Oracle® Secure Backup

Readme

Release 10.1.0.3

B32518-01

January 2007

Purpose of this Readme

This Readme document applies only to Oracle Secure Backup Release 10.1.0.3. This Readme documents licensing, supported platforms and devices as well as known and fixed issues.

Documentation

For documentation, use your Web browser to access the Oracle Secure Backup documentation library. The library home page is named `index.htm` and is located in the `doc` directory of your CD-ROM image. You can also access the library online at the following URL:

`http://www.oracle.com/technology/documentation/`

Contents

1 CD-ROM Image Contents

The CD-ROM image for each platform contains all necessary tools, documentation, and software to install and operate Oracle Secure Backup on the selected platform.

> **Note:** Each supported platform requires its own separate CD-ROM or installation Zip file. For example, if you are running an administrative domain using both Windows and Linux clients, you require separate installation media (CD-ROM or downloaded Zip file) for Windows and for Linux.

You can access the installation files from a physical CD-ROM or through a Zip file downloaded from the following product site:

http://www.oracle.com/technology/products/secure-backup/

The contents of the CD-ROM and Zip file for a given platform are identical.

2 Release Components

The only product in this release is Oracle Secure Backup.

3 Licensing Information

Refer to *Oracle Secure Backup Licensing Information* for licensing terms.

4 Upgrading Existing Oracle Secure Backup Installations to 10.1.0.3

In an upgrade installation, all information that is part of the administrative domain is retained, including backup catalogs, host data, user data, device configuration and scheduled jobs. This data is stored in the `admin` directory under the Oracle Secure Backup home on your administrative server.

Note: Oracle recommends backing up the administrative server prior to any upgrade of Oracle Secure Backup.

Before upgrading an existing Oracle Secure Backup administrative domain to 10.1.0.3, you must shut down Oracle Secure Backup-related drivers and background processes on all hosts. Upgrade the administrative server, host first, and then the other hosts in the domain.

Brief instructions on each step are described in the following sections.

4.1 Preparing Administrative Domain Hosts for Upgrade Installation of Oracle Secure Backup

Before performing an upgrade installation, you must stop the Oracle Secure Backup-related daemons and services on all hosts in your administrative domain.

On Linux or Unix, use the `ps` command to identify the Oracle Secure Backup daemon processes:

```
# /bin/ps -ef | grep ob
```

Use the `kill -9` command to stop each process.

On Windows hosts, you must stop the Oracle Secure Backup Services service, and, on media servers, disable the Oracle Secure Backup device driver.

To disable the driver, in Device Manger, under Tape Drives, right-click **Oracle Secure Backup Device Driver**, and select **Disable**. Then reboot the system.

To stop the Oracle Secure Backup Services service, open the Services applet, right-click the **Oracle Secure Backup Services** service, and select **Stop**.

4.2 Upgrade Installation of Oracle Secure Backup on Windows

To upgrade a Windows installation of Oracle Secure Backup, follow the Windows installation process described in *Oracle Secure Backup Installation Guide*.

The Oracle Secure Backup installer takes all necessary steps to upgrade your existing installation. During the Windows upgrade process, the installer displays messages referring to uninstalling the previous version. Uninstalling the previous version of Oracle Secure Backup is part of the normal upgrade process.

Note: On a Windows administrative server, the uninstaller program displays the following prompt:

```
This system was configured as an Oracle Secure Backup
Administrative Server.

Oracle Secure Backup creates files specific to this administrative
domain in the "admin" directory.
Would you like to keep these files in case you reinstall Oracle
Secure Backup?

If you choose "Delete" all files related to Oracle Secure Backup
will be removed from this system.
If you choose "Keep" the files specific to this administrative
domain will be retained.
```

Click **Keep** to upgrade and preserve your administrative domain data.

