile	See “GSO Database Server Monitors Monitoring Profile” on page 70.
GSO Server Up	See “GSO Server Up” on page 71.
GSO Server Disk Space Used -/opt/dcelocal/var	See “GSO Server Disk Space Used - /opt/dcelocal/var” on page 71.
GSO Server File Size -fatal.log	See “GSO Server File Size - fatal.log” on page 72 .
GSO Server File Size -error.log	See “GSO Server File Size - error.log” on page 72 .
GSO Server File Size -warning.log	See “GSO Server File Size - warning.log” on page 73 .
GSO Server File Size -notice.log	See “GSO Server File Size - notice.log” on page 73 .
GSO Server File Size -notice_verbose.log	See “GSO Server File Size - notice_verbose.log” on page 74.
GSO Server File Size -bin.log	See “GSO Server File Size - bin.log” on page 75 .
Available Swap Space	See “Swap Space Available” on page 75.
GSO UNIX Monitors Monitoring Profile	See “GSO UNIX Monitors Monitoring Profile” on page 76 .
Percent I-nodes Used	See “Percent I-nodes Used” on page 76.

GSO Monitor Probes

This section describes the new monitor probes defined in the GSO_Server_Monitors collection.

GSO Server Up

GSO Server Up checks whether a GSO server is up. A GSO server can consist of several server processes, some of which are DCE servers. This probe checks whether all the processes are up and functioning properly.

Command Line Format

serverUp

Arguments

NONE

Output One of the following string values are output:

up All the specified servers are up and listening.

down All the specified servers are NOT up.

TEC Event Class

GSOServerUp

GSO Server Disk Space Used

GSO Server Disk Space Used returns the percentage of disk space used on the specified disk. The probe provides support for specifying two parameters; one is used for a Windows NT file system, and one is used for a UNIX file system.

For all platforms, a directory name is specified. The directory and its location indicate the area of the system that the probe will check. On a UNIX system, the probe checks the file system where the specified directory is located. It returns the percentage of space used in the file system. On a Windows NT system, the probe checks the disk where the specified directory is located. It returns the percentage of disk space used.

Command Line Format

diskSpaceUsed -a UNIX Name -a NT Environment Variable

Arguments

UNIX Name

The name to use if this is a UNIX operating system.

NT Environment Variable

The name of the Windows NT environment variable that specifies which disk and directory to check.

Output The following number value is returned:

percentage

A number 0-100 that represents the percentage of space used in the location of the specified directory.

TEC Event Class

GSODiskSpaceUsed

GSO Server File Size

GSO Server File Size returns the size of the specified GSO Server file. This probe allows you to specify base directories for UNIX and Windows NT as separate arguments.

Command Line Format

fileSize -a UNIX Base Name -a NT Base Name -a File Name

Arguments

UNIX Base Name

The base directory name to check in a UNIX environment. The keyword "none" means there is no UNIX base name.

NT Base Name

The environment variable that contains the Windows NT base directory name.

File Name

The actual audit file name relative to the two base names specified.

Output The following number value is returned:

fileSize

The size of the specified files in Kbytes.

TEC Event Class

GSOServerFileSize

GSO Server Audit Files Size

GSO Server Audit Files Size returns the size of the specified GSO Server audit file, and all the backup files associated with that audit file. GSO Auditing, automatically moves audit files to backup files when those files get to a certain size. The backup files have the same name as the audit files, but have an extension indicating the time the files were archived.

Command Line Format

auditFilesSize -a *UNIX Base Name* -a *NT Base Name* -a *Audit File Name*

Arguments

UNIX Base Name

The base directory name to use in a UNIX environment.

NT Base Name

The environment variable which contains the Windows NT base directory name.

Audit File Name

The actual audit file name relative to the two base names specified.

Output The following number value is returned:

fileSize

The size of the specified files in Kbytes.

TEC Event Class

GSOAuditFilesSize

GSO Server Checkpoint Space Available

GSO Server Checkpoint Space Available calculates the percentage of required checkpoint space that is available. The checkpoint is performed by the DCE subsystem and requires enough space to copy some GSO/DCE databases. This probe first calculates how much disk space is available in the filesystem that DCE uses for data. It then calculates the amount of space required to perform a checkpoint. The value returned is the percentage of required space that is available.

Here is an example. If 40MB of space is required to perform a GSO/DCE checkpoint, and */var/dce* contains 80MB of free space, then 200% would be returned.

If this value is greater than 100%, then there is enough space available to perform a checkpoint. If the value is equal to or less than 100%, then there is not enough space to perform the checkpoint.

Command Line Format

checkpointSpaceAvailable

Arguments

NONE

Output The following number value is returned:

percentage

The percentage of space available compared to what is needed.

TEC Event Class

GSOCheckpointSpaceAvailable

GSO Server Monitors Monitoring Profile

This section describes the function of each GSO server status monitor. This Distributed Monitor Profile is designed to monitor a GSO server. For information on the new monitor probes defined for GSO see “GSO Monitor Probes” on page 60. For information on viewing a monitor’s status report, see “Viewing the Status of Monitored Resources” on page 58.

GSO Server Up

GSO Server Up checks to make sure the GSO processes on this server are up. This monitor runs every 15 minutes, and issues the **serverUp** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Is down/unavailable	Change icon Send TEC event
Severe	N/A	None
Warning	N/A	None
Reset	Becomes available	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server Disk Space Used - /var/gso

GSO Server Disk Space Used - /var/gso checks to make sure there is enough space in /var/gso. This monitor runs every 15 minutes, and issues the **diskSpaceUsed -a /var/gso -a IBMGSOPATH** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 95%	Change icon Send TEC event
Severe	Greater than 90%	Change icon Send TEC event
Warning	Greater than 85%	Change icon Send TEC event
Reset	Decreases below 85%	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server Disk Space Used - /opt/dcelocal/var

GSO Server Disk Space Used - /opt/dcelocal/var checks to make sure there is enough space in /opt/dcelocal/var. This monitor runs every 15 minutes, and issues the **diskSpaceUsed -a /opt/dcelocal/var -a DCELOC** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 95%	Change icon Send TEC event
Severe	Greater than 90%	Change icon Send TEC event
Warning	Greater than 85%	Change icon Send TEC event

Response Level	Trigger When	Default Actions
Reset	Decreases below 85%	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - fatal.log

GSO Server File Size - fatal.log returns the size of the GSO/DCE fatal.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/fatal.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - error.log

GSO Server File Size - error.log returns the size of the GSO/DCE error.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/error.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event

Response Level	Trigger When	Default Actions
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - warning.log

GSO Server File Size - warning.log returns the size of the GSO/DCE warning.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/warning.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - notice.log

GSO Server File Size - notice.log returns the size of the GSO/DCE notice.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/notice.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - notice_verbose.log

GSO Server File Size - notice_verbose.log returns the size of the GSO/DCE notice_verbose.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/notice_verbose.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - bin.log

GSO Server File Size - bin.log returns the size of the GSO/DCE bin.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/bin.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 10000KB	Change icon Send TEC event
Severe	Greater than 8000KB	Change icon Send TEC event
Warning	Greater than 6000KB	Change icon Send TEC event
Reset	Decreases below 6000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server Audit Files Size - gsod Audit files

GSO Server Audit Files Size - gsod Audit files return the size of the gsod Audit files. This monitor runs every 15 minutes, and issues the **auditFilesSize -a none -a IBMGSOPATH -a /var/gso/gsod/audit.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 10000KB	Change icon Send TEC event
Severe	Greater than 8000KB	Change icon Send TEC event
Warning	Greater than 6000KB	Change icon Send TEC event

Response Level	Trigger When	Default Actions
Reset	Decreases below 6000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server Audit Files Size - secd Audit files

GSO Server Audit Files Size - secd Audit files return the size of secd Audit files. This monitor runs every 15 minutes, and issues the **auditFilesSize -a /opt -a DCELOC -a /dcelocal/var/security/sec_audit_trail** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 10000KB	Change icon Send TEC event
Severe	Greater than 8000KB	Change icon Send TEC event
Warning	Greater than 6000KB	Change icon Send TEC event
Reset	Decreases below 6000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server Checkpoint Space Available

GSO Server Checkpoint Space Available checks that the GSO Server can perform checkpoint. This monitor runs every 15 minutes, and issues the **checkpointSpaceAvailable** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Less than 100%	Change icon Send TEC event

Response Level	Trigger When	Default Actions
Severe	Less than 120%	Change icon Send TEC event
Warning	Less than 140%	Change icon Send TEC event
Reset	Increases beyond 140%	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

Swap Space Available

Swap Space Available checks that the GSO server has enough swap space. This monitor probe is from the universal collection. This monitor runs every 15 minutes, and issues the **Universal/swapavail** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Less than 10MB	Change icon Send TEC event
Severe	Less than 15MB	Change icon Send TEC event
Warning	Less than 20MB	Change icon Send TEC event
Reset	Increases beyond 20MB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Database Server Monitors Monitoring Profile

This section describes the function of each GSO database server status monitor. This Distributed Monitor Profile is designed to monitor a GSO database server. It contains monitor instances specific to the resources on a machine with the GSO database servers on it.

For information on the new monitor probes defined for GSO see “GSO Monitor Probes” on page 60.

For information on viewing a monitor’s status report, see “Viewing the Status of Monitored Resources” on page 58.

GSO Server Up

GSO Server Up checks to make sure the GSO database processes on this machine are up. This monitor runs every 15 minutes, and issues the **serverUp** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Is down/unavailable	Change icon Send TEC event
Severe	N/A	None
Warning	N/A	None
Reset	Becomes available	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server Disk Space Used - /opt/dcelocal/var

GSO Server Disk Space Used - /opt/dcelocal/var checks to make sure there is enough space in /opt/dcelocal/var. This monitor runs every 15 minutes, and issues the **diskSpaceUsed -a /opt/dcelocal/var -a DCELOC** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 95%	Change icon Send TEC event
Severe	Greater than 90%	Change icon Send TEC event
Warning	Greater than 85%	Change icon Send TEC event

Response Level	Trigger When	Default Actions
Reset	Decreases below 85%	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - fatal.log

GSO Server File Size - fatal.log status the size of the GSO/DCE fatal.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/fatal.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - error.log

GSO Server File Size - error.log returns the size of the GSO/DCE error.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/error.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event

Response Level	Trigger When	Default Actions
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - warning.log

GSO Server File Size - warning.log returns the size of the GSO/DCE warning.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/warning.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - notice.log

GSO Server File Size - notice.log returns the size of the GSO/DCE notice.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/notice.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - notice_verbose.log

GSO Server File Size - notice_verbose.log returns the size of the GSO/DCE notice_verbose.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/notice_verbose.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 8000KB	Change icon Send TEC event
Severe	Greater than 6000KB	Change icon Send TEC event
Warning	Greater than 4000KB	Change icon Send TEC event
Reset	Decreases below 4000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Server File Size - bin.log

GSO Server File Size - bin.log returns the size of the GSO/DCE bin.log file. This monitor runs every 15 minutes, and issues the **fileSize -a /opt -a DCELOC -a /dcelocal/var/svc/bin.log** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 10000KB	Change icon Send TEC event
Severe	Greater than 8000KB	Change icon Send TEC event
Warning	Greater than 6000KB	Change icon Send TEC event
Reset	Decreases below 6000KB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

Swap Space Available

Swap Space Available checks that the GSO server has enough swap space. This monitor probe is from the universal collection. This monitor runs every 15 minutes, and issues the **Universal/swapavail** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Less than 10MB	Change icon Send TEC event
Severe	Less than 15MB	Change icon Send TEC event
Warning	Less than 20MB	Change icon Send TEC event

Response Level	Trigger When	Default Actions
Reset	Increases beyond 20MB	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO UNIX Monitors Monitoring Profile

This section describes the function of the GSO UNIX server status monitor. This Distributed Monitor Profile is designed to monitor a UNIX GSO server. You can distribute it to a GSO database server, or to a GSO server. Do not distribute it to a Windows NT GSO server.

Percent I-nodes Used

Percent I-nodes Used checks to make sure the GSO server directory has enough i-nodes. This monitor is UNIX specific. This monitor probe is from the UNIX collection. This monitor runs every 15 minutes, and issues the **Unix_Sentry/inodesusedpct -a /opt/dcelocal/var** monitor probe.

The following table lists the preconfigured actions for this monitoring source.

Response Level	Trigger When	Default Actions
Critical	Greater than 95%	Change icon Send TEC event
Severe	Greater than 90%	Change icon Send TEC event
Warning	Greater than 85%	Change icon Send TEC event
Reset	Decreases below 85%	Change icon Send TEC event
Normal	N/A	None
Always	N/A	None

GSO Automated Actions

The Tivoli Integration Toolkit automatically creates hidden task libraries for each Sentry Monitor Component defined in a Plus module. For GSO, the hidden tasks are in two of the task libraries: **GSO Server Monitors Tasks**, and **GSO UNIX Monitors Tasks**.

The monitors in the GSO Server Monitors and GSO Database Server Monitors Distributed Monitoring Profiles, use the tasks in the GSO Server Monitors Tasks task library. The monitors in the GSO UNIX Monitors Monitoring profile should use the GSO UNIX Monitors Tasks task library.

Tasks can also be run in reaction to events received from monitors in the monitoring profiles mentioned.

GSO Server Monitors Tasks

Restart Server

This task restarts the GSO server on a specified machine. This task first stops all the currently executing server processes and then restarts them. This task runs as a reaction to the "GSO Server Up" monitor probe or the event that is generated by that probe.

Arguments

None

Monitor Probes to Run From

GSO Server Up

Checkpoint Server

This task forces the GSO servers to perform a checkpoint. The DCE subsystem performs the checkpoint and requires enough space to copy some of the GSO/DCE databases to */opt/dcelocal/var*. The original databases reside in */opt/dcelocal/var* or on Windows NT in *\$dceloc/dcelocal/var*. The checkpoint operation accomplishes the following:

- Copies the databases to temporary files located in the same directory.
- Performs the checkpoint.
- Deletes the temporary files.

This task runs as a reaction to the "GSO Server Checkpoint Space Available" monitor probe or the event that is generated by that probe.

Arguments

None

Monitor Probes to Run From

GSO Server Checkpoint Space Available

Remove Log File

This task deletes a GSO log file on a specified host machine. The task first stops the currently executing GSO server processes, removes the log file, and then starts the GSO Server processes again. This task runs as a reaction to the "GSO Server File Size" monitor probe or the event that is generated by that probe.

Arguments

The arguments are set by the GSO Server File Size monitor.

Monitor Probes to Run From

GSO Server File Size

Remove Core Files

This task removes GSO server core files. GSO searches the file system `/opt/dcelocal/var` for core files, and removes the core files that are found. This task runs only on UNIX platforms and runs as a reaction to the "GSO Server Disk Space" monitor probe or the event that is generated by that probe.

Arguments

The arguments are set by the GSO Server Disk Space monitor.

Monitor Probes to Run From

GSO Server Disk Space

Remove Audit Log Files

This task removes GSO Server audit log files and all associated backup files. GSO auditing automatically moves audit files to backup files when those files get to a certain size. The backup files have the same name as the audit files, but have an extension that indicates the time the files were archived. **When this task is executed, all audit information is removed.** This task runs as a reaction to the "GSO Server Audit Files Size" monitor probe or the event that is generated by that probe.

Arguments

The arguments are set by the GSO Server Audit Files Size monitor.

Monitor Probes to Run From

GSO Server Audit Files Size

GSO UNIX Monitors Tasks

Clean Up Credentials

This task cleans up stale credential files and frees up i-nodes in a UNIX file system. This task runs only on AIX platforms and runs as a reaction to the "Percent I-nodes Used" monitor probe or the event that is generated by that probe.

Arguments

None

Monitor Probes to Run From

Percent I-nodes Used

Chapter 7. Enterprise Event Management

With the Tivoli Enterprise Console, GSO provides a set of filters for identifying events and a set of predefined correlation rules to automate the task of responding to specific events. An event is any significant change in the state of system resources or an application. In the case of GSO, an event is a change that affects GSO. An event can be starting or stopping a GSO process, successful completion of the GSO change password function, or when the server is unable to allocate more memory.

Using event management, you get predefined rules or automated responses to specific events, so that potential problems are identified and responded to before causing system downtime. For example, the Tivoli Enterprise Console can notify the system administrator of repeated process failures that can indicate a more severe problem with an application in the network.

The Tivoli Enterprise Console can also determine if a number of separate events are related to each other through a predefined rule that correlates the events and triggers; this is a response known as correlation activity. When a rule defines a response to a single event, this is known as an automated action. Some events do not require an automated response except for a message being displayed on the Tivoli Enterprise Console.

Configuration Activity

The following list describes the configuration tasks that are used to set up the Tivoli Enterprise Console to be used with GSO. These tasks are run on the Tivoli Enterprise Console server managed node and any GSO server managed nodes. GSO performs most of the set up activity automatically.

- **Tivoli Enterprise Console Server**

Using the **Set Up Event Server for GSO** icon, the Tivoli Enterprise ConsoleServer is set up to:

- Recognize and accept GSO events.
- Respond to GSO events according to the predefined rules.
- Notify the system administrator of the events received and the action taken.



Set Up Event Server for GSO

- **GSO Event Adapter**

Using the **Configure GSO Event Adapter** icon accomplishes the following configuration activity on a GSO server or GSO database server:

- GSO is configured to output events.
- The GSO event adapter is configured to recognize and forward GSO events to the Tivoli Enterprise Console.



Configure GSO Event Adapter

Setting Up the Tivoli Enterprise Console

Use the procedures in this section to set up the Tivoli Enterprise Console to receive GSO events. After completing the set up procedure for the Tivoli Enterprise Console, complete the procedure in “Configure the GSO Event Adapter” on page 84.

To set up the Tivoli Enterprise Console, select the **Run job...** option from the **Set Up Event Server for GSO** icon's pop-up menu. This action displays the **Set Up Event Server for GSO** dialog.

From the **Set Up Event Server for GSO** dialog you have two options; you can create a new rule base or adding to an existing rule base.

Creating a New Rule Base

New rule bases are created by copying (cloning) and modifying an existing rule. From the **Set Up Event Server for GSO** dialog, use the following steps to create a new rule base.

1. In the **New Rule Base Name** field, enter the name of the rule base you want to create.
2. In the **Rule Base to Clone** field, enter the name of the rule base to be copied.
3. In the **Path for New Rule Base** field, specify the path name to the directory on the Event Server in which you want to create the new rule base.

Note: The user ID corresponding to the TME Administrator must have write access to the specified path.

4. **Optional:** Use the **Name of Event Console to Configure** field to display GSO related events on a particular system administrator's event console. To make this assignment, enter the name that appears under the desired system administrator's event console icon.
5. Press the **Set And Close** button when finished.

Adding to an Existing Rule Base

From the **Set Up Event Server for GSO** dialog, use the following steps to add the specific rules for GSO to an existing rule base.

1. Select the **Add to Existing Rule Base** button. This action displays the **Existing Rule Base Name** field.



2. In the **Existing Rule Base Name** field, enter the name of an existing rule base that you want to modify to contain the GSO event classes and rules.

Note: It is not advisable to modify the **Default** rule base because it is the source used to create a new rule base.

3. **Optional:** Use the **Name of Event Console to Configure** field to display GSO related events on a particular system administrator's event console. To make this assignment, enter the name that appears under the desired system administrator's event console icon.
4. Press the **Set and Close** button when finished.

Configure the GSO Event Adapter

This task configures and starts the GSO event adapter to enable it to send GSO events from a GSO server or GSO database server to the TME 10 Enterprise Console Server. This task also modifies the DCE serviceability (SVC) routing file to enable appropriate routing of the SVC messages. For more information about SVC messages, see "SVC Event Class" on page 93.

The GSO Event Adapter is installed with the GSO server package. The event adapter needs to run on all GSO servers. Use the following steps to configure the GSO event adapter:

1. From the **GSO Plus** window, double-click **GSO Configuration Tasks** to display the **Task Library: GSO Configuration Tasks** window.
2. Double-click on the **Configure GSO Event Adapter** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Execution Targets** block, select the machines where the event adapter needs to be running by using the left and right arrow buttons to move the name of the machines into the **Selected Task Endpoints** field.
5. Press the **Execute & Dismiss** button to configure and start the GSO event adapter on the selected machine.

To make the changes to the event adapter take effect, you must restart the GSO servers. For instructions, see “Stop Server” on page 43, and “Start Server” on page 43.

To disable the event adapter, see “Disable Event Adapter” on page 55. To unconfigure the event adapter, see “Unconfigure GSO Event Adapter” on page 94.

Events and Rules

GSO configures the Tivoli Enterprise Console to receive events from GSO log files and Tivoli/Sentry. The Tivoli Enterprise Console classifies the events and then matches them against the rule base to see if the event has a predefined rule.

The following tables contain the Tivoli Enterprise Console events and rules.

GSO Server Monitor Events and Rules

The following table describes the events and rules that the event server uses when monitoring GSO servers. The GSO server monitors generate the events that these rules process. The term, slot, refers to one of the attributes of an event (e.g., the severity slot, the hostname slot).

GSO Server Monitor Events and Rules
<p>Event Class: GSOServerUp</p> <p>Event Response Level: reset (server up indication)</p> <p>Event Correlation: This is a GSO Up event. It is not duplicated and is CLOSED automatically when it is encountered. When the GSO Up event is encountered, any active GSO Down events, SVCEvent class events, and DCEInsufficientMemory class events are CLOSED that originated from the same host as the GSO Up event.</p>
<p>Event Class: GSOServerUp</p> <p>Event Response Level: critical (server down indication)</p> <p>Event Correlation: Duplicate GSO Down events are discarded and the repeat count is increased by one. If this Down event is not a duplicate event, then a 70 minute timer is started. If the time expires and the GSO Down event is still active and there is no active swapavail class event for the same host, the "Restart Server" task is executed to restart GSO on the corresponding host.</p> <p>Note: It is important not to have the GSOServerUp monitor poll interval set to more than an hour unless the 70 minute timer is also changed.</p>
<p>Event Class: GSDiskSpaceUsed GSOServerFileSize GSOAuditFilesSize GSOCheckpointSpaceAvailable Sentry2_0_indoesusedpct universal_swapavail</p> <p>Event Response Level: reset</p> <p>Event Correlation: All active events of the same event class from the same host and monitor are CLOSED. This does not apply to response levels of normal or always.</p>

GSO Server Monitor Events and Rules

Event Class:

GSODiskSpaceUsed
GSOServerFileSize
GSOAuditFilesSize
GSOCheckpointSpaceAvailable
Sentry2_0_indoesusedpct
universal_swapavail

Event Response Level:

warning, severe

Event Correlation:

All active events of the same event class, from the same host and monitor, of a higher response level are CLOSED. If an administrator has acted on the cause of a critical response level event, then the next time the monitor sent an event it could be of a different response level. In this case, a less severe event will CLOSE an older, more critical response level event.

Event Class:

GSODiskSpaceUsed
GSOServerFileSize
GSOAuditFilesSize
GSOCheckpointSpaceAvailable
Sentry2_0_indoesusedpct
universal_swapavail

Event Response Level:

normal, always

Event Correlation:

(NONE) Because none of these events are expected, they are allowed to accumulate. It is the administrator's responsibility to act on them.

GSO Server Monitor Events and Rules

Event Class:

GSODiskSpaceUsed
GSOServerFileSize
GSOAuditFilesSize
GSOCheckpointSpaceAvailable
Sentry2_0_indoesusedpct
universal_swapavail

Event Response Level:

warning, severe, critical

Event Correlation:

All duplicate events are discarded and the repeat count is increased by one. For the event to be a duplicate, the response_level, probe_arg, monitor, and hostname event slots must match.

Event Class:

GSODiskSpaceUsed (probe_arg = '/opt/dcelocal/var, DCELOC')

Event Response Level:

warning, severe, critical

Event Correlation:

If there is an active GSOServerFileSize event from the same host and there is no active swapavail class event for the same host, then the "Remove Log File" task is executed to remove the corresponding log file.

If there is an active non-FATAL GSOAuditFilesSize (probe_arg = '/opt, DCELOC, /dcelocal/var/security/sec_audit_trail') event from the same host, then the event's severity is changed to FATAL to draw an administrator's attention to it.

The GSOAuditFilesSize event by itself is relative to the disk space that you have available so one with a response level of critical might not be critical. However, if a GSODiskSpaceUsed event occurs in conjunction with a GSOAuditFilesSize event at any response level, the GSOAuditFilesSize event becomes more critical even if its response level was at the warning level.

GSO Server Monitor Events and Rules

Event Class:

GSODiskSpaceUsed (probe_arg = '/var/gso, IBMGSOPATH')

Event Response Level:

warning, severe, critical

Event Correlation:

If there is an active non-FATAL GSOAuditFilesSize (probe_arg = 'none, IBMGSOPATH, /var/gso/gsod/audit.log') event from the same host, then the event's severity is changed to FATAL to draw an administrator's attention to it.

The GSOAuditFilesSize event by itself is relative to the disk space that you have available so one with a response level of critical might not be critical. However, if a GSODiskSpaceUsed event occurs in conjunction with a GSOAuditFilesSize event at any response level, the GSOAuditFilesSize event becomes more critical even if its response level was at the warning level.

Event Class:

GSOCheckpointSpaceAvailable

Event Response Level:

warning, severe, critical

Event Correlation:

If there is an active GSOServerFileSize event from the same host and there is no active swapavail class event for the same host, then the "Remove Log File" task is executed to remove the corresponding log file.

If there is an active non-FATAL GSOAuditFilesSize (probe_arg = '/opt, DCELOC, /dcelocal/var/security/sec_audit_trail') event from the same host, then the event's severity is changed to FATAL to draw an administrator's attention to it.

The GSOAuditFilesSize event by itself is relative to the disk space that you have available so one with a response level of critical might not be critical. However, if a GSOCheckpointSpaceAvailable event occurs in conjunction with a GSOAuditFilesSize event at any response level, the GSOAuditFilesSize event becomes more critical even if its response level was at the warning level.

GSO Server Monitor Events and Rules
<p>Event Class: GSODiskSpaceUsed GSOFileSize GSOAuditFilesSize GSOCheckpointSpaceAvailable Sentry2_0_indoesusedpct universal_swapavail</p> <p>Event Response Level: severe, critical</p> <p>Event Correlation: If the event is not a duplicate, then all active events from the same host and monitor that have the same probe_arg slot and a smaller response level are CLOSED. In this case, the monitor has encountered a higher threshold condition.</p>
<p>Event Class: Sentry2_0_indoesusedpct</p> <p>Event Response Level: warning, severe, critical</p> <p>Event Correlation: If this event is not a duplicate, there is no active swapavail class event for the same host, and the probe_arg slot is '/opt/dcelocal/var', then the "Clean Up Credentials" task is executed on the same host where the event originated.</p>
<p>Event Class: GSODiskSpaceUsed</p> <p>Event Response Level: warning, severe, critical</p> <p>Event Correlation: If this event is not a duplicate event and there is no active swapavail class event for the same host, then the "Remove Core Files" task is executed on the same host where the event originated.</p>
<p>Event Class: GSOCheckpointSpaceAvailable</p> <p>Event Response Level: critical</p> <p>Event Correlation: If this is not a duplicate event, then the event's severity is set to FATAL. There is no longer enough room to initiate a GSO Checkpoint.</p>

GSO Server Monitor Events and Rules

Event Class:

GSOCheckpointSpaceAvailable

Event Response Level:

warning, severe

Event Correlation:

If this is not a duplicate event and there is no active swapavail class event for the same host, then the event cache is searched for a CLOSED GSOCheckpointSpaceAvailable event from the same host with a warning or severe response level that occurred in the last hour. If one is not found, then the "Checkpoint Server" task is executed on the same host where the event originated and the event is closed.

GSO DCE Serviceability Events and Rules

The following table describes the events and rules that the event server may use when monitoring GSO DCE serviceability events.

The GSO event adapters monitor GSO serviceability events, convert them to TEC events, and send them to the TEC server.

GSO DCE Serviceability Events and Rules

Event Class:

DCEInsufficientMemory

Event Severity:

fatal

Event Correlation:

Any of the DCE SVC memory-related events cause the DCEInsufficientMemory event to be generated by the rules. Because different DCE SVC events generate the event, it makes the processing of the different events that cover the same type of problem easier to handle. The DCE SVC event's hostname, origin, and sub_origin slots are propagated to the generated event. The DCE SVC message identifier and message text are placed in the dup_id_msg slot.

Any duplicate DCEInsufficientMemory event is discarded and the repeat count is increased by one. The duplicate event's dup_id_msg slot is appended to the original's dup_id_msg slot. This provides an audit trail of the events associated with the DCEInsufficientMemory event.

GSO DCE Serviceability Events and Rules	
<p>Event Class: DCEPotentialSecViolationAttempt</p> <p>Event Severity: fatal</p> <p>Event Correlation: Since the original WARNING DCEPotentialSecViolationAttempt event was encountered, it has been duplicated at least 5 times within a 15 minute time period. An administrator must CLOSE this event when the condition has been investigated satisfactorily.</p>	
<p>Event Class: GSORootSignonFailureAttempt</p> <p>Event Severity: warning</p> <p>Event Correlation: The GSO SVC event, sso_s_not_root (0x1735E038), will cause the rules generated event, GSORootSignonFailureAttempt, to be generated. The event is CLOSED if after 15 minutes less than 5 duplicates have been encountered.</p>	
<p>Event Class: GSORootSignonFailureAttempt</p> <p>Event Severity: fatal</p> <p>Event Correlation: Since the original warning GSORootSignonFailureAttempt event was encountered, it has been duplicated at least 5 times within a 15 minute time period. An administrator must CLOSE this event when the condition has been investigated satisfactorily.</p>	
<p>Event Class: SVCEvent</p> <p>Event Severity: harmless, warning, critical, fatal</p> <p>Event Correlation: The duplicate event is from the same host, has the same SVC message ID and severity, and has the same svc_src_file, svc_src_line, svc_component, and svc_sub_component slot values. All duplicates are discarded and the repeat count is increased by one.</p>	

Summary of GSO Monitor Event Classes

You can use this table to reference the event classes. These event classes are used by the GSO Server Monitor Events and Rules.

Monitor Name	Event Class
GSO Server Up	GSOServerUp
GSO Server Disk Space Used	GSODiskSpaceUsed
GSO Server File Size	GSOServerFileSize
GSO Server Audit Files Size	GSOAuditFilesSize
GSO Server Checkpoint Space Available	GSOCheckpointSpaceAvailable

SVC Event Class

The SVC Event Class was designed to map a DCE SVC message into a TME 10 Enterprise Console (T/EC) event. For more information on DCE SVC messages, see the *OSF DCE Application Development Guide*.

The SVC Event Class defines the format of the GSO event. GSO events appear on the TME 10 Enterprise Console with the following attributes:

source Identifies the source of this event. For DCE SVC events, the string value will always be DCEServiceability.

sub_source

A more detailed description of where the event was generated. It can be DCERules or GSORules. DCERules and GSORules indicate it was generated by the respective predefined rules. Otherwise, it was generated by the GSO event adapter.

svc_time

The time stamp in UTC format of when the event occurred.

svc_process_ID

The process ID or program name of the program that issued the SVC event.

svc_severity

The SVC severity level. It can be FATAL, ERROR, WARNING, NOTICE, or NOTICE_VERBOSE.

svc_component

The name of the DCE component that issued this SVC message.

svc_sub_component

The name of the DCE subcomponent that issued this SVC message.

svc_src_file

The name of the source file that issued this SVC message.

svc_src_line	The name of the source line in the source file that issued this SVC message.
svc_thread_ID	The threadID of the thread in the process that issued the SVC message.
svc_msg_ID	The message ID that uniquely defines this SVC message.
msg	The actual text for this SVC message.
hostname	The name of the system on which the event occurred.
origin	The IP address of the resource that generated the event.
sub_origin	The name of the DCE cell this host belongs to.
severity	svc_severity mapped to an appropriate Tivoli severity. The mapping is as follows:
svc_severity	severity
FATAL	FATAL
ERROR	CRITICAL
WARNING	WARNING
NOTICE	HARMLESS
NOTICE_VERBOSE	HARMLESS

Unconfigure GSO Event Adapter

Use the following steps to unconfigure the GSO event adapter:

1. From the **GSO Plus** window, double-click **GSO Configuration Tasks** to display the **Task Library: GSO Configuration Task** window.
2. Double-click on the **Unconfigure GSO Event Adapter** icon to display the **Execute Task** window.
3. In the **Timeout** field of the **Execution Parameters** block, change the default timeout value to 0.
4. In the **Execution Targets** block, select all the machines where the event adapter needs to be running by using the left and right arrow buttons to move the names of the machines into the **Selected Task Endpoints** field.
5. Press the **Execute & Dismiss** button to display the **Unconfigure GSO Event Adapter** dialog.

To make the changes to the event adapter take effect, you must restart the GSO servers. For instructions, see “Stop Server” on page 43, and “Start Server” on page 43.

Appendix A. Installing Smart Card Administration

GSO supports Litronic smart cards that use the PKCS#11 interface.

Before attempting to install the Smart Card Administration software make sure you review the following prerequisites:

- You must have a GSO client installed and configured on the same machine where you plan to install the Smart Card Administration software.
- You must use the TME user interface to create a GSO user as a security officer.
- You must install and configure the smart card hardware before following the steps below. See your vendor's directions for installing the smart card hardware.