There are some special cases for upgrades which require attention, as described below:

- Upgrading Oracle Secure Backup from 10.1.0.0 on Windows
- Windows Installer Does Not Support Modify or Repair Installation Options
- Upgrading Windows 64-Bit Systems: Manually Delete orasbt32.dll

Complete the rest of the installation process as described in *Oracle Secure Backup Installation Guide*.

Note: Usually, you should specify the same host roles for each host as were used in the previous installation.

4.2.1 Upgrading Oracle Secure Backup from 10.1.0.0 on Windows

When uninstalling Oracle Secure Backup on a Windows administrative server, the uninstaller allows you to click **Keep**, to keep files containing the record of your administrative domain and backups for use by a future installation of Oracle Secure Backup, or **Delete**, to delete these files and create a new administrative domain in a future installation.

However, the uninstaller from version 10.1.0.0 for Windows (32-bit and 64-bit platforms) does not correctly keep these files, if you run the uninstaller directly. The administrative domain configuration is deleted, even if you choose **Keep**.

To preserve the current Oracle Secure Backup configuration, just run the Windows installation program for the new version, without performing an

explicit uninstall of version 10.1.0.0. Do not run the uninstaller for release 10.1.0.0 directly, and do not use the Add/Remove Programs option in the Windows Control Panel to uninstall release 10.1.0.0. The Oracle Secure Backup uninstaller takes all necessary steps to upgrade to the new version, including uninstalling the 10.1.0.0 installation and preserving your administrative domain.

4.2.2 Windows Installer Does Not Support Modify or Repair Installation Options

If you run the installer for Oracle Secure Backup for Windows (all versions) on a system with the same version already installed, the installer displays the **Modify**, **Repair** and **Remove** options. Only the **Remove** option is correctly supported. Do not use the **Modify** or **Repair** options in the installer when installing in place over an existing installation.

4.2.3 Upgrading Windows 64-Bit Systems: Manually Delete orasbt32.dll

When upgrading an existing Windows 64-bit installation of Oracle Secure Backup release 10.1.0.0 to release 10.1.0.2, the Microsoft Installer reports an internal error, if the file `C:\Windows\system32\orasbt.dll` is present when you run the Windows installer for Oracle Secure Backup release 10.1.0.2. Therefore, delete this file manually before running the installer for Oracle Secure Backup release 10.1.0.2.

Note: If the Windows installation directory is stored in some location other than the default `C:\Windows`, then delete the file in the `System32` subdirectory of the Windows installation directory.

4.3 Upgrade Installation of Oracle Secure Backup on Linux or Unix

To upgrade a Linux or Unix installation of Oracle Secure Backup, follow the setup and installation process described in *Oracle Secure Backup Installation Guide*.

During the upgrade process, the installer displays the following prompt:

```
Oracle Secure Backup is already installed on this machine (myhostname-sun2).
Would you like to re-install it preserving current configuration data[no]?
```

Enter `yes` to perform the upgrade installation, retaining your previous configuration.

5 Outstanding Bugs and Known Issues

The following sections describe outstanding bugs and known issues with Oracle Secure Backup.

5.1 Manually Start Oracle Secure Backup Services After Installation (Windows)

On Windows Server 2003 and Windows 2000, on hosts that are only configured for the media server or client roles, the Oracle Secure Backup Services service is not started automatically after installation. You must start it manually.

Note:

- This issue does not apply to Windows XP.
- This issue does not apply to hosts configured for the administrative server role.
- This issue only occurs immediately after the installation. The service is started automatically whenever Windows is rebooted.

To start the Oracle Secure Backup Services service, open the Services applet, right-click the **Oracle Secure Backup Services** service, and select **Start**.

5.2 Using Upper-Case Letters in the Job Summary Title Prevents E-Mail Notification (Windows)

On Windows administrative servers, if the title for a backup job contains upper case characters, email notification of the backup job summary fails.