Use the following steps to install the Smart Card Administration software:

1. Insert the CD labeled **CD-ROM 2 (Windows NT/95 Client)** into your CD-ROM drive.
2. At a command prompt, type:

```
x:  
cd \scadm
```

where x is your CD-ROM drive.

3. Type setup and follow the instructions.
4. Restart your computer to activate the installation.

Appendix B. Installing the Client Machine Without Software Distribution

If a client machine does not have Tivoli Software Distribution installed, use the following procedure to install and configure the client machine.

Installing the GSO Client 2.0 on Windows NT/95

The GSO client software for Windows NT and Windows 95 requires that you must first install the Dascom IntraVerse NetSEAT DCE client.

Use the following steps to install a DCE client:

1. Insert the CD labeled **CD-ROM 2 (Windows NT/95 Client)** into your CD-ROM drive.
2. At a command prompt, type:

```
x:  
cd \dce
```

where x is your CD-ROM drive.

3. Type setup and follow the instructions.
4. Restart your computer to activate the installation.

When you are installing the GSO client on Windows NT, you can use either the File Allocation Table (FAT) file system or the New Technology File System (NTFS). However, the NTFS provides better security and data integrity because it enforces stricter file access.

Notes:

1. If you are planning to also install the GSO server on the same Windows NT machine, you must select a drive formatted with NTFS.
2. Make sure you are logged on the Windows NT machine with administrator privileges.

Use the following steps to install the Windows NT and Windows 95 client:

1. Insert the CD labeled **CD-ROM 2 (Windows NT/95 Client)** into your CD-ROM drive.
2. Do one of the following:

- At a Windows NT command prompt, type:

```
x:  
cd \gso\nt
```

- At a Windows 95 command prompt, type:

```
x:  
cd \gso\w95
```

where x is your CD-ROM drive.

3. Type setup and follow the instructions.
4. Restart your computer to activate the installation.

Use the following steps to install the database:

1. Insert the CD labeled **CD-ROM 2 (Windows NT/95 Client)** into your CD-ROM drive.
2. At a command prompt from the CD-ROM drive, do one or more of the following:
 - For CTLIB, type:
`cd \db\ctl1ib`
 - For OCI, type:
`cd \db\oci`
 - For ODBC, type:
`cd \db\odbc`
3. Type setup and follow the instructions.
4. Restart your computer to activate the installation.

Installing the GSO Client 1.5 on OS/2 Warp

The GSO 1.5 client software for OS/2 must be installed on OS/2 Warp Version 3.0 (or higher) and requires that you first install the IBM DCE Client Including DFS, Version 4. For instructions on how to install and configure the DCE client, refer to the *IBM DCE for OS/2 Warp: Getting Started* online book. For a listing of all the DCE documents, see "Online Information" on page 105.

To install the OS/2 GSO client:

1. Select the appropriate OS/2 CD. If the language of your choice is not available, use the English version.
2. Insert the CD labeled **CD-ROM 3 (OS/2 Client)** into your CD-ROM drive.
3. At a command prompt, type:
x:
`cd \gso\<language>`

Where x is your CD-ROM drive, and <language> is one of the following:

- de_de for German
 - en_us for U.S. English
 - es_es for Spanish
 - ja_jp for Japanese
 - ko_kr for Korean
 - pt_br for Brazilian Portugese
 - zh_cn for Simplified Chinese
 - zh_tw for Traditional Chinese
4. Type `install` and follow the instructions.
 5. Restart your computer to activate the installation.

Configuring the GSO Client 2.0 on Windows NT/95

Use the **cfgclient** command to configure the GSO 2.0 client. You can also use the **cfgclient** command to:

- Set up the DCE configuration.
- Enable or disable integrated login.
- Set up GSO to use a device, such as smart card for user authentication.

The syntax for the client configuration command follows.

cfgclient -config

Purpose

Use this option to configure the GSO client. All of the flags are required.

Format

```
cfgclient -config -cell cellname -servers hostname [hostname] [hostname]
```

Flags

-cell *cellname*

Use this flag to specify the name of the GSO cell where the GSO servers are located.

-servers *hostname*

Use this flag to specify the TCP/IP host name of the GSO server. At least one and up to three names can be specified in GSO. You must have GSO installed on each host system that you name. The first host name that you specify will be used as the primary server and the second and third host name will be used as the backup servers. Each specified server must have a DCE DTS and a security server configured. You can use an IP address as the name of a server.

Privilege Required

On Windows NT, you must be a member of the Administrators group.

Exit Status

0 Successful completion

>0 An error occurred

Examples

For example, you want to configure the client into cell abcCell. At the command line you would enter:

```
cfgclient -config -cell abcCell -servers abc def
```


cfgclient -login

Purpose

Use this option to enable or disable integrated login.

Format

cfgclient -login integ|nointeg

Flags

integ Use this flag to enable integrated login.

nointeg Use this flag to disable integrated login.

Privilege Required

On Windows NT, you must be a member of the Administrators group.

Exit Status

0 Successful completion

>0 An error occurred

Examples

For example, you want to enable integrated login on a client machine. At the command line you would enter:

```
cfgclient -login integ
```

cfgclient -logindev

Purpose

Use this option to specify an authentication device, such as a smart card, to be used by a GSO workstation. The device support, both hardware and software must be installed and properly configured; otherwise, users will not be able to log in to GSO. This command registers only the module containing the interfaces that GSO will use to interact with the device. No error is returned by this command if the library module cannot be loaded. These failures are detected at the time the user tries to use the device to log in to the workstation.

Note: Before you use this option, the smart card hardware must already be installed and configured. For more information, see "Appendix A. Installing Smart Card Administration" on page 95.

Format

```
cfgclient -logindev none|-library dll name [-description description]
```

Flags

none Use this flag when no special device is attached. Use default authentication.

-library *dll name*

Use this flag to specify the full path and name of the DLL that contains the authentication functions that are called by GSO to authenticate the user. If a full path is not specified, the DLL must be in a directory in the Windows path environment variable.

[*description description*]

Use this flag if you want to include a description of the device. If the description contains blanks, then the entire description must be enclosed in double quotation marks ("").

Privilege Required

On Windows NT, you must be a member of the Administrators group.

Examples

The following is an example of how to use the **cfgclient** command to specify smart card support from XYZ Corp.

```
cfgclient -logindev -library c:\ibmgso\bin\litronsc.dll  
-description "SmartCard for Litronic."
```

where *c:\xyzCorp\bin\smartcard.dll* is the full path and name of the DLL containing the authentication functions. For information about the module that is compatible with IBM GSO client, contact the vendor of the authentication device.

cfgclient -view

Purpose

Use this option to display the current configuration for the client. Items that are not configured are shown with a value of < >. Configuration information is written to **stdout**.

Format

cfgclient -view

Flags

-view Specify this flag to display the current configuration for the client.

cfgclient -?| -h

Purpose

Use this option to display the online help containing the command syntax.

Format

cfgclient -? | -h

Flags

-?| -h Specify this flag to display the online help for this command.

DCE for OS/2 Warp Client Information

The following books contain information about the DCE Version 4 for the OS/2 release:

Online Information

The following online books are installed with the OS/2 Warp DCE Client package in the `lopt\dcelocal\books` directory. They can be viewed from the CD before installation by typing `view filename` while in the `\pubs` directory on the OS/2 GSO Client CD.

dcegetst.inf

IBM DCE for OS/2 Warp: Getting Started

dceadmin.inf

IBM DCE for OS/2 Warp: Administration Guide

dceadcmd.inf

IBM DCE for OS/2 Warp: Administration Commands Reference

dcedfscl.inf

IBM DCE for OS/2 Warp: Distributed File Service Client Guide and Reference

dceerrmsg.inf

IBM DCE for OS/2 Warp: Error Messages Manual

Printable Documentation

The following books are printable in PostScript format from the `\pubs\ps` directory on the OS/2 GSO Client CD for customers who prefer printed documentation.

dcegetst.ps

IBM DCE for OS/2 Warp: Getting Started

dceadmin.ps

IBM DCE for OS/2 Warp: Administration Guide

dceadcmd.ps

IBM DCE for OS/2 Warp: Administration Commands Reference

dcedfscl.ps

IBM DCE for OS/2 Warp: Distributed File Service Client Guide and Reference

Appendix C. GSO Database-Specific Configuration

IBM Global Sign-On for Multiplatforms, V2.0 supports the Microsoft Open Database Connectivity (ODBC), the Oracle Call Interface (OCI), and the Sybase CT-LIB interface (CT-LIB). After GSO authenticates a user, that user can connect to the supported databases without having to log on again. The following steps summarize the database connection process:

1. Using a client application, the GSO user initiates a connection request to a supported database server.
2. The GSO database client looks up the location of the GSO database server that provides access to the specified database server. This action is transparent to the client user.
3. Because GSO has already authenticated the user, the GSO database server connects to the specified database server without requiring a user ID or password.
4. The GSO database client sends a Remote Procedure Call (RPC) to the appropriate database server.
5. A local database call is sent to the Relational Database Management System (RDBMS) on behalf of the client application.
6. When the RPC completes, the RDBMS passes return values to the GSO database client.
7. The GSO database client passes those values to the client application.

GSO provides a Windows NT and Windows 95 database client for each of the supported database servers listed in the following table:

Table 1. Supported GSO Databases

Supported GSO Database Server Products	Supported Operating Systems		
	AIX	Solaris	WinNT
Oracle (OCI/ODBC)	Available	Available	Available
Sybase (CT-LIB)	Available	Available	N/A
DB2 (ODBC)	Available	Available	N/A
Informix (ODBC)	Available	Available	N/A
Microsoft SQL Server (ODBC)	N/A	N/A	Available

This appendix explains how to configure database-specific information after GSO Plus installs and configures the GSO database servers and clients. See the product README for platform-specific supported versions.

Configuring ODBC

This section describes how to configure the Microsoft Open Database Connectivity (ODBC) server and client database.

The GSO ODBC database server uses the Microsoft ODBC to access one or more databases. The GSO database client is an ODBC driver implemented as a dynamic link library (DLL) on Windows clients. The GSO database server accepts requests from the GSO database client and passes them to the appropriate ODBC database server.

Configuring ODBC on AIX and Solaris Servers

The gsodb login account is created during the ODBC database-server installation.

- You must set a gsodb account password.
- To set a password for the gsodb account, you must have root permission.

The following files are created on AIX and Solaris during the database server installation process:

- `.odbc.db2.sh` — setup script for the DB2 database server.
- `.odbc.infx.sh` — setup script for the Informix database server.
- `.odbc.ora.sh` — setup script for the Oracle database server.

Edit these files to uncomment and set your environment-specific variables. GSO Plus uses these *.sh files (depending on your database server: `.odbc.db2.sh`, `.odbc.infx.sh`, or `.odbc.ora.sh`) to start the database server processes. The files are created in the gsodb user's home directory. Each shell script defines the platform-specific environment variables required to run the various database servers. For example, after you run these scripts, they set the path for the `OH_HOME` and `ODBCHOME` environment variables (the `OH_HOME` and `ODBCHOME` environment variables are referenced throughout this appendix).

After you set your environment variables and configure your `.ini` file parameters and ODBC drivers, return to the GSO Administration Tasks window and select the icon called Start Server to start your server processes (see "Starting the Database Servers" on page 116 and "Starting the Database Servers" on page 122).

Before starting a ODBC database server, edit the `ohodbc.ini` file in the `$OH_HOME/admin` home directory. This is one of the files that was installed with the database server. The `ohodbc.ini` file is the initialization file for the ODBC database.

Locating the ohodbc.ini File

When an ODBC database server starts, it looks for the `ohodbc.ini` file in the current directory. If it does not find the `.ini` file, it looks for it in the `$OH_HOME/admin` directory. If it does not find the file there, the server will not start, and will print a message to the screen that reads `Cannot find environment file or registry.`

Setting Server Configuration Parameters

The following configuration parameters control the behavior of the database server. These parameters are contained in the `ohodbc.ini` file. An ODBC database server reads these parameters when it is initialized. Do not change these parameters while your database server is running. You can edit the `ohodbc.ini` file directly with `vi`, or any other UNIX editor. The parameters and valid setting values are described below.

OH_CDS_NAME

Set this required parameter to the name that will be used to identify the database. This is also the name that the database server uses to register itself in the Cell Directory Service.

OH_DBNAME

Set this required parameter to the ODBC data source name required to connect to the database. The OH_DBNAME must be different from the OH_CDS_NAME. The OH_DBNAME must correspond to an entry in your ODBC driver's .odbc.ini file. (Note that the ODBC driver's initialization file is .odbc.ini, while the database server's file is ohodbc.ini. The .odbc.ini file defines ODBC data sources and is located in the ODBCHOME directory.)

OH_DB_ADMIN

The principal that the database server uses to log in to the database. This principal needs to have the privilege to alter other user's passwords. For Oracle databases you can use either a valid user name or a forward slash (/). This parameter is not used with Informix databases. See "Implementing Database-Specific Configurations" on page 114.

OH_DB_ADMIN_PASSWORD

This parameter is the password for the OH_DB_ADMIN principal.

OH_DB_ALTER_PASSWORD

This parameter contains the command to change user's passwords. This enables proxy logins. The command contains placeholders for the user name and password, represented by %1 and %2. See the sample in the ohodbc.ini file. This parameter is used with Oracle databases. Use the following command for Oracle: "alter user %2 identified by %1".

OH_ENFORCE_PROXY_LOGIN

If this optional parameter is set to TRUE (default), the database server accepts *only* proxy logins from client workstations. See "Setting Proxy Logins" on page 121. The client's user name can be a forward slash (/) or left empty. Any supplied password is ignored.

If this parameter is set to FALSE, the database server can accept either proxy logins or regular database logins. The client's user name can be either a forward slash (/) (which is interpreted as a proxy login, and any supplied password is ignored) or *<user name>* (which is interpreted as a regular database user name; the client must provide a valid password).

Note: When using the ODBC database server with DB2 or Informix, the ODBC performs as if OH_ENFORCE_PROXY_LOGIN is set to TRUE. Setting this parameter to FALSE has no effect.

OH_PROXYPREFIX

OH_PROXYPREFIX should be used *only* when connecting to an Oracle database. Use this optional configuration parameter to set the proxy prefix. The default value is NULL. For example, if this parameter is set to the default Oracle prefix "ops\$," then users will connect to a database account of *ops\$ <principal_name>*.

OH_MAXSVR

This optional parameter is an integer value that specifies the maximum number of concurrent replica processes (threads). The default is 100.

OH_PROTN

This optional parameter sets the minimum level of protection that a client can request for all RPCs associated with a server. These protection levels are CONNECT, CALL, PKT, PKT_INTEGRITY, PKT_PRIVACY. See "Setting Protection Levels" on page 119 for details.

OH_TRACE

This is an optional parameter that is typically set to FALSE or not at all. If it is set to "0xffffffff" then the server will write information to a trace file in the same directory in which the server is running. The trace file will have a ".trc" extension. This trace file can be useful for support personnel to help isolate and fix problems. When a problem has been resolved, be sure to disable tracing by setting it to FALSE or removing this parameter. Tracing will slow performance, and over time the trace files might grow large.

The ohodbc.ini file contains sample values for these parameters. You can edit these parameters directly with vi or any other text editor.

Editing the ohodbc.ini File: When editing the ohodbc.ini file, take care to preserve the proper format of this file. The ohodbc.ini file contains lines that have the following format:

<parameter> = value

Example:

OH_TRACE = 0xffffffff

If the value for a parameter contains a space, the entire value must be enclosed in double quotation marks, as follows:

<parameter> = "current value"

Each parameter/value pair should be on a separate, single line.

Use the pound character (#) in the first column to indicate a comment, or to disable a parameter.

Example:

```
#OH_TRACE = 0xffffffff
```

The name of the parameter is *not* case sensitive; however, the value of the parameter is case sensitive.

Configuring the ODBC Server Environment

When you access an ODBC data source, the client application sends a call through the ODBC client to the ODBC server. The server passes the call through the ODBC driver associated with the desired data source. The data source then returns data or confirmation to the client application. The GSO database product includes various ODBC drivers from Intersolv.

Configuring ODBC Drivers: There is a specific server-resident ODBC driver for each database. Use the following steps to configure a ODBC database server to use a server-resident ODBC driver:

1. Configure an ODBC data source on the server.
2. Set the ODBC database server to use the ODBC data source.

The method for configuring an ODBC data source will vary depending on your target database and platform.

Use the following steps to configure your ODBC environment:

1. Perform database-specific ODBC driver post-installation steps.
If you use the Oracle 7 ODBC driver, link the driver with some Oracle libraries. Refer to the steps in "Linking the Oracle ODBC Driver" on page 112.
If you use the DB2 ODBC driver, bind some packages in your DB2 database. Refer to the steps in "DB2 ODBC Driver Post-Installation Steps" on page 112.
2. Edit the `.odbc.ini` file.
To use an ODBC driver, an ODBC data-source name (DSN) must be defined in the `.odbc.ini` file. A DSN defines a particular driver to be used along with various attributes that define how a connection should be made.
The ODBC driver manager consults the `.odbc.ini` file located in the current user's home directory when it attempts to connect to an ODBC DSN. There is a sample `$ORACLE_HOME/.odbc.ini` file. Refer to "Configuring the `.odbc.ini` File" on page 113.
3. Test a connection to an ODBC data source.

Before starting a database server that has been configured to use a particular ODBC data source, it is good practice to test that a connection can be made to that data source with a sample application.

There is a demo \$ORACLE_HOME/demo that allows you to test a connection to an ODBC data source. Refer to the read.me file to run this application.

Linking the Oracle ODBC Driver: The Oracle 7 ODBC driver requires one-time site linking to build an Oracle SQL*Net driver on AIX. This site linking binds your unique Oracle SQL*Net configuration into the file, which is used by the Oracle drivers to access the local databases.

1. Before you build the Oracle SQL*Net DLL, install Oracle and set the environment variable ORACLE_HOME to the directory where you installed Oracle.
2. A make file is provided that builds the Oracle SQL*Net driver. This make file is in the \$ORACLE_HOME/bin directory. The Oracle SQL*Net driver should be either built-in or copied to the \$ORACLE_HOME/d11s directory where the other Intersolv ODBC DLLs are installed.
3. The following example builds the Oracle SQL*Net driver if you are in the \$ORACLE_HOME/bin directory:

```
% make -f .jqeora7.mk EXE=../dlls
```

The EXE= directive builds the Oracle SQL*Net DLL in the location you specify.

For Oracle 7.2 and 7.3 Users: If you use Oracle 7.2, build the Oracle SQL*Net driver using the qeora72.mk file. For example, if you are in the \$ORACLE_HOME/bin directory, you would run the following command:

```
% make -f .jqeora72.mk EXE=../dlls for Oracle 7.2
```

```
% make -f .jqeora73.mk EXE=../dlls for Oracle 7.3
```

DB2 ODBC Driver Post-Installation Steps: Before you can access a table with the DB2 ODBC driver, bind the driver to the database. Bind the driver to every database you intend to access. Run the bind files in the \$ORACLE_HOME/d11s directory with a file extension of ".bnd".

To use the bind files:

1. Become the DB2 user.
2. Use the "db2" utility while you are the operating system ID of the owner of the database.

Refer to the following example:

```
db2> connect to <database>
db2> BIND qecsv1.bnd BLOCKING ALL GRANT <authorization_list>
db2> BIND qerrv1.bnd BLOCKING ALL GRANT <authorization_list>
db2> BIND qeurv1.bnd BLOCKING ALL GRANT <authorization_list>
```

```
db2> BIND qecswhv1.bnd BLOCKING ALL GRANT <authorization_list>
db2> BIND qerrwhv1.bnd BLOCKING ALL GRANT <authorization_list>
db2> BIND qeurwhv1.bnd BLOCKING ALL GRANT <authorization_list>
```

Note: *<authorization_list>* is a list of comma-separated authorization IDs, group IDs, or PUBLIC (if you want to grant access to all users).

This sets the DB2 environment.

Configuring the .odbc.ini File: The `.odbc.ini` file is a plain text file that stores ODBC configuration information. The `.odbc.ini` file defines data source entries.

UNIX (AIX and Solaris) support of the database drivers also allows the use of a centralized `.odbc.ini` file that a system administrator can control. This is accomplished by setting the environment variable `ODBC_INI` to point to the fully qualified name of the centralized file. The `ODBC_INI` variable is set in the `.odbc.*.sh` files.

By default, Intersolv will look for the `.odbc.ini` file in the user's `$HOME` directory. If users have a private copy of `.odbc.ini` in their `$HOME` directory, this copy is used instead of the centralized version, regardless of the value of the `ODBC_INI` environment variable.

For every driver you want to use, at least one data source must be defined. Use any plain text editor (`vi`, for example) to edit the `.odbc.ini` file and define the data sources you need there.

The `.odbc.ini` file has the following structure:

```
[ODBC Data Sources]
```

```
<ds_name1> = description
```

```
<ds_name2> = description
```

```
[ds_name1]
```

```
Driver = <path/dll>
```

```
[ds_name2]
```

```
Driver = <path/dll>
```

The [ODBC Data Sources] Section

The [ODBC Data Sources] section is mandatory. It provides the Driver Manager with a list of data sources that are supported for your connection requests. You can change the names in this list, but each entry must match an entry in the [ds_name] section in this file.

The [ds_name] Section

The [ds_name] section contains Driver specifications that point to the location of the installed driver, as well as a Description specification that describes the driver. If you change the location of a driver, change the Driver specification to match the new location, or you can use just the name of the driver and the driver manager will attempt to locate the driver in your shared library path. (This variable is LIBPATH on AIX platforms and LD_LIBRARY_PATH on Solaris platforms.)

You might need to assign other entries depending on the driver that is being configured. In the man page for each driver, see the ATTRIBUTES section for a list of entries supported for data sources. Setting these attributes in the .odbc.ini file changes their default settings.

Note: In the .odbc.ini file, you are required to use the long name of these attributes.

Comments in the .odbc.ini File

You can add comments, or comment out existing lines, in the .odbc.ini file by starting the line with a semicolon (;).

Implementing Database-Specific Configurations

The following sections detail database configurations for different databases. These are arranged alphabetically.

DB2 Databases:

- GSO user IDs are created for every operating system account that will be used to connect to DB2.
- Proxy logins are automatically enforced for DB2 databases. See “OH_ENFORCE_PROXY_LOGIN” on page 109.

When the ODBC database server receives a request to connect, it will spawn a new process and set its `userid` to the GSO user ID that initiated the connection request. If the `userid` does not have privileges to connect to DB2, the connection will be rejected.

Set OH_DBNAME: A DB2 RDBMS must be running and an ODBC data source must be configured, before the ODBC database server can connect to the DB2 RDBMS. Set the `OH_DBNAME` in the `ohodbc.ini` file to the name of the ODBC data source that maps to the DB2 RDBMS.

DB2 Environment: For DB2, set the following environment variables for the user who starts the ODBC database server:

- `DB2INSTANCE` = the DB2 instance name.
- `DB2DBDFT` = the DB2 Database Default.
- `DB2DIR` = the directory where DB2 is installed.

Set these variables in the `.odbc.db2.sh` file and verify that you can connect directly to DB2 using the **db2** command line tool. Refer to your DB2 documentation.

Informix Databases:

- GSO user IDs are created for every operating system account that will be used to connect to Informix.
- Proxy logins are automatically enforced for Informix databases.

When the ODBC database server receives a request to connect, it will spawn a new process and set its `userid` to the GSO user ID that initiated the connection request. If the `userid` does not have privileges to connect to Informix, the connection will be rejected.

Set `OH_DBNAME`: An Informix RDBMS must be running, and an ODBC data source must be configured, before the ODBC database server can connect to the Informix RDBMS. Set the `OH_DBNAME` in the `ohodbc.ini` file to the name of the ODBC data source that maps to the Informix RDBMS.

Informix Environment: For Informix, set the following environment variables for the user who starts the ODBC database server:

- `INFORMIXDIR` = the location where Informix is installed.
- `INFORMIXSERVER` = the Informix server name.
- `ONCONFIG` = the configuration file name associated with the Informix server.
- `SQLEXEC` = the location of the relay module.

Set these variables in the `.odbc.infx.sh` file and verify that you can connect directly to Informix with the `dbaccess` command line tool. Refer to your Informix documentation.

Creating a Special Oracle Account: Before the ODBC database server can implement the proxy login security features, there must be an Oracle account with the "alter user" privilege. This account name is specified by the `OH_DB_ADMIN` configuration parameter. The following two sections describe two ways to accomplish this task.

First Method:

By creating this account as an externally authenticated account you can set the `OH_DB_ADMIN` parameter to a forward slash (/). In this way you do not have to set the password in the `OH_DB_ADMIN_PASSWORD` parameter.

Use the following steps to create an externally identified database account:

1. Determine the `OS_AUTHENT_PREFIX` parameter for your database. This parameter is defined in your `init<sid>.ora` file. The default is `ops$`. If your `OS_AUTHENT_PREFIX` is not `ops$`, replace every occurrence of `ops$` in the SQL*DBA commands below with your prefix. (You can use any tool that accesses the SQL command line, such as SQL*DBA or SQL*Plus.)
2. As the Oracle operating system user, run Oracle's SQL*DBA tool, then run the following commands:

```
SQLDBA> connect system /<system_password>;
```

```

SQLDBA> create user <ops$gsodb> identified externally;
SQLDBA> grant create session to <ops$gsodb>;
SQLDBA> grant alter user to <ops$gsodb>;
SQLDBA> grant restricted session to <ops$gsodb>; (oracle 7.2 only)
SQLDBA> exit;

```

Note: If the database user name is gsodb, the default Oracle account is ops\$gsodb.

Second Method: Alternatively, you can set OH_DB_ADMIN to a valid Oracle user name; then, set OH_DB_ADMIN_PASSWORD.

Only one step is required to create this database account:

1. As the Oracle operating system user, run Oracle's SQL*DBA tool, then run the following commands:

```

SQLDBA> connect system/<system_password>;
SQLDBA> create user <user_name> identified by <password>;
SQLDBA> grant create session to <user_name>;
SQLDBA> grant alter user to <user_name>;
SQLDBA> grant restricted session to <ops$user_name>; (oracle 7.2 only)
SQLDBA> exit;

```

Set OH_DBNAME: An Oracle RDBMS must be running, and you must have an ODBC data source configured before the ODBC database server can connect to the Oracle RDBMS. Set the OH_DBNAME in the ohodbc.ini file to the name of the ODBC data source that maps to the Oracle RDBMS.

Oracle Environment: For Oracle, set the following environment variables for the user who starts the ODBC database server:

- ORACLE_HOME = the directory where Oracle is installed.
- ORACLE_OWNER = the Oracle system user; this user installs and administers Oracle.
- ORACLE_SID = the name of the Oracle database instance.

Set these variables in the .odbc.ora.sh file and verify that you can connect directly to Oracle with the SQL*PLUS command line tool. Refer to your Oracle documentation.

Starting the Database Servers

To start the ODBC database servers, do the following:

1. In the rc.odbc file (located in /usr/lpp/gso/odbc on AIX and /opt/ibmgso/odbc on Solaris), uncomment the #ODBC_TYPE line that contains the ODBC database you want to start (remove the pound sign (#)).
2. Save your changes.

3. From the **Global Sign-On Plus for Tivoli** window, double-click **GSO Administration Tasks**.
4. From the **GSO Administration Tasks** window, double-click the **Start Server** icon.
5. From the **Execute Tasks** window, select the database server managed node that corresponds to the database you selected in the rc.odbc file.
6. Press the **Execute** button.

Configuring ODBC on Windows NT Servers

Use the following steps to configure ODBC on the Windows NT server:

1. From the desktop, select **Start -> Programs -> IBM Global Sign-On Server v2.0 -> ODBC Server -> Server Configuration** to display the **ODBC Server Configuration** window.
2. Press the **Settings** button to display the **Data Source** window.
3. Enter a data source name in the **Name that Client will use to Connect** field. This is the name that the clients will use to access the database. Supply this name to the clients. They need to enter it in step 3 of "Configuring a Client Data Source" on page 122 .
The **Database This Server Uses** area is for connecting the ODBC database server to the database.
4. Press the **Data Sources** button to display the Server Configuration message.
5. Press the **OK** button to display the **Data Sources** window.
6. Press the **System DSN** button to display the **System Data Sources** window.
7. Press the **Add** button to display the **Add Data Source** window.
8. Select the Intersolv driver you want to add.
9. Press the **OK** button to display the driver-specific setup window.
10. In the **Data Source Name** field, enter a data source name.
The remaining fields are optional.
11. Press the **OK** button to return to the **System Data Sources** window.
12. Press the **Close** button to return to the **Data Sources** window.
13. Press the **Close** button to return to the **Data Source** window.
14. From the **Data Source** scrolling list box, select the data source you just created.
15. Press the **Change DB Vendor** button to choose a database vendor.
This window displays a radio button for each supported database vendor (Oracle, Microsoft SQL Server, Text Driver, and User Defined).
If you select Text Driver there is no user authentication because you are not accessing a database. If you select User Defined, provide the alter password command.
16. Select a radio button.
17. Press the **OK** button to display the **Change Database Administrator** window.
Enter the name and password of the database administrator for the database you

are using. If you are connecting to an Oracle database, enter the user ID and password for a database account used to alter users' passwords.

18. Press the **OK** button to return to the **Data Source** window.
19. Select a level from the **Protection Level** scrolling list to set the security level. The levels are described in "Setting Protection Levels" on page 119. Supply this level to the clients.
20. **Enforce Proxy Login** is optional. Select this field to require proxy logins. If not selected, proxy logins are permitted, but not required.
21. Press the **OK** button to return to the **ODBC Server Configuration** window.
22. Your data source is now configured. Press the **OK** button.

Implementing Server Security

This section applies to both UNIX (AIX and Solaris) and Windows NT server systems.

Verifying Application Authentication

Application authentication is the ability to verify that the client is running an authorized application.

When this feature is enabled, the ODBC Database Broker prevents unauthorized applications from connecting to the target database through the ODBC database server. This feature can provide an additional level of security.

GSO ODBC database support includes the Application authentication.

You must enable this feature manually, by using the Windows NT Registry Editor to set the value of the OH_APPLICATION_AUTHN parameter to TRUE.

Configuring Application Authentication Using the Windows NT Registry: Use the following steps to enable the Application Authentication feature:

1. Create an .ini file in the ODBC database server's installation directory that matches the CDS name of this server.
2. For each client application executable that must be authenticated, add the following entry to the .ini file you created:
[<appname>.exe]
<full path to the copy of the client application>
3. Place a copy of each client application's executable in the server's installation directory.
4. Use the NT Registry Editor utility (regedt32.exe) to set the value of the OH_APPLICATION_AUTHN parameter to TRUE for this server.

In this example, the server is installed in the c:\ibmgso, the CDS name of the Server is prod_server (that is the OH_CDS_NAME parameter in the Windows NT registry is set to prod_server), and the client application's executable is called salesform.exe.

Create an ASCII file called `prod_server.ini` in the `c:\ibmgso` directory and add the following two lines:

[salesform.exe]

`c:\ibmgso\salesform.exe`

Next, place a copy of the `salesform.exe` program in the `c:\ibmgso` directory. Run `regedt32.exe` and edit the `OH_APPLICATION_AUTHN` Windows NT registry entry for this Server.

The Registry Entry for this Server can be found under:

`HKEY_LOCAL_MACHINE\SOFTWARE\Open Horizon\Connection ODBC
\Settings`

If the `OH_APPLICATION_AUTHN` entry is missing, add it as follows:

1. In `regedt32.exe`, select the **Edit Menu** item.
2. Select the **Add Value** option from within the **Edit Menu** item to display the **Add Value** window.
3. In the **Value Name** field, enter the following:
OH_APPLICATION_AUTHN
4. Press the **OK** button to display the **String Editor** window.
5. In the String, enter the following: **TRUE**.
Press the **OK** button.

The Application Authentication option is now active. To turn this option off, run `regedt32.exe` and set `OH_APPLICATION_AUTHN` to `FALSE`.

Authenticating Users

Users must be authenticated before they can connect to a ODBC database. A user can authenticate a server by requesting verification that the server was started by a specific principal.

Using Authenticated Proxy Logins: Authenticated proxy logins permit only users who are authenticated to connect securely to a database without having to supply a database user name and password. The advantages of this approach follow:

- The database account is secure because no one can access the account without being authenticated first.
- No database passwords are stored outside the database.
- The user does not need an operating system account on the server. (However, Informix users *do* need an operating system account on the server.)
- No passwords go over the network.

Setting Protection Levels: The user can specify whether any of the communications with the server are validated or encrypted. "Validated" means that no data was changed or inserted in the communication. In general, the higher the level of protection, the slower the performance.

When a ODBC database server is started, the OH_PROTN configuration parameter can be used to require a minimum level of protection by all clients. Clients must have a protection level set to this minimum level or to a higher, more restrictive setting, to communicate with the server. See the table below.