5.3 Setting Permissions for Generic SCSI Device Files (SUSE)

On SUSE Linux, permissions for the Generic SCSI device files `/dev/sg0 -/dev/sg31` and `/dev/sga - /dev/sgp` must be changed from 640 to 666 for Oracle Secure Backup to operate properly.

5.4 Bidirectional PNI Support

The Preferred Network Interface (PNI) capability supports bidirectional specification of communication between hosts. The PNI behavior is described below.

In cases where hosts have more than one network interface, you can specify which interface is used to transmit data to be backed up or restored between hosts by configuring Preferred Network Interface (PNI) settings for each host.

Configuring host A to specify a Preferred Network Interface on host B identifies the network interface on host B to use when host A and host B communicate.

When host A attempts to establish a connection with host B, the PNI settings on host A and host B are applied in the following manner:

- Host A queries the administrative server for the PNI settings configured for host B, to see if a specific interface on host B should be used for transfers from host A. If an interface at host B is specified for communications with host A, then it is used for the transfer.
- Host A also queries the administrative server for the PNI settings configured for host A, to see if a specific interface is preferred for transfers to host B. If an interface at host A is specified for communications with host B, then it is used for the transfer.

For example, suppose the host storabck10 has the following PNI setting configured:

```
ob> lspni
storabck10:
    PNI 1:
```

```
interface:        storabck10-rac
clients:          stacx53
```

When the host stacx53 connects to storabck10, it consults the configured PNI settings and determines that it must connect over the interface on storabck10 named storabck10-rac.

Now suppose that storabck10, acting as a client, wants to connect to a device connected to stacx53 (that is, stacx53 is now acting as a media server). storabck10 also references the PNI settings for both hosts, and discovers that it should use the local interface storabck10-rac in order to establish the connection with stacx53.

The `obtar` command reports which interfaces are in use for a connection between `obtar` and a remote backup device. To display this information in the `obtar` transcript, use the `-J` option on the `obtar` command line, or as part of the `backupoptions` policy. In the example above, the connection would be shown as:

```
09:38:38 A_O: sock 8 connects (local) storabck10.rac to (remote) stacx53
```

5.5 Creating Attach Points for Solaris 10 Fibre Channel Devices

As of release 10.1.0.3, Oracle Secure Backup now supports the use of Fibre Channel-attached tape devices on media servers running Solaris 10. However, the `install` script and `makedev` utility cannot be used to create the needed links in /dev to the device special files for such devices.

During installation, the Oracle Secure Backup driver automatically identifies Fibre Channel-attached devices by their World Wide Names. After installing the driver, you must determine the World Wide Name for each device, and then manually create symbolic links in `/dev` that point to the actual attach points for the devices.

To create device special files for Solaris 10 tape devices:

1. Run the Oracle Secure Backup `install` script on your media server.

   Note: When the Oracle Secure Backup driver is installed, the `install` script prompts:

   ```
   NOTE: The Oracle Secure Backup device driver has been successfully
   installed.
   Would you like to configure (or reconfigure) any Oracle Secure
   Backup devices that
   are attached to dlsun1976 [no]?
   ```

   Enter `no`.

2. After `install` completes, run the `dmesg` command and examine the output. The Oracle Secure Backup driver adds messages to the log that contain the World Wide Names for the Fibre Channel-attached tape devices. The attach points for tape drives contain the string `sgen`. The attach points for tape libraries contain the string `st`.

For example, the following output contains the World Wide Names and corresponding attach points for a tape drive and a tape library:

```
Dec 12 17:12:53 storabck22 scsi: [ID 799468 kern.info] ob30 at fp0: name
w500308c162680e24,1, bus address 6119e8
Dec 12 17:12:53 storabck22 genunix: [ID 936769 kern.info] ob30 is
/pci@1f,4000/fibre-channel@2/fp@0,0/sgen@w500308c162680e24,1
Dec 12 17:12:53 storabck22 scsi: [ID 799468 kern.info] ob31 at fp0: name
w500308c162680e24,0, bus address 6119e8
Dec 12 17:12:53 storabck22 genunix: [ID 936769 kern.info] ob31 is
/pci@1f,4000/fibre-channel@2/fp@0,0/st@w500308c162680e24,0
```

3. For each device listed in the `dmesg` output, assign an Oracle Secure Backup logical unit number. Create a symbolic link in `/dev` that references the attach point.