AIX and Solaris Protection Levels	Windows NT Protection Levels	Description
CONNECT	On Connect Only	Lowest level. Protection performed when the client connects with the server. Client and server mutually authenticate when the RPC connection is established. Subsequent calls over the same connection are not individually authenticated.
CALL	On Each RPC Call	Protection performed when the server receives an RPC request. Client and server mutually authenticate on every call. RPC computes a check sum on the protocol header of the first packet to each call to ensure that the header has not been modified. When running over a transport like TCP, this protection level automatically upgrades to Packet.
PKT	On Each Packet	Ensures that data is received from the expected client. Client and server mutually authenticate on every call. Checksum is computed on every packet header.
PKT_INTEGRITY	Each Packet + Verify Data	Ensures that data is received from the expected client and that the data has not been modified. Client and server mutually authenticate on every call. Checksum is computed on both header and user data.

AIX and Solaris Protection Levels	Windows NT Protection Levels	Description
PKT_PRIVACY	Each Packet + Verify Data and Encrypt	Highest level. Performs protection as specified by all previous levels, encrypts data. Client and server mutually authenticate on every call. Checksum is computed on both header and user data. User data is DES encrypted.

Setting Proxy Logins

The ODBC database server allows a GSO client identity to be used when establishing a connection to a database. Proxy logins are implemented differently for each database.

DB2 and Informix Proxy Logins: For DB2 or Informix databases, users can enter a forward slash (/) as the user name or leave the user name blank. The ODBC database server will create a new process and set its user ID to an operating system account. This account name is the same as the GSO user ID.

Oracle Proxy Logins: For Oracle databases, users can enter a forward slash (a forward slash (/)) as the user name or leave the user name blank. The ODBC database server will create a new process and connect to the Oracle database. The Oracle user name is the same as the GSO user ID. If the user OH_PROXYPREFIX parameter was set, the Oracle user name will contain the prefix value.

The OH_ENFORCE_PROXY_LOGIN Parameter: For all databases, when you start a ODBC database server with OH_ENFORCE_PROXY_LOGIN set to TRUE, users can connect only through a proxy login. On Windows NT servers, check the Enforce Proxy Login check box. See step 20 on page 118. Users cannot connect to other database accounts, even if they enter a valid database user name and password.

If OH_ENFORCE_PROXY_LOGIN is set to FALSE (Enforce Proxy Login box not selected) when the ODBC database server is started, users can connect to the database by supplying a valid database user name and password. Note, however, that these user names and passwords are sent over the network through a DCE RPC and might be unprotected, depending on the protection level of the connection. For more details, see "Configuring a Client Data Source" on page 122 .

Note that setting OH_ENFORCE_PROXY_LOGIN to FALSE does not prevent users from performing proxy logins.

DB2 and Informix Proxy Logins: When using the ODBC database server with a DB2 or Informix database proxy logins are always enforced, even if OH_ENFORCE_PROXY_LOGIN is set to FALSE.

Starting the Database Servers

To start the ODBC database servers, do the following:

1. From the **Global Sign-On Plus for Tivoli** window, double-click **GSO Administration Tasks** icon.
2. From the **GSO Administration Tasks** window, double-click the **Start Server** icon.
3. From the **Execute Tasks** window, select the database server managed node that corresponds to the database you selected in the rc.odbc file.
4. Press the **Execute** button.

Configuring a Client Data Source

Before using the ODBC Database Broker, configure one or more data sources on your workstation to use the ODBC client. Set options that control how the database is created (such as level of security, which protocol to use, and so on).

1. From the desktop, select **Start -> Programs -> IBM Global Sign-On Client v2.0 -> ODBC Client -> 32-bit ODBC Administrator** to display the **ODBC Data Source Administrator** window.
2. In the **ODBC Data Source Administrator** window, press the **Add** button to display the **Create New Data Source** window.
3. Highlight **IBM Global Sign-On Driver** and press the **Finish** button to display the **ODBC Setup** window.
4. Enter the **Data Source Name**. This name should be supplied by your GSO administrator and must correspond to the OH_CDS_NAME configuration parameter on 108.
5. The **Description** field is optional. You can enter a description for your own use.
6. The **Data Base Name** field is optional. Enter the name of the database. When connecting to an Oracle database, this field is not used. When connecting to Informix servers, this field specifies the database. If left blank, clients will connect to whatever database is set in the ODBC data source that the ODBC database server is using.
7. Select a **Protection Level** from the scrolling list. This level should be provided by your GSO administrator.
8. The **Don't Prompt For User ID** is optional. Select this field to suppress the user ID and password login window.
9. Press the **OK** button to return to the **ODBC Data Source Administrator** window.
10. You have finished installing ODBC client. Press the **OK** button.

ODBC Server Configuration Parameters

The following table summarizes the configuration parameters that users can set in the database environment.

On UNIX (AIX and Solaris) servers, users can set configuration parameters in the `ohodbc.ini` file.

On Windows NT servers the parameters are stored in the Windows NT registry. Users can set these parameters in the ODBC **Server Configuration** window.

Configuration Parameters	Value and Description
OH_CDS_NAME	<p><name of database server></p> <p>This is the name that the ODBC database server uses to advertise itself in the DCE Cell Directory Service. The OH_CDS_NAME must be different from the OH_DBNAME. This is the name that clients enter for the ODBC data-source name.</p>
OH_DBNAME	<p><ODBC data source_name></p> <p>Server and client. The ODBC Data Source Name that the ODBC database server uses to connect to a database. The oh_dbname must be different from the oh_cds_name. The oh_cds_name must correspond to an entry in the .odbc.ini file.</p>
OH_DB_ADMIN	<p><principal_id></p> <p>The principal ID that the ODBC database server uses to log in to the database. This ID must have the privilege to alter other users' passwords. This parameter is required.</p>
OH_DB_ADMIN_PASSWORD	<p><password></p> <p>This required parameter is the password for the oh_db_admin principal.</p>
OH_MAXSVR	<p>an integer</p> <p>(default=100)</p> <p>Maximum number of concurrent connections allowed by the server.</p>

Configuration Parameters	Value and Description
OH_PROTN	CONNECT CALL PKT PKT_INTEGRITY PKT_PRIVACY (default=CONNECT) Server and client. See "Setting Protection Levels" on page 119 for a complete description. These values are listed in increasing levels of security. The client must set OH_PROTN to a level that matches or exceeds that of the server.
OH_ENFORCE_PROXY_LOGIN	TRUE FALSE (default=TRUE) See page 109 for a complete description. This value defines whether only proxy logins are allowed, or alternatively, if you can connect to a database account that is different from your GSO user ID when a valid password is supplied.
OH_PROXYPREFIX	<proxy_prefix> " " null (default=null) Optional parameter. Use this value to set a prefix for proxy logins.

Configuration Parameters	Value and Description
OH_TRACE	<p>FALSE</p> <p>0xffffffff</p> <p>(default=FALSE)</p> <p>Server and client. This is an optional value that should normally be set to false or not at all. When set to "0xffffffff" then the server will write information to a trace file. The trace file has a ".trc" extension. Tracing slows performance, and over time the trace files might grow large.</p>

Resolving ODBC Issues and Known Problems

The following information provides some help regarding existing database issues.

Oracle 7.2 on Windows NT

ODBC performs best with Oracle 7.2 on UNIX operating systems. ODBC does not support Oracle 7.2 on Windows NT.

Supported ODBC Functions

The client ODBC driver is a generic ODBC driver. The ODBC functions and datatypes that it supports depend on the capabilities of the server resident ODBC driver that the ODBC database server is using.

The following ODBC functionality is *not* supported by the client ODBC driver, regardless of the ODBC driver used by the ODBC database server.

- SQLBrowseConnect.
- Row-Wise binding in SQLExtended Fetch (Column-Wise binding *is* supported).

Configuring OCI

This section describes how to configure the GSO OCI database servers and clients. The OCI database server uses the Oracle Call Interface (OCI) to access an Oracle database. The GSO database client is an OCI driver implemented as a dynamic link library (DLL) on Windows clients. The GSO database server accepts requests from the GSO database client and passes them to the appropriate OCI database server.

Configuring OCI on AIX and Solaris Servers

The gsodb login account is created during the OCI database-server installation.

- You must set a gsodb account password.
- To set a password for the gsodb account, you must have root permission.

The .oci.sh setup script is created on AIX and Solaris during the database server installation process. Edit this file to uncomment and set your environment-specific variables.

GSO Plus uses the .oci.sh file to start the database server processes. This file is created in the gsodb user's home directory. It defines the environment variables required to run the database server. For example, after you run this script, it sets the path for the OH_HOME environment variable (the OH_HOME environment variable is referenced throughout this appendix).

After you set your environment variables and configure your .ini file parameters, return to the GSO Administration Tasks window and select the icon called Start Server to start your server processes (see "Starting the Database Servers" on page 129 and "Starting the Database Servers" on page 134).

Associating Oracle with an OCI Server

To associate an Oracle server with an OCI server, you must have an Oracle RDBMS instance running before you start an OCI server. When you run an Oracle RDBMS instance, the ORACLE_SID environment variable and the OH_CDS_NAME configuration parameter map the Oracle RDBMS instance to an OCI server.

The entry name used by an OCI server for its location information is the OH_CDS_NAME. If your Oracle database's SID is finance, and the OH_CDS_NAME is forecasting, then forecasting is associated with the Oracle finance database. In this example, forecasting is used as the connect string to get to the finance database. Oracle databases that are serviced by OCI server do not need globally unique SIDs throughout the GSO cell.

Setting Server Configuration Parameters

The following configuration parameters control the behavior of the OCI server. These parameters are contained in the \$OH_HOME/admin/ohoci.ini file. An OCI server reads these parameters when it is initialized. Do not change these parameters while your OCI server is running. You can edit these parameters directly with vi or any other text editor.

OH_PROTN

This optional parameter sets the minimum level of protection that a client can request for all RPCs associated with a server. These protection levels, are defined by GSO as CONNECT, CALL, PACKET, INTEGRITY, and PRIVACY. See "Setting Protection Levels" on page 133 .

OH_ENFORCE_PROXY_LOGIN

If this optional parameter is set to TRUE (default value), the OCI server accepts only proxy logins from the client workstation. The client's user name can be entered as a forward slash (/) or left empty. Any supplied password is ignored. OCI uses the GSO user ID, prefixed by the OH_PROXYPREFIX, as the Oracle user name for a proxy login.

If the OH_ENFORCE_PROXY_LOGIN parameter is set to FALSE, the OCI server can accept either proxy logins or regular Oracle logins. The client's user name can be specified as a forward slash (/) (which is interpreted as a proxy login, and any supplied password is ignored) or <user_name> (which is interpreted as a regular Oracle user name; the client must provide a valid Oracle password), or left empty. See "Using Authenticated Proxy Logins" on page 132.

OH_PROXYPREFIX

Use this optional configuration parameter to add prefixes to your GSO user ID. This parameter modifies the user name for database access. For example if you set this value to "gso" when gso user ID scott performs a proxy login, he will connect to the database as gso.scott. The default value is null.

OH_CDS_NAME

Set this required parameter to the unique name (within that GSO cell) users can associate with the database.

OH_MAXSVR

This optional parameter is an integer value that specifies the maximum number of concurrent client connections that can be managed by the OCI server. The default is 100.

OH_TRACE

This is an optional parameter that is typically set to FALSE, or not at all. (The default value is FALSE.) If it is set to "0xffffffff", the server writes information to a trace file in the same directory in which the server is running. The trace file will be named "ohoci.trc" and be located in the directory where you start the OCI server. This trace file can be useful for support personnel to help isolate and fix problems. When a problem has been resolved, be sure to disable tracing by setting it to FALSE or removing this parameter. Tracing will slow performance, and over time the trace files might grow large.

The GSO OCI database server supports PeopleSoft version 5.1.

OH_PEOPLESOFT

The GSO OCI database server supports PeopleSoft version 5.1 configuration parameters. Edit these parameters with a text editor just as you edit the other parameters.

Acceptable values are TRUE and FALSE. The default setting is FALSE. If set to TRUE this parameter changes the login routine to the PeopleSoft login architecture, and sets the OH_ENFORCE_PROXY_LOGIN and OH_APPLICATION_AUTHN configuration parameters to TRUE.

The users will login to the application under their usual user name and be authenticated by the OCI server as their GSO user ID. Then, users will be logged in to the database as the operating system authenticated database account, such as ops\$gsodb. This is the operating system account that is used to start the OCI server.

IMPORTANT: The gsodb account must be the owner of the PeopleSoft database.

OH_APPLICATION_AUTHN

Set this configuration parameter to either TRUE or FALSE. When set to TRUE, the OCI server will connect only to authorized applications. You will create a file that lists the authorized applications. Any application not on the list will not be allowed to connect OCI server, even if the user is authenticated. Give this file the same name as your OH_CDS_NAME parameter and add the ".ini" extension, that is, <OH_CDS_NAME>.ini.

For those applications that are specified in the <OH_CDS_NAME>.ini file, the OCI server will compare the client application executable against a reference copy to verify that the correct application is being used. Use the full path name of the reference executable so that the OCI server can find it. This file can be either a separate binary copy of the executable file, or the executable that users invoke. Use the following file format:

<OH_CDS_NAME>.INI	Corresponds to OH_CDS_NAME in ohoci.ini file
pstools.exe PATH=<your_path>/pstools	Application to be authorized. Not case sensitive.
<app>.exe PATH=<your_path>/tools	Path to secure copy of the executable file on the server. Is case sensitive.

There is one authorization file for each OCI server instance (OH_CDS_NAME) but the file might contain any number of entries, authorizing any number of applications.

Creating a Special Oracle Database Account

Each Oracle database must have a special database account. For the OCI server to implement the proxy login security features, there must be a privileged Oracle database account. To create this database account, use one of the following two methods:

First Method:

By creating this account as an externally authenticated account you can set the OH_DB_ADMIN parameter to a forward slash (/). In this way you do not have to set the password in the OH_DB_ADMIN_PASSWORD parameter.

Use the following steps to create an externally identified database account:

1. Determine what the OS_AUTHENT_PREFIX parameter is for your database. This parameter is defined in your init<sid>.ora file. The default is ops\$. If your OS_AUTHENT_PREFIX is not ops\$, replace every occurrence of ops\$ in the SQL commands with your prefix. (You can use any tool that accesses the SQL command line, such as SQL*DBA or SQL*Plus.)
2. As the Oracle operating system user, go to the SQL command line, then run the following commands:

```
SQL> connect system/<system_password>;
SQL> create user <ops$gsodb> identified externally;
SQL> grant create session to <ops$gsodb>;
SQL> grant alter user to <ops$gsodb>;
SQL> grant restricted session to <ops$gsodb>; (Oracle 7.2 or later only)
SQL> exit;
```

Note: If the database user name is gsodb, the default Oracle account is ops\$gsodb.

Second Method: Alternatively, you can set OH_DB_ADMIN to a valid Oracle user name; then, set OH_DB_ADMIN_PASSWORD.

Only one step is required to create this database account:

1. As the Oracle operating system user, run Oracle's SQL*DBA tool, then run the following commands:

```
SQL> connect system/<system_password>;
SQL> create user <user_name> identified by <password>;
SQL> grant create session to <user_name>;
SQL> grant alter user to <user_name>;
SQL> grant restricted session to <ops$user_name>; (oracle 7.2 only)
SQL> exit;
```

The ohsec.sql file in the \$OH_HOME/admin directory contains the SQL commands shown above. Run the script for every Oracle database using the commands above.

Starting the Database Servers

To start the OCI database servers, do the following:

1. From the **Global Sign-On Plus for Tivoli** window, double-click **GSO Administration Tasks**.

2. From the **GSO Administration Tasks** window, double-click the **Start Server** icon.
3. From the **Execute Tasks** window, select the database server managed node that corresponds to the database you selected in the rc.odbc file.
4. Press the **Execute** button.

Configuring OCI on Windows NT Servers

Before starting an OCI server, set the configuration parameters in the Windows NT Software Registry to customize various server options. See “OCI Server Configuration Parameters” on page 136.

Use the following steps to set the configuration parameters:

1. From the desktop, select **Start -> Programs -> IBM Global Sign-On Server v2.0 -> OCI Server -> Server Configuration** to display the **OCI Server Configuration** window.
2. Press the **Settings** button to display the **Data Source** window.
3. Enter a data source name in the **Name that Client will use to Connect** field. This is the name (connect string) that the clients will use to access the database. The clients need to enter it in step 3 on page 134. (This is also the OH_CDS_NAME parameter in the Windows NT registry.)
4. From the **Protection Level** scrolling list, select a security level. The levels are described in “Setting Protection Levels” on page 133. (This is also the OH_PROTN parameter in the Windows NT registry.)
The default value is **On Connect Only**. If you change this setting, supply the level to the clients. They need to use this level of protection or higher to connect. See step 5 on page 134.
5. **Enforce Proxy Login** is optional. Select this field to require proxy logins. If not selected, proxy logins are permitted, but not required. (This is the OH_ENFORCE_PROXY_LOGIN parameter in the Windows NT Registry.)
6. Press the **OK** button to return to the **OCI Server Configuration** window.
7. Press the **Oracle Settings** button to display the **Oracle Settings** window.
8. In the **Administrative Username** field, enter either a forward slash (/) (see “First Method” on page 129) or an externally-defined user name (see “Second Method” on page 129), depending on the method you used to configure your Oracle database account.
9. If you provided an externally-defined administrative user name, you must also provide a password in the **Administrative Password** field.
10. Press the **OK** button to return to the **Data Source** window.
11. If you provided an administrative password, confirm it in the **Confirm Password** field.
12. Press the **OK** button to return to the **OCI Server Configuration** window.
13. Your data source is now configured. Press the **OK** button.

If you are using PeopleSoft version 5.1, use the following parameters. Use the Windows NT Registry (HKEY_LOCAL_MACHINE\SOFTWARE\Open Horizon\Connection OCI Server\Settings) to set these parameters.

OH_PEOPLESOFT

Acceptable values are TRUE and FALSE. The default setting is FALSE. If set to TRUE this parameter changes the login routine to the PeopleSoft login architecture, and sets the OH_ENFORCE_PROXY_LOGIN and OH_APPLICATION_AUTHN configuration parameters to TRUE. (If OH_PEOPLESOFT = TRUE it will override the values for the other two parameters.)

The users will log in to the application under their usual user name and be authenticated by the OCI server as their GSO user ID. Then, users are logged in to the database as the operating system authenticated database account, such as ops\$gsodb. This operating system account is used to start the OCI server.

Note: Your OCI database operating system account must match the PeopleSoft database owner account.

OH_APPLICATION_AUTHN

Set this configuration parameter to either TRUE or FALSE. When set to TRUE, the OCI server connects only to authorized applications. You will create a file which lists the authorized applications. Any application not on the list will not be allowed to connect to the OCI server, even if the user is authenticated. Give this file the same name as your OH_CDS_NAME parameter and add the ".ini" extension, that is, <OH_CDS_NAME>.ini.

For those applications that are specified in the <OH_CDS_NAME>.ini file, the OCI server compares the client application executable against a reference copy on the server machine to verify that the correct application is being used. Use the full path name to the reference executable so that the OCI server can find the it. This file can be either a separate binary copy of the executable file, or the executable that users invoke.

Use the following file format:

<OH_CDS_NAME>.INI	Corresponds to OH_CDS_NAME file
x:<pstools> PATH=<your_path>\tools	Application to be authorized . Not case sensitive.
<app>.exe PATH=<your_path>tools	Path to secure copy of the executable file on the server. Is case sensitive.

There is one authorization file for each OCI server instance (OH_CDS_NAME) but the file might contain any number of entries, authorizing any number of applications.

Using the Trace Utility

There is a trace utility included with the OCI database. To run the trace utility from the Windows NT desktop, select **Start -> Programs -> IBM Global Sign-On Server v2.0 -> OCI Server -> Server Trace**.

Implementing Server Security

This section applies to both UNIX (AIX and Solaris) and Windows NT servers.

Authenticating OCI Users

Users must always be authenticated by GSO before they can connect to an Oracle database. A user can also authenticate a server by requesting verification that the server was started by a specific user.

Using Authenticated Proxy Logins: A proxy login enables GSO to log in to the database on the user's behalf. The user no longer has to supply a user name or password. For a proxy login, GSO uses the GSO user ID name prefixed by the OH_PROXYPREFIX (if it is set) for the Oracle user name.

When you start OCI with the configuration parameter OH_ENFORCE_PROXY_LOGIN set to TRUE, users can connect only through a proxy login.

Authenticated proxy logins permit only users who are authenticated by GSO to securely connect to an Oracle database. The advantages of this approach are as follows:

- Each GSO user ID can connect to only one Oracle database account. This means that user ID ben cannot connect to Oracle as karyn, but only as ben.
- Database passwords are administered centrally for all GSO databases.
- The user does not need an operating system account on the server.
- No passwords go over the network.

If OH_ENFORCE_PROXY_LOGIN is set to FALSE when the OCI server is started, users can connect to Oracle by supplying a valid database user name and password. However, these Oracle user names and passwords *are* sent over the network through a DCE RPC and might be unprotected, depending on the protection level of the connection. See "Configuring a Client Data Source" on page 134 for more details. The user still needs valid GSO credentials, but the GSO user ID does not have to match their Oracle user ID.

Note that setting OH_ENFORCE_PROXY_LOGIN to FALSE does not prevent users from performing proxy logins by entering a forward slash (a forward slash (/)) as the user name.

Note: On Windows NT Servers this parameter is set in the Server Configuration window.

Setting Up Single Login Capability: Users can access multiple databases with a single login. This is the default option and requires no system administrator intervention.

Setting Protection Levels

The user can specify whether the communications with the server are validated, or encrypted means that no data was changed or inserted in the communication. In general, the higher the level of protection, the slower the performance.

When an OCI server is started, the `OH_PROTN` configuration parameter, or the **Protection Level** field (see step 4 on page 130), sets a minimum level of protection required by all clients. Clients must have a protection level set to this minimum level or to a higher, more secure setting, to communicate with the server.

This table lists the protection levels used by OCI. The order of protection levels is from lowest to highest.

AIX and Solaris Protection Levels	Windows NT Protection Levels	Description
CONNECT	On Connect Only	Lowest level. Protection performed when the client connects with the server. Client and server mutually authenticate when the RPC connection is established. Subsequent calls over the same connection are not individually authenticated.
CALL	On Each RPC Call	Protection performed when the server receives an RPC request. Client and server mutually authenticate on every call. RPC computes a check sum on the protocol header of the first packet to each call to ensure that the header has not been modified. When running over a transport like TCP, this protection level automatically upgrades to Packet.
PKT	On Each Packet	Ensures that data is received from the expected client. Client and server mutually authenticate on every call. Checksum is computed on every packet header.

AIX and Solaris Protection Levels	Windows NT Protection Levels	Description
PKT_INTEGRITY	Each Packet + Verify Data	Ensures that data is received from the expected client and that the data has not been modified. Client and server mutually authenticate on every call. Checksum is computed on both header and user data.
PKT_PRIVACY	Each Packet + Verify Data and Encrypt	Highest level. Performs protection as specified by all previous levels, encrypts data. Client and server mutually authenticate on every call. Checksum is computed on both header and user data. User data is DES encrypted.

Starting the Database Servers

To start the OCI database servers, do the following:

1. From the **Global Sign-On Plus for Tivoli** window, double-click **GSO Administration Tasks**.
2. From the **GSO Administration Tasks** window, double-click the **Start Server** icon.
3. From the **Execute Tasks** window, select the database server managed node that corresponds to the database you selected in the rc.odbc file.
4. Press the **Execute** button.

Configuring a Client Data Source

Before using the OCI, configure the data source. Use the following steps to perform this task.

1. From the desktop, select **Start -> Programs -> IBM Global Sign-On Client V2.0 -> OCI Client -> OCI Client Configuration** to display the **Data Sources** window.
2. In the **Data Sources** window, press the **Add** button to display the **OCI Client Configuration** window.
The following steps apply to the fields shown in the OCI Setup window:
 3. In the **Data Source Name** field, enter the name specified by your administrator. The Data Source Name corresponds to the CDS name entry of the OCI server.
 4. In the **Description** field, enter a comment that describes the type of information the database contains. This field is optional.
 5. Select a protection level from the **Protection Level** scrolling list. This value governs the level of security in effect for all communication between the client and the server. Your GSO administrator should give you this value. See "Implementing

Server Security” on page 132 for more information. Note that if the security level chosen is lower than that required by the server, the connection fails. The default Protection Level is On Connect Only.

6. Press the **OK** button to return to the **Data Sources** window.
7. Your data source is configured. Press the **Close** button.

Ensuring Correct Path to Oracle Executables

The OCI client is implemented in the following three files: ohres.dll, ora7win.dll (or ora71win.dll ora72.dll) and bc500rt1.dll.

Note: The OCI database includes both ora71win.dll and ora7win.dll. Your application can load one or the other, depending on which version of Oracle it was linked with. These DLLs are essentially the same.

When a Windows program loads one of these DLLs, Windows searches for the required DLL in the following order:

1. The current directory (the directory where the Windows application resides)
2. The windows directory
3. The windows\system directory
4. Each directory in your DOS path.

If it does not find the DLL, it returns an error. If your workstation has Oracle SQL*Net installed, the Oracle executable files (and the Oracle ora7win.dll) reside in one of the directories in your DOS path. Since, the installation places the OCI ora7win.dll into the c:\windows\system directory, Windows loads this DLL first whenever ora7win.dll is required by an application.

Note that the above situation does not prevent Oracle's ora7win.dll from residing in the same directory as the Windows application. Regardless of the current DOS path settings, the application first tries to use the DLLs located in its current directory. In case of problems, take the appropriate action (such as renaming Oracle's ora7win.dll to ora7win.ora or by removing it from that directory).

Attention: Renaming Oracle's ora7win.dll will disable it. If you should need to revert to SQL*Net you would have to rename this file and ora7win.dll.

Some applications might try to invoke a DLL name other than ora7win.dll. On Windows NT the file is either ora7nt.dll, orant71.dll, or ora72.dll depending on the Oracle version your application was linked with. In this case, rename the OCI DLL to the appropriate DLL name.

Making Directory Changes to Use SQL*Plus and Other Oracle Tools

You cannot use SQL*Plus or other Oracle tools with the OCI client because they call proprietary, undocumented functions in the Oracle version of `ora7win.dll`; however, you can use Oracle tools separately from the OCI database connection. To run the Oracle tools:

1. Oracle's `ora7win.dll` must reside in the Oracle bin directory (typically `c:\orawin\bin`), or the same directory as the Oracle tools.
2. Then, when you run Windows applications such as Power-Builder or Visual Basic, those applications will find the database connection DLL (and not Oracle's DLL) in `windows\system` before searching the DOS path.
3. When you run an Oracle tool such as SQL*Plus, which resides in the Oracle bin directory, it finds the appropriate Oracle DLL in the same Oracle bin directory and does not have to search the current path.

Providing a New Connect String Syntax

To use the OCI database connection, your client applications must provide a new connect string syntax. Use the Data Source Name (`OH_CDS_NAME` of the OCI server) from the OCI Configuration window, see step 3 on page 134.

For example:

```
scott/tiger@finance
```

Here, `finance` is the CDS entry where an OCI server places its location information. The location for this entry is in `././subsys/gso/db`. See "Associating Oracle with an OCI Server" on page 126.

Testing the Database Connection

When you finish installation and configuration, test your application with the Oracle database.

Use the `WINOCI32.exe` tool to test the connection. This tool is available during custom installation of GSO OCI client.

OCI Server Configuration Parameters

The following table summarizes the configuration parameters users can set in the Oracle/OCI database environment.

On UNIX (AIX and Solaris) servers, users can set configuration parameters in the `ohoci.ini` file.

On Windows NT servers the parameters are stored in the Windows NT registry. Users can set these parameters in the **Server Configuration** window.

OH Configuration Parameter	Value/Description
OH_CDS_NAME	<p><database_name></p> <p>Server only. Use the name that users will use to identify the database.</p>
OH_MAXSVR	<p>An integer</p> <p>(default=100)</p> <p>Server only. Maximum number of concurrent connections allowed by the server.</p>
OH_ENFORCE_PROXY_LOGIN	<p>TRUE</p> <p>FALSE</p> <p>(default=true)</p> <p>Server only. See "Setting Up Single Login Capability" on page 132 for a complete explanation. This parameter defines whether only proxy logins are allowed, or alternatively, if you can connect to an Oracle account that is different than your GSO user ID when a valid password is supplied.</p>
OH_PROXYPREFIX	<p><proxy_prefix></p> <p>" " null</p> <p>(default=null)</p> <p>Server only. Optional parameter. Use this parameter to set a prefix for proxy logins.</p>
OH_POOL_SIZE	<p>An integer</p> <p>(default=0)</p> <p>Optional, server only. Set to number of spare processes you want the database server to maintain. Speeds login time. Recommended setting is between 2 and 10.</p>

OH Configuration Parameter	Value/Description
OH_PEOPLESOFT	<p>TRUE</p> <p>FALSE</p> <p>(default = FALSE)</p> <p>Sets OH_ENFORCE_PROXY_LOGIN to and OH_APPLICATION_AUTHN to true. Uses PeopleSoft login process..</p>
OH_APPLICATION_AUTHN	<p>TRUE</p> <p>FALSE</p> <p>(default = FALSE)</p> <p>OCI server will connect only authenticated applications.</p>
OH_PROTN	<p>CONNECT</p> <p>CALL</p> <p>PKT</p> <p>PKT_INTEGRITY</p> <p>PKT_PRIVACY</p> <p>(default=connect)</p> <p>Server and client. See "Implementing Server Security" on page 132 for a complete description. Here, they are listed in increasing levels of security. The client must set OH_PROTN to a level that matches or exceeds that of the server.</p>
OH_PROTOCOL	<p>ncacn_ip_tcp</p> <p>ncadg_ip_udp</p> <p>(default=null. Will use any available protocol.)</p> <p>Client only. Sets the network transport protocol.</p>
OH_TIMEOUT	<p>0 ... 10</p> <p>(default=5)</p> <p>Client only. Amount of time for the client to wait for a response from the server before returning an error. This is not in seconds but rather in units defined by the protocol. 0 is the shortest, 10 waits indefinitely for the RPC operation to complete.</p>

Resolving Oracle Issues and Known Problems

The following information provides some help regarding error messages generated by the Oracle server if your environment is not set up correctly.

GSODB-161 Your login context has expired. Login again and restart your application.: Either you have not logged in or your login has expired. Log in again and restart your application.

GSODB-179 Cannot Search CDS Name Space: Either the OCI server was not started properly, or it has stopped running. If the OCI server was started properly and is still up, then there is no value in the OH_CDS_NAME configuration parameter. Stop the OCI server. Enter a value in the OH_CDS_NAME and restart the OCI server.

ORA-3121 No interface driver connected.: Your application is invoking Oracle's ora7win.dll instead of OCI's ora7win.dll. Remove Oracle's ora7win.dll from the search path, or move it to another directory, such as oracle\bin.

GSODB-202 Cannot find the specified server. Make sure the server is up with the correct name: Your OCI server has a CDS entry but is no longer running and so does not respond. Restart the OCI server.

GSODB-1046 RPC Failed: Either you have tried to connect more than the OH_MAXSVR parameter allows, or your OCI server has stopped. If you have too many connections, increase OH_MAXSVR on the server and restart it. If your OCI server stopped, check your configuration parameters, and restart it.

GSODB-1044 Unable to find a suitable server for connection: The operation system environment of the OCI server is no configured correctly. Check ORACLE_HOME, ORACLE_SID, and PATH. You should be able to connect to Oracle as forward slash (/) Or, your Oracle server could be down.

Configuring CT-LIB

This section describes how to configure the GSO Sybase database servers and clients.

The GSO Sybase database server uses the CT-LIB interface to access one or more Sybase databases. The GSO database client is a CT-LIB driver implemented as a dynamic link library (DLL) on Windows clients. GSO augments the Sybase Open Client environment by replacing some of the Open Client libraries. The GSO database server accepts requests from the GSO database client and passes them to the appropriate Sybase SQL server.

Setting CT-LIB Environment Variables on AIX and Solaris Servers

The gsodb login account is created during the database-server installation.

- You must set a gsodb account password.

- To set a password for the gsodb account, you must have root permission.

The `.ctlib.sh` setup script is created on AIX and Solaris during the database server installation process. Edit this file to uncomment and set your environment-specific variables.

GSO Plus uses the `.ctlib.sh` file to start the database server processes. This file is created in the gsodb user's home directory. It defines the environment variables required to run the database server. For example, after you run this script, it sets the path for the `OH_HOME` environment variable (the `OH_HOME` environment variable is referenced throughout this appendix).

After you set your environment variables and configure your `.ini` file parameters, return to the GSO Administration Tasks window and select the icon called Start Server to start your server processes (see "Starting the Database Servers" on page 146).

Associating a Sybase SQL Server with a CT-LIB Server

A Sybase SQL server must be running before you start a CT-LIB Server. The CT-LIB server is mapped to the Sybase SQL Server by the `DSQUERY` and the `SYBASE` environment variables when you start the CT-LIB server.

The CDS entry name used by a CT-LIB server for its location information is the same as the `DSQUERY` value by default. If your Sybase database's `DSQUERY` is `finance`, the CT-LIB server for Sybase exports its location information to the CDS entry `././subsys/gso/db/finance`. You can change the database name by changing the `OH_CDS_NAME` parameter.

Setting Server Configuration Parameters

The following configuration parameters control the behavior of the CT-LIB Database Broker. They are set in the `$OH_HOME/admin/ohctlibs.ini` file on AIX and Solaris servers. A CT-LIB server reads these parameters when it is initialized. Do not change these parameters while your CT-LIB server is running. You can edit these parameters directly with `vi` or any other text editor.