   The name for the symbolic link should be `/dev/obt`*n* for tape drives, and `/dev/obl`*n* for tape libraries, where *n* is the Oracle Secure Backup LUN you assigned for the device.

   For example, assume that you assign the devices listed in the output of step 2 the Oracle Secure Backup logical unit number 0. The resulting device names are `/dev/obl0` for the tape library, and `/dev/obt0` for the tape drive. The following commands create the required symbolic links in `/dev`:

```
ln -s /devices/pci@1f,4000/fibre-channel@2/fp@0,0/sgen@w500308c162680e24,1:fp0
/dev/obl0

ln -s /devices/pci@1f,4000/fibre-channel@2/fp@0,0/st@w500308c162680e24,0:fp0 /dev/obt0
```

You can now use the `mkdev` command in obtool or the Oracle Secure Backup Web Tool to add these devices to your administrative domain.

5.6 Globalization Restrictions Within Oracle Secure Backup

The following globalization restrictions apply to Oracle Secure Backup:

- The Oracle Secure Backup Web Tool and command line interface are English-only, and are not globalized. Localizations or multi-byte character set data are not supported. All messages and documentation are in English.
- Oracle Secure Backup does not support filenames or RMAN Backup names that are encoded in character sets that do not support null termination, such as Universal Character Set (UCS).

5.7 Visibility of Oracle Secure Backup Links on the Enterprise Manager Maintenance Page

On a Linux host running Enterprise Manager Database Control or Enterprise Manager Grid Control, support for managing Oracle Secure Backup is not included until you apply the first Oracle Database 10g Release 2 patch set.

Also, in releases 10.2.0.1 and 10.2.0.2 of Enterprise Manager Grid Control and release 10.2.0.2 of Enterprise Manager Database Control, the Oracle Secure Backup section of the Maintenance page is not displayed by default.

Follow the steps in the section "Using Enterprise Manager" in the "Getting Started" chapter of *Oracle Secure Backup Administrator's Guide* to configure

Enterprise Manager to include the Oracle Secure Backup section in the Maintenance page.

Note: In Oracle Secure Backup Release 10.1.0.2, in Database Control, the Oracle Secure Backup section of the Maintenance page may not appear, even after enabling display of Enterprise Manager links using the steps from *Oracle Secure Backup Administrator's Guide*.

The resolution for this problem is described in Metalink note 399826.1.

5.8 Time Synchronization and "failed to validate certificate" Errors

The clocks on the administrative server, clients and media servers must be synchronized to within 60 minutes of each other. If the time skew among hosts in the administrative domain is more that 60 minutes, then you may encounter problems when attempting to issue the `mkhost` command to configure new hosts. The error that appears in the `observiced` log file on the client or media server is "`failed to validate certificate`".

The solution is to synchronize the clock on all hosts in the administrative domain to match the clock on the administrative server, and then retry the failed operation.

5.9 Cannot Edit RMAN-DEFAULT Media Family in Enterprise Manager

You cannot edit the `RMAN-DEFAULT` media family when using Enterprise Manager.

Use the Oracle Secure Backup Web tool or `obtool` to edit the `RMAN-DEFAULT` media family.

5.10 Installing SCSI Generic Driver on Linux

Configuring a Linux host for the Oracle Secure Backup media server role requires that the SCSI Generic driver be installed on that host. The host must also be configured to automatically reload the driver after a reboot.