`OH_CDS_NAME`

Set this parameter to the unique name that clients associate with the SQL Server. This is the name used to register the CT-LIB server in DCE's CDS. The default value is the value of `DSQUERY` environment variable.

`OH_DB_ADMIN`

The Sybase login that the CT-LIB server uses to connect to the SQL server. This login needs permission to alter other user's passwords. The default value for this parameter is `sa`. You can change this value. See "Creating a Special Sybase Database Account" on page 143.

OH_DB_ADMIN_PASSWORD

This required parameter is the password for the Sybase Login specified by the OH_DB_ADMIN. The default value for this parameter is null. You can change this value. See “Creating a Special Sybase Database Account” on page 143.

Note: It is important that the ohctlibs.ini file *not* be readable by others to protect this password.

OH_MAXSVR

This optional parameter is an integer value that specifies the maximum number of concurrent client connections that can be managed by the CT-LIB server. The default is 100.

OH_PROTN

This optional parameter sets the minimum level of protection that a client can request for all RPCs associated with a server. These protection levels are as follows: CONNECT, CALL, PACKET, INTEGRITY, PKT_PRIVACY. See “Setting Protection Levels” on page 145.

OH_ENFORCE_PROXY_LOGIN

If this optional parameter is set to TRUE (default), the CT-LIB server accepts only proxy logins from the client workstation. See “Setting Proxy Logins” on page 144. The client’s user name can be entered as a forward slash (/) or left empty. Any supplied password is ignored.

If this parameter is set to FALSE, the CT-LIB server can accept either proxy logins or regular Sybase logins. The client’s user name can be either a forward slash (/) (which is interpreted as a proxy login, and any supplied password is ignored) or *<user_name>* (which is interpreted as a regular Sybase user name; the client must provide a valid Sybase password).

OH_MULTITHREADED_SERVER

When set to TRUE, the master and replica servers handle multiple concurrent requests from clients. When omitted or set to FALSE, the master server starts one dedicated replica server for each client. The default setting is FALSE. This parameter is optional.

OH_MASTER_AS_SERVER

When set to TRUE, the Master server processes multiple concurrent database requests from clients. When omitted or set to FALSE, the master server starts one or more replica servers, each handling multiple concurrent database requests from clients.

Use this parameter only when OH_MULTITHREADED_SERVER is set to TRUE.

OH_THREADSAFE_RUNTIME

When set to TRUE, multiple simultaneous requests can be presented to the database client runtime by the master and replica servers. When omitted or set to FALSE, access to the database client runtime is serialized by the multithreaded master and replica servers.

Use this parameter only when OH_MULTITHREADED_SERVER is set to TRUE.

OH_MESSAGE_BASE

Set this optional parameter to a numeric value. The value is added to internally generated message numbers before they are sent to the client application. Client and server values might be set independently, or identically, for the client and server (in ohctlibc.ini and ohctlibs.ini, respectively).

This feature is useful in database server environments where other third-party applications might present errors to database client applications. The default value is 20,000.

OH_TRACE

This is an optional parameter that should normally be set to FALSE or not at all. (The default value is FALSE.) If it is set to "0xffffffff" then the server will write information to a trace file in the same directory in which the server is running. The trace file will have a ".trc" extension. This trace file can be useful for support personnel to help isolate and fix problems. When a problem has been resolved, be sure to disable tracing by setting it to FALSE or removing this parameter. Tracing will slow performance, and over time the trace files might grow large.

OH_LISTEN_THREADS

This parameter enables you to set the maximum number of RPC requests that the CT-LIB server can handle concurrently. The default value is 10. Valid values are whole integers between 1 and the limit set by the max_calls_exec parameter of the DCE function rpc_server_listen. You can set this value to the number of users you expect to use the CT-LIB server simultaneously.

Setting this value too low could limit your throughput.

OH_APPLICATION_AUTHN

Set this configuration parameter to either TRUE or FALSE. When set to TRUE, the CT-LIB server will connect only to authorized applications. You will create a file that lists the authorized applications. Any application not on the list will not be allowed to connect to the CT-LIB server, even if the user is authenticated. Give this file the same name as

your `OH_CDS_NAME` parameter and add the “.ini” extension (`<OH_CDS_NAME>.ini`). Place this file in the `$OH_HOME` environment variable and the `OH_HOME` configuration parameter must point to the same directory.

For those applications that are specified in the `<OH_CDS_NAME>.ini` file, the CT-LIB server will compare the client application executable against a reference copy to verify that the correct application is being used. Use the full path name to the reference executable or the executable that users invoke.

1. Create the `<OH_CDS_NAME>.ini` text file in your `$OH_HOME` directory.
2. Make sure that your `OH_HOME` environment variable and your `OH_HOME` configuration parameter point to the same directory.
3. The applications that make use of this feature must be Windows NT or Windows 95 applications.

You can have only one authorization file for each CT-LIB server instance (`OH_CDS_NAME`), but the file might contain any number of entries, authorizing any number of applications. You can choose to have multiple groups of users access the same database through different groups of authorized applications. Create multiple CT-LIB server instances with different authorization lists. Restrict access to each CT-LIB server instance (and each list of authorized applications) to a specific DCE group. See discussion on “Enforcing Data Source Level User Authorization”.

The `ohctlibs.ini` file contains sample values of these configuration parameters. You can edit the values directly with `vi` or any other text editor.

Creating a Special Sybase Database Account

Each SQL server used with CT-LIB must have a special database account. For the CT-LIB server to implement the proxy login security features, there must be a privileged Sybase account. Use the following steps to create this database account:

1. Choose a Sybase user name that is *not* a GSO user ID. This example uses `dbadmin`.
2. Connect to the target SQL Server as the system administrator using ISQL, and enter the following commands:

```
% isql -Usa -P<sa_password> -S<sql_server>;
> sp_addlogin <gsodb>, <gsodb_password>
> go
> sp_adduser <dbadmin>
> go
> sp_role "grant", sso_role, <dbadmin>
> go
> quit;
```

These commands create the user `dbadmin`, and grant it permission to change users' passwords.

3. Edit the `ohc1libs.ini` file to set `OH_DB_ADMIN` to the **<dbadmin>** user name you just created, and `OH_DB_ADMIN_PASSWORD` to the **<dbadmin_password>** that you just created.

Using the Sybase Interfaces File

You need to copy your local Sybase interfaces file to the `$OH_HOME` directory or create a softlink to your local Sybase interfaces file. This copy or link is required so the CT-LIB server can find the appropriate SQL server listed in the configuration file or `DSQUERY` environment variable. Creating a softlink to the interfaces file might save on disk space and might require less system administration.

Sybase Environment Variable

The database client configuration is required by the CT-LIB server. Set the Sybase environment variable to the `$OH_HOME` directory location. Do not point the `SYBASE` environment variable to an existing Sybase database client directory structure.

Implementing Server Security

This section applies to AIX and Solaris server systems.

Authenticating CT-LIB Users

Users must *always* be authenticated before they can connect to a SQL server with CT-LIB. A user can also authenticate a server by requesting verification that the server was started by a specific principal.

Using Authenticated Proxy Logins: Authenticated proxy logins permit only users who are authenticated to securely connect to an Sybase SQL Server without having to supply a database user name and password. The advantages of this approach are as follows:

- The database account is secure because no one can access the account without being authenticated first.
- The user does not need an SQL Server login.
- No passwords go over the network.

Setting Proxy Logins

When you start a CT-LIB database server with `OH_ENFORCE_PROXY_LOGIN=TRUE`, users can connect to that server only through a proxy login.

When you start a CT-LIB database server with `OH_ENFORCE_PROXY_LOGIN=FALSE`, users can connect to Sybase by supplying a valid SQL Server login name and password. Note, however, that these Sybase user names and passwords are sent over the network through a DCE RPC and might be unprotected, depending on the protection level of the connection.

Setting OH_ENFORCE_PROXY_LOGIN to FALSE does not prevent users from performing proxy logins by omitting the user name from the connect request. If the CS_USERNAME and CD_PASSWORD properties of the CS_CONNECTION structure are omitted users are not prevented from performing proxy logins.

Setting Protection Levels

The user can specify whether the communications with the server are validated or encrypted, or both. "Validated" means that no data was changed or inserted in the communication. In general, the higher the level of protection, the slower the performance.

When a CT-LIB server is started, the OH_PROTN configuration parameter can be used to require a minimum level of protection by all clients. Clients must have a protection level set to this minimum level or to a higher, more restrictive setting, to communicate with the server.

The following table lists the protection levels used by CT-LIB. The order of protection levels is from lowest to highest.

AIX and Solaris Protection Levels	Windows NT Protection Levels	Description
CONNECT	On Connect Only	Lowest level. Protection performed when the client connects with the server. Client and server mutually authenticate when the RPC connection is established. Subsequent calls over the same connection are not individually authenticated.
CALL	On Each RPC Call	Protection performed when the server receives an RPC request. Client and server mutually authenticate on every call. RPC computes a check sum on the protocol header of the first packet to each call to ensure that the header has not been modified. When running over a transport like TCP, this protection level automatically upgrades to Packet.

AIX and Solaris Protection Levels	Windows NT Protection Levels	Description
PKT	On Each Packet	Ensures that data is received from the expected client. Client and server mutually authenticate on every call. Checksum is computed on every packet header.
PKT_INTEGRITY	Each Packet + Verify Data	Ensures that data is received from the expected client and that the data has not been modified. Client and server mutually authenticate on every call. Checksum is computed on both header and user data.
PKT_PRIVACY	Each Packet + Verify Data and Encrypt	Highest level. Performs protection as specified by all previous levels, encrypts data. Client and server mutually authenticate on every call. Checksum is computed on both header and user data. User data is DES encrypted.

Note: Increasing the level of protection might have a significant impact on application performance.

Starting the Database Servers

To start the CT-LIB database servers, do the following:

1. From the **Global Sign-On Plus for Tivoli** window, double-click the **GSO Administration Tasks** icon.
2. From the **GSO Administration Tasks** window, double-click the **Start Server** icon.
3. From the **Execute Tasks** window, select the database server managed node that corresponds to the database you selected in the rc.odbc file.
4. Press the **Execute** button.

Configuring a Client Data Source

Before using CT-LIB, configure a Sybase SQLServer data source on your workstation to use the CT-LIB client (libct.dll). Change options that control how the connection is made (such as level of security, and so on).

1. From the desktop, select **Start -> Programs -> IBM Global Sign-On Client V2.0 -> CTLIB Client -> CTLIB Client Configuration** to display the **Data Sources** window.
2. Press the **Add** button to display the **CTLIB Client Configuration** window.

The following steps apply to the fields shown in the Setup window. The data you enter in this window changes the registry.

3. In the **Data Source Name** field, enter the name specified by your GSO administrator. **The Data Source Name:**
 - Corresponds to the CDS entry of the CT-LIB server
 - Maps to the Sybase SQL Server to which you want to connect
4. In the **Description** field, enter a comment that describes the type of information the database contains. This field is optional.
5. Select a protection level from the **Protection Level** scrolling list. This value specifies the level of security in effect for all communication between the client and the server. Your GSO administrator should give you this value. See “Setting Protection Levels” on page 145 for more information. Note that if the security level chosen is lower than that required by the server, the connection fails.
6. Press the **OK** button to return to the Data Sources window. You can add more data sources. To reconfigure (change) a data source, highlight it and select **Setup**. The Setup window is displayed with the data already filled in.
7. You have configured the data source. Press the **Close** button.

Ensuring the Correct DOS Path to Sybase Executables

The database client is implemented in `libct.dll`.

When a Windows program loads this DLL, Windows searches for the required DLL in the following order:

1. The current directory (the directory where the Windows application resides).
2. The windows directory.
3. The windows\system directory.
4. Each directory in your DOS path.

If it does not find the DLL, it returns an error.

If your workstation has Sybase database client installed, the Sybase executables (and their `libct.dll`) reside in one of the directories in your DOS path. Because `libct.dll` is installed in the `/ibmgso/ctlib/dll` directory, Windows loads this DLL dynamically whenever `ctlib.dll` is required by an application.

Note that the above situation does not prevent Sybase's `libct.dll` from residing in the same directory as the Windows application. Regardless of the current DOS path settings, the application first tries to use the DLLs located in its current directory. In case of problems, take the appropriate action (such as renaming Sybase's `libct.dll` to `libct.syb` or by removing it from that directory).

Testing the Database Connection

When you finish installation and configuration, test your application with the CT-LIB database.

Use the WISQL32.exe tool to test the connection. This tool is available during custom installation of GSO CT-LIB client.

Using the Trace Utility

There is a trace utility included with the CT-LIB client database. This executable file (ohtrace.exe on Windows 95 and ohtrc32.exe on Windows NT) is installed in the /ibmgso/ctlib/bin directory.

CT-LIB Server Configuration Parameters

The following table summarizes the parameters that users can set in the CT-LIB database environment. The file containing these values is the ohctlibs.ini.

Configuration Parameter	Value/Description
OH_CDS_NAME	<p><database_name></p> <p>Use the name that users will use to identify the SQL Server. The default value is the value of the DSQUERY environment variable.</p>
OH_DB_ADMIN	The user ID that logs users in to the database. This ID needs to have the privilege to alter other user's passwords. This parameter is required.
OH_DB_ADMIN_PASSWORD	This required parameter is the password for the OH_DB_ADMIN principal.
OH_MAXSVR	<p>An integer</p> <p>(default=100)</p> <p>Server only. Maximum number of concurrent connections allowed by the server.</p>
OH_ENFORCE_PROXY_LOGIN	<p>TRUE</p> <p>FALSE</p> <p>(default=TRUE)</p> <p>Server only. See "Setting Proxy Logins" on page 144 for a complete explanation. This parameter defines whether only proxy logins are allowed, or alternatively, if you can connect to an Oracle account that is different from your GSO user ID when a valid password is supplied.</p>

Configuration Parameter	Value/Description
OH_MULTITHREADED_SERVER	<p>TRUE</p> <p>FALSE</p> <p>(default=FALSE)</p> <p>Set to TRUE to have master and replica processes handle multiple concurrent requests from clients.</p>
OH_MASTER_AS_SERVER	<p>TRUE</p> <p>FALSE</p> <p>(default=FALSE)</p> <p>Set to TRUE to have master processes handle multiple concurrent database requests from clients. Use this parameter only when OH_MULTITHREADED_SERVER is set to TRUE.</p>
OH_THREADSAFE_RUNTIME	<p>TRUE</p> <p>FALSE</p> <p>(default=FALSE)</p> <p>Server only.</p> <p>Set to TRUE to have multiple simultaneous requests presented to database client runtime by master of replica processes.</p> <p>Use this parameter only when</p> <p>OH_MULTITHREADED_SERVER is set to TRUE.</p>

Configuration Parameter	Value/Description
OH_PROTN	CONNECT CALL PKT PKT_INTEGRITY PKT_PRIVACY default=CONNECT Server and Client. See "Setting Protection Levels" on page 145 for a complete description. These values are listed in increasing levels of security. The client must set OH_PROTN to a level that matches or exceeds that of the server.
OH_MESSAGE_BASE	<numeric value> (default = 20,000) This value is added to the message numbers and might be set differently for the database client and server.
OH_LISTEN_THREADS	<numeric value> (default = 10) Set this value to the number of users you expect to use the CT-LIB server simultaneously. Valid values are whole integers between 1 and the limit set by the max_calls_exec parameter of the DCE function rpc_server_listen.
OH_APPLICATION_AUTHN	TRUE FALSE When set to TRUE, the server connects only to authorized applications.

Parameter Changes

OH_OPTIMIZE_NETWORK

Valid settings for this parameter are TRUE and FALSE. Setting this parameter to FALSE disables this facility. The default setting is FALSE.

When set to TRUE, this parameter optimizes network round trips, improving application performance.

With OH_OPTIMIZE_NETWORK on, the database client function `ct_get_data` cannot be used on `CS_COMMAND`. Remove this parameter, or set it to FALSE if the client program uses this function.

This parameter also causes the CT-LIB database client to bundle multiple database client calls together in a single RPC, where appropriate, in order to reduce network traffic. As a result of this optimization, error messages might be presented to callback functions in a manner different from how it functions in the native database client. For example, if OH_OPTIMIZE_NETWORK=TRUE, `ct_command` and `ct_send` are bundled together into the same network round trip. If an error is returned to the CT-LIB server as a result of the `ct_command` call, it is presented to the client after the `ct_send` call.

If your application requires that error presentation conform with database client, specify `OH_OPTIMIZE_NETWORK=FALSE`, or remove this parameter from the client's environment.

Resolving CT-LIB Issues and Known Problems

The following information provides some help regarding existing database issues.

AIX and Solaris Servers

If you have many clients trying to connect at the same time, some of them might fail to connect to the CT-LIB server.

To avoid this problem increase the UNIX file descriptions limit. The default setting is usually 64. Your UNIX (AIX and Solaris) system administrator must reset the file descriptors limit to a higher value, such as 512. Setting the file descriptors limit to 1024 might decrease your machine's performance.

Sybase Errors

Error messages generated by the Sybase server are returned to the client. The following errors might be generated when your environment is not set up correctly.

No More Bindings (dce/rpc): The server you are trying to connect to cannot be found or is not running. Verify that you are trying to connect to the correct database name, and confirm with your system administrator that there is a CT-LIB server for Sybase running under an identical `OH_CDS_NAME`.

No currently established network identity for specified context(dce/sec): You have not logged on to GSO. Use your client's GSO login utility to establish a connection.

Supported CT-LIB Functions

This section summarizes the currently supported CT-LIB calls.

The columns of this table are defined as follows:

CT-LIB Routine	CT-LIB entry, as documented.
Subfunction	Subfunction of CT-LIB routine.
Comments	Comments pertaining to the CT-LIB entry.

CT-LIB Routine	Subfunction	Comments
ct-bind		<i>locale</i> not supported
ct_callback	Determine by <i>type</i> :	
	CS_CLIENTMSG_CB	Client message callback.
	CS_COMPLETION_CD	Completion callback.
	CS_SERVERMSG_CB	Server message callback.
	CS_NOTIF_CB	Registered procedure notification callback.
ct_cancel		
ct_capability		
ct_close		
ct_cmd_alloc		
ct_cmd_drop		
ct_cmd_props		
ct_command	Determined by <i>type</i> :	
	CS_LANG_CMD	
	CS_MSG_CMD	
	CS_PACKAGE_CMD	
	CD_RPC_CMD	
	CS_SEND_DATA_CMD	
ct_compute_info		
ct_con_alloc		
ct_con_drop		
ct_con_props		See Properties, below.
ct_config		See Properties, below.
ct_connect		
ct_cursor		

CT-LIB Routine	Subfunction	Comments
ct_data_info		Locale not supported.
ct_describe		Locale not supported.
ct_diag		
ct_dynamic		
ct_exit		
ct_fetch		
ct_get_data		
ct_init		
ct_options		
ct_param		
ct_poll		
ct_res_info		
ct_results		
ct_send		
ct_send_data		Locale not supported.
ct_wakeup		

Appendix D. Product Packages on the GSO CDs

This appendix lists the product packages and related information that is provided with GSO.

Server Packages

The following server packages are included with GSO on the Server CD labeled **CD-ROM 1 (Server)**.

For Windows NT:

- **OCI DB server**
CD location: \nt\db\oci
- **ODBC DB server**
CD location: \nt\db\odbc
- **IBM DCE server**
CD location: \nt\dce
- **GSO server**
CD location: \nt\gso

For Solaris (DES only):

- **OCI DB server**
CD location: /solaris/db/IGSOoci
- **CTLIB DB server**
CD location: /solaris/db/IGSOctlib
- **ODBC DB server**
CD location: /solaris/db/IGSOodbc
- **Transarc DCE 1.1**
CD location: /solaris/dce
- **GSO server**
CD location: /solaris/gso/IGSOsrvr

For AIX:

- **OCI DB server**
CD location: /usr/sys/inst.images
- **CTLIB DB server**
CD location: /usr/sys/inst.images
- **ODBC DB server**
CD location: /usr/sys/inst.images
- **IBM DCE 2.2 server**
CD location: /usr/sys/inst.images

- **GSO server**
CD location: /usr/sys/inst.images

For Tivoli:

- **Tivoli/Plus GSO module**
CD location: /tme/gso/plus
- **Tivoli User Admin GSO module**
CD location: /tme/gso/user

Client Packages

The following client packages are included with GSO on the Windows NT/95 Client CD labeled **CD-ROM 2 (Windows NT/95 Client)**:

For Windows NT:

- **CTLIB DB**
CD location: \db\ctlib
- **OCI DB client**
CD location: \db\oci
- **ODBC DB client**
CD location: \db\odbc
- **NetSEAT DCE client**
CD location: \dce
- **GSO client**
CD location: \gso\nt
- **GSO Smart Card Administration**
CD location: \gso\smcard\admin

For Windows 95:

- **CTLIB DB**
CD location: \db\ctlib
- **OCI DB client**
CD location: \db\oci
- **ODBC DB client**
CD location: \db\odbc
- **NetSEAT DCE client**
CD location: \dce
- **GSO client**
CD location: \gso\w95
- **GSO Smart Card Administration**
CD location: \gso\smcard\admin

The following client packages are included with GSO on the OS/2 Client CD labeled **CD-ROM 3 (OS/2 Client)**:

- **GSO client**
CD location: \gso\
Where <language> can be one of the following:
 - de_de for German
 - en_us for U.S. English
 - es_es for Spanish
 - ja_jp for Japanese
 - ko_kr for Korean
 - pt_br for Brazilian Portugese
 - zh_cn for Simplified Chinese
 - zh_tw for Traditional Chinese
- **IBM DCE client**
CD location: \

GSO Information

The following books are provided as part of the IBM Global Sign-On package.

Printed Information

This book, *IBM Global Sign-On Installation and Server Management Guide*, and the *IBM Global Sign-On User Administration Guide* are provided in printed format.

Online Information

The following books are provided online on each GSO client. You can access each book through the **Start** menu on the taskbar.

- *IBM Global Sign-On Administration Help*
- *IBM Global Sign-On Help*
- *IBM Global Sign-On Command Reference*
- *IBM Global Sign-On Programming Guide* (Also available in \docs\program.ps)

Readme Files

The Server CD README file is located in the root directory.

The following README files are included on the GSO Client CD:

- **U.S. English**
CD location: \READMEs\README.enus

- **German**
CD location: \READMEs\README.dede
- **Spanish**
CD location: \READMEs\README.eses
- **Brazilian Portugese**
CD location: \READMEs\README.ptbr
- **French**
CD location: \READMEs\README.frfr
- **Japanese**
CD location: \READMEs\README.jajp
- **Korean**
CD location: \READMEs\README.kokr
- **Simplified Chinese**
CD location: \READMEs\README.zhcn
- **Traditional Chinese**
CD location: \READMEs\README.zhtw

GSO Code Page Compatibility

The GSO product is national language support (NLS) enabled. Windows NT/95, and OS/2 support different code pages. To accommodate all clients, make sure you use only the portable character set (PCS) to create strings such as user IDs, passwords, host names, domain names, and application names that are stored in the GSO server database.

The portable character set includes the following characters:

```

0 1 2 3 4 5 6 7 8 9
: ; < = > ? @ [ \ ] ^ _ ` ' - { | } ! " # $ % & ( ) * + , - . /
<space>
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

```

Note that some fields can further restrict the allowable characters beyond this list. For example, < and > are not permitted in file paths or file names.

Appendix E. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

Trademarks

The following are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AS/400
AIX
DB2
IBM

Global Sign-On
OS/2
RACF

Intel is a trademark of Intel Corporation in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

Solaris is a trademark of Sun Microsystems, Inc. in the United States and/or other countries.

Tivoli is a registered trademark of Tivoli Systems, Inc..

UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Index

Special Characters

\$OH_HOME/admin directory 108

A

AIX managed nodes
 special considerations 10
application authentication
 configuring using Windows NT 118
 definition 118
authenticating users
 CT-LIB 144
 OCI 132
 ODBC 119

B

backup cell 44
bc500rtl.dll 135
books
 GSO 157
 OS/2 client 105

C

CDMF 13
cells
 backing up 44
 definition 3
 removing machine from 46
 restoring 45
cfgclient command
 -?|-h 104
 -config 99
 -login 101
 -logindev 102
 -view 103
client
 configuring 40
 configuring Windows NT/95 using command 99
 installing 34
 installing without software distribution 97, 98
client data source
 configuring for CT-LIB 146
 configuring for OCI 134
 configuring for ODBC 122
code page compatibility 158
command, cfgclient
 -?|-h 104
 -config 99
 -login 101
 -logindev 102
 -view 103

command line
 installing 19
commercial data masking facility (CDMF) 13
components, GSO 4
configuration parameters
 defining for CT-LIB 140
 defining for OCI 126, 136
 defining for ODBC 108
configuring
 client on Windows NT/95 using command 99
clients 40
 CT-LIB client data source 146
 CT-LIB server 139
 database server 39
 master server 37
 OCI client data source 134
 OCI on Windows NT 130
 OCI server 126
 ODBC client data source 122
 ODBC on Windows NT 117
 ODBC server 108
 replica server 38
configuring environment
 OCI servers 130
 ODBC servers 111
configuring file packages
 for the client 28
 for the database client 32
 for the database server 30
 for the server 26
connect string syntax 136
creating
 GSO targets 42
 GSO users 42
CT-LIB
 authenticating users 144
 configuration parameters 140, 148
 configuring client data source 146
 configuring on AIX and Solaris 139
 know problems 151
 parameter changes 150
 protection levels, setting 145
 security, implementing 144
 starting database servers 146
 supported functions 152
 Sybase errors 151
 testing connection 147
 trace utility, using 148

D

data encryption standard (DES) 13

- database account
 - creating a special for CT-LIB 143
 - creating a special for OCI 128
 - creating a special for ODBC 115
- database server monitors monitoring profile 59
- databases
 - configuring servers 39
 - custom configuration 114
 - DB2, customizing 114
 - description 107
 - Informix 115
- DB2
 - customizing 114
 - environment 114
 - Informix proxy logins 121
 - post installation 112
- DES 13
- disk space requirements 6
- display current client 103
- distribution return codes 11

E

- encryption 133
 - CDMF 13
 - DES 13
- enterprise console
 - adding to an existing rule base 83
 - creating a new rule base 83
 - setting up 82
- enterprise event management
 - configuration activity 81
 - configuring GSO event adapter 84
 - events and rules 85
 - introduction 81
 - setting up enterprise console 82
 - summary of GSO monitor event classes 93
 - SVC event class 93
 - unconfiguring GSO event adapter 94
- event adapter
 - configuring 84
 - disabling 55
 - enabling 54
 - unconfiguring 94
- event classes 93
- events and rules 85
 - DCE serviceability 91
 - server monitor 85

F

- file packages
 - for the client 28
 - for the database client 32
 - for the database server 30
 - for the server 26
- free seating 2

H

- hardware requirements 6
- hidden task library 76

I

- icons, Tivoli/Plus 23
- information
 - online 157
 - printable 105
 - printed 157
- Informix
 - customizing database 115
 - DB2 and proxy logins 121
 - DB2 proxy logins 121
 - environment 115
- installing
 - client 1.5 on OS/2 Warp 98
 - client on Windows NT/95 without software distribution 97
 - clients using Software Distribution 34
 - from the command line 19
 - from the desktop 15
 - introduction 15
 - on the TMR server 18
 - servers 34
 - smart cards 95
 - starting a module 20
 - user administration extension 17
- integrated login
 - disabling via interface 53
 - enabling via command 101
 - enabling via interface 53
- interface file, using 144
- ISQL 143

L

- levels of user authority 2
- libct.dll 147
- library, hidden task 76
- litronic smart card
 - disabling 54
 - enabling 53

M

- managed node 3
- managed resources 3
 - policies 3
- master server
 - configuring 37
 - moving 50
- module
 - starting 20
- monitor probes
 - server audit files size 62
 - server checkpoint space available 62

monitor probes (*continued*)
 server disk space used 61
 server file size 61
 server up 60
monitored resources 59
move master server 50

N

NT managed nodes
 special considerations 10

O

OCI

 authenticating users 132
 changes to Oracle tools 136
 configuration parameters 126, 136
 configuring client data source 134
 configuring in Windows NT 130
 configuring on AIX and Solaris 126
 connect string syntax 136
 Oracle, correct path 135
 security, implementing 132
 starting database server 134
 starting database servers 129
 testing connection 136
 trace utility, using 131

ODBC

 authenticating users 119
 configuration parameters 108, 122
 configuring client data source 122
 configuring in Windows NT 117
 configuring odbc.ini file 113
 configuring on AIX and Solaris 108
 configuring the drivers 111
 configuring the environment 111
 connecting to DB2 RDBMS 114
 connecting to Informix RDBMS 115
 connecting to Oracle RDBMS 116
 known problems 125
 linking the Oracle drivers 112
 post installation 112
 protection levels, setting 119
 proxy logins 109
 security, implementing 118
 starting database servers 116, 122
 supported functions 125

OH_APPLICATION_AUTHN 131

OH_CDS_NAME 109, 126, 127

OH_DB_ADMIN 109, 140

OH_DB_ADMIN_PASSWORD 109

OH_DBNAME 109, 114, 115, 116

OH_ENFORCE_PROXY_LOGIN 109

 CT-LIB databases 141

 OCI databases 127

 ODBC databases 121

OH_MASTER_AS_SERVER 141

OH_MAXSVR 110, 127, 141

OH_MESSAGE_BASE 142

OH_MULTITHREADED_SERVER 141

OH_PEOPLESOFT 127, 131

OH_PROTN 110, 126, 141

OH_PROXYPREFIX 132

ohodbc.ini 108, 110

ohorizon directory 129

ohres.dll 135

ohsec.sql 129

online information

 DCE 105

 GSO 157

ora71win.dll 135

ora7win.dll 136

Oracle

 associating with OCI server 126

 correct path, OCI 135

 creating database account for OCI 128

 creating database account for ODBC 115

 environment 116

 known problems 139

 linking ODBC driver 112

 proxy logins 121

 using tools, OCI 136

ORACLE_SID 126

OS_AUTHENT_PREFIX 115

overview and planning

 cells and managed resources 3

 concepts 2

 introduction 1

 requirements 6

 supported platforms 5

P

packages

 client CD 156

 server CD 155

parameters

 configuring CT-LIB servers 140

 configuring OCI servers 126, 136

 configuring ODBC servers 108, 122

passticket 2

password 2

 resetting 48

 setting policy 47

PC managed nodes

 distribution return codes 11

 special considerations 10

PeopleSoft 127

policies 3

prerequisites 6

printable documentation 105

- program template files (PTF) 2
- programs 2
- protection levels
 - encryption 133
 - setting for CT-LIB 145
 - validation 133
- proxy logins
 - authenticating CT-LIB users 144
 - authenticating OCI users 132
 - authenticating ODBC users 119
 - CT-LIB databases 141, 144
 - DB2 and Informix databases 121
 - DB2 databases 114
 - Informix databases 115
 - OCI databases 127
 - ODBC databases 109, 121
 - Oracle databases 121
- PTF 2
- R**
- RAM requirements 6
- recover replica 52
- replica server
 - configuring 38
 - converting to a master server 50
 - recovering 52
 - synchronizing 49
- requirements
 - additional considerations 13
 - hardware 6
 - prerequisites 7
 - RAM and disk space 6
 - software 7
- resource monitoring
 - introduction 57
 - monitored resources 59
 - using GSO monitors 57
 - viewing the status of monitored resources 58
- S**
- security roles 2
- server monitors monitoring profile 59
- servers
 - configuration parameters for CT-LIB 140
 - configuration parameters for OCI 126, 136
 - configuration parameters for ODBC 108, 122
 - implementing security on CT-LIB 144
 - implementing security on OCI 132
 - implementing security on ODBC 118
 - installing 34
 - prerequisites 8
 - security, implementing 118
 - starting 43
 - starting CT-LIB database 146
 - starting OCI database 129, 134

- servers (*continued*)
 - starting ODBC database 116, 122
 - stopping 43
- single login 132
- smart card
 - disabling 54
 - enabling 53
 - installing 95
 - prerequisites 95
 - set up via command 102
- software distribution
 - configuring file packages 25
 - creating users and targets 42
 - installing servers and clients 34
 - introduction 25
- software requirements
 - client prerequisites 8
 - server prerequisites 8
- Solaris managed nodes 8
- special considerations
 - AIX managed nodes 10
 - client/server time synchronization 12
 - NT managed nodes 10
 - PC managed nodes 10
 - replica servers 12
 - Solaris managed nodes 8
- SQL*DBA 115, 116, 129
- SQL*Plus 136
- status, viewing monitored resources 58
- string syntax, connecting 136
- summary of GSO monitor event classes 93
- supported platforms 5
- SVC event class 93
- Sybase 139
 - associating with CT-LIB server 140
 - correct DOS path 147
 - creating database account 143
 - environment variable 144
 - errors 151
 - interface file, using 144
- synchronization, time 12
- synchronizing servers 49

- T**
- targets
 - concept 2
 - creating 42
 - GSO supports 5
- time synchronization 12
- trace utility
 - CT-LIB database, using 148
 - OCI database, using 131

U

UNIX

monitors monitoring profile 59

user administration extension

installing 17

users, creating GSO 42

using GSO monitors 57

V

validation 133

viewing the status of monitored resources 58



Part Number: GC320284



Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC32-0284-00



GC320284