Kernel modules are usually loaded directly by the facility that requires them, if the correct settings are present in the `/etc/modprobe.conf` file. However, it is sometimes necessary to explicitly force the loading of a module at boot time.

For example, on RedHat Enterprise Linux, the module for the SCSI Generic driver is named `sg`. Red Hat Enterprise Linux checks for the existence of the `/etc/rc.modules` file at boot time, which contains various commands to load modules.

Note: The `rc.modules` should be used, and not `rc.local`, because `rc.modules` is executed earlier in the boot process.

The following commands can be used to add the `sg` module to the list of modules configured to load as `root` at boot time:

```
# echo modprobe sg >> /etc/rc.modules
# chmod +x /etc/rc.modules
```

5.11 Securecomms Security Policy and obtool (Windows)

On Windows platforms, when the `securecomms` security policy is enabled (the default setting), you must be logged in as Administrator (or your logged-in account must belong to the Administrators group) in order to run the Oracle Secure Backup `obtool` command line tool.

5.12 Oracle Secure Backup Driver CPU Usage (Windows 2000)

If you configure the media server role on a Windows 2000 host with no attached media devices, then the operating system will continuously try to load the Oracle Secure Backup driver. Continuously trying to load the driver uses most of the available CPU cycles on that system, and renders the system unusable.

Microsoft has provided a hotfix which should be applied to any Windows 2000 host configured for the media server role. For a description of the Windows 2000 issue that causes this problem and the hotfix that resolves it, refer to the following URL:

`http://support.microsoft.com/default.aspx?kbid=841382`

To avoid this issue, when there are no media devices attached to a Windows 2000 host, do not configure that host for the media server role.

5.13 Interaction of Windows Firewall with Oracle Secure Backup (Windows XP)

The default configuration of the Windows Firewall in Windows XP can block ports used by Windows hosts running Oracle Secure Backup. This can prevent Windows hosts from connecting to other hosts in the administrative domain.

Instructions for configuring the Windows Firewall to not interfere with Oracle Secure Backup are contained in the *Oracle Secure Backup Installation Guide*.

6 Bugs Fixed in Release 10.1.0.3

The following tables list bugs addressed in releases of Oracle Secure Backup since the original 10.1 release.

- Table 1, " Bugs Fixed in Release 10.1.0.3"
- Table 2, " Bugs Fixed in Release 10.1.0.2"

Table 1 Bugs Fixed in Release 10.1.0.3

Bug Number	Description
5575021	**Attach-Point Specification in a Device Restriction Is Not Being Honored** The device restriction for a backup job can include an attach point specification, that can specify both a media device for the backup and a media server to which the tape device is attached. If a tape device had attach points to multiple media servers, then Oracle Secure Backup did not honor the media server specified in the device restriction. It was not possible to consistently predict which media server attached to the device was selected.

Table 1 (Cont.) Bugs Fixed in Release 10.1.0.3

Bug Number	Description
5479541	**Performance Improvement for Oracle Database Backups with Direct I/O in Linux** The I/O buffers used for a database backup were not page aligned. This reduced the performance improvement in Linux with Direct I/O enabled.
5474741	**Cannot Browse Admin Catalogues from a Non-Admin Host** The administrative service catalogues cannot be browsed from a non-admin host in an OSB domain. The `obtool` command `cd -h` *`adminhostname`* from any OSB client resulted in a failure with the error message: `Error: can't read backup section map record - wrong message type received`
5409398	**Junk Characters Seen LSD -LG Output in SUSE 9** In SUSE 9, the output of `lsd -lg` can contain corrupted output characters. In some cases, the corrupted output renders the entire shell session unusable.
5663666	**NDMP Block Size Is Being Incorrectly Set During Backup** When backing up a NAS using NDMP, the blockingfactor and the maxblockingfactor policies must be equal. If they are not equal, then the resulting volume cannot be restored.
5668578	**In Windows, Backup of File with Name Containing CTRL-Z Fails** Backing up Windows files with names containing the CTRL-Z Windows end of file character are now supported correctly.

Table 2 Bugs Fixed in Release 10.1.0.2

Bug Number	Description
4878473	**Very Long Volume IDs Became Corrupted** When a volume ID of 25 or more characters is used, the last six characters are required to be numeric. Previous versions of Oracle Secure Backup did not correctly enforce this requirement and generated Volume IDs that did not end with numeric characters. Oracle Secure Backup now replaces the last six characters of long volume IDs with numeric characters.
5228264	**"Device Already Opened By This Process" Error** When testing whether a locally attached tape device was already in use, Oracle Secure Backup compared the SCSI channel, SCSI ID and SCSI LUN but did not compare the addresses of the SCSI adapters. This meant that a process could not simultaneously open two tape devices whose addresses differed only on adapter address. As a result, backups or other operations failed with a "Device already opened by this process" error if two media devices on different SCSI adapters had the same SCSI channel, SCSI ID and SCSI LUN values.

Table 2 (Cont.) Bugs Fixed in Release 10.1.0.2

Bug Number	Description
5389348	**Windows 2000 Client Host Database Backup Fails with Repeated Warning "unsupported message 0.0 received"** A database backup from a Windows 2000 client could fail with repeated error messages sent to RMAN. The communication between RMAN and the Windows 2000 client was handled incorrectly, and caused repeated zero-length messages to be sent. In this case, the `obproxyd.log` file contained repeated `unsupported message 0.0 received` messages, for each of the zero-length messages sent. This behavior caused the backup to fail. RMAN database backups no longer fail in this manner.
5370286	**"Page Not Found" Errors in Web Tool After Login** Selecting a user password that was a multiple of eight characters long would make the Web tool inaccessible.
5221340	**Can Only Use Lower-Case Letters in Host Names on Windows Administrative Servers** Windows administrative servers now support upper-case letters in host names.
5211979	**Tape Device Debug Logging Can Cause Backup Failures** Restriction on enabling tape device-related debug logging has been removed.
5207935	**RMAN Backup Failed with RMAN-00600 Error** An RMAN database backup could fail when a file system backup job was started by the scheduler during a long-running backup job. This failure no longer occurs.
4398115	**Restriction on Number of Hosts and Tape Drives with Windows Administrative Servers** The previous limitation on the maximum number of hosts and tape drives supported when using a Windows host as administrative server has been removed.
5149059	**Restart Windows Media Servers and Clients When Changing Policy Parameters** It is no longer necessary to restart Windows media servers when changing policy parameters.
5040299	**Database Backup Jobs Fail If Tape Device Becomes Temporarily Unavailable During Backup** If the device becomes available again within the user-configured RMAN resource wait time, then the database backup job will now continue when the tape device becomes available again.
5016065	**Backup of Oracle Sparse Files Fails if Exclude Oracle Files Option is Specified** The backup of a database sparse file of size greater than 2GB now succeeds on Linux when the backup excludes database temporary files.
4924506	**Device Restrictions Cannot Be Removed Via Web Browser** Web tool can now remove device restrictions
4736477	**Obtool LSBU Command Not Handling '\' in Path** Obtool now supports the backslash character `\` in path names.

Table 2 (Cont.) Bugs Fixed in Release 10.1.0.2

Bug Number	Description
5353546	**Administrative Server Role Not Supported on Non-English Windows Installations** Oracle Secure Backup can now be successfully configured as an administrative server on supported non-English versions of Windows. Previous limitations have been removed.

7 Supported Tape Devices and Platforms

Supported platforms, web browsers and NAS are listed on Certify on Metalink, at the following URL:

http://metalink.oracle.com/

Tape drive and library matrixes are available at the following URL:

http://www.oracle.com/technology/products/secure-backup/

8 Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Oracle Secure Backup Readme, Release 10.1.0.3
B32518-01

with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.