Oracle® Fail Safe

Release Notes

Release 3.4.1 for Microsoft Windows

E10719-04

November 2008

This document describes the new features in this release, software errors fixed, software compatibility, hardware compatibility, and notes about installation and deinstallation.

1 How These Notes Are Organized

The remainder of these release notes are divided into the following sections:

2 Certification Information

The latest certification information for Oracle Fail Safe is available on Oracle*MetaLink* at:

`https://metalink.oracle.com`

Support for Microsoft Windows Server 2008

Oracle Fail Safe is certified on Windows Server 2008 starting with the 3.4.1.1 patch set for 32-bit and 3.4.1.2 for 64-bit.

To ensure that only trusted applications run on your computer, Windows Server 2008 provides User Account Control. If you have enabled this security feature, then,

depending on how you have configured it, Oracle Universal Installer prompts you for either your consent or your credentials during the install.

3 New and Changed Features

This release of Oracle Fail Safe provides the new and changed features described in the following sections:

3.1 Support for Oracle Database 11*g*

This release introduces support for Oracle Database 11*g*, excluding the Management Agent. See "Software Compatibility" for details about the supported version of each of these resources.

3.2 Sample Database Seed Files No Longer Included in Installation

In prior releases of Oracle Fail Safe a database seed (`.DFB`) file was included in the Fail Safe installation kit for each supported release of Oracle Database. Those files are no longer included. When a sample database is created by Oracle Fail Safe the database seed file in the Database Configuration Assistant template directory is used.

For example, in previous releases of Oracle Fail Safe, when creating a sample database for Oracle Database 10*g* Release 2, the file `Oracle_Fail_Safe_Sample_102.dfb` would be copied to the Database Configuration Assistant templates directory, *`ORACLE_HOME`*`\assistants\dbca\templates`, and Database Configuration Assistant would be invoked to create the sample database. With this release the template file provided by the Oracle Database installation, `Seed_Database.dfb`, is used instead.

Using the Database Configuration Assistant template seed file ensures that the template file is compatible with the installed version of Oracle Database.

3.3 New Surrogate Process Trace Log

In prior releases, when the Oracle Fail Safe trace facility was enabled, the Fail Safe Server (FSS) trace file would sometimes get overwritten when remote operations were invoked from other nodes.

> **See Also:** Section B.3, "Tracing Oracle Fail Safe Problems" in *Oracle Fail Safe Concepts and Administration Guide* for a description of the trace facility

This problem would occur because two different processes were using the same trace file definition, `FSS_TRACE_OUTPUT`. The Fail Safe Server (`FsSvr.exe`) is the intended user of the log file, but the file would also be opened and written to by ephemeral Fail Safe surrogate processes (`FsSurrogate.exe`) that would be invoked by the Microsoft DCOM subsystem. When those processes were invoked they would create a new copy of the trace file, deleting the contents created by the main Fail Safe Server.

In this release of Oracle Fail Safe, a new registry entry has been created that enables the surrogate process to have its own trace file specification, eliminating the chance that the surrogate would overwrite trace files. Refer to Section B.3 in *Oracle Fail Safe Concepts and Administration Guide* for more information on how to utilize this new feature.

3.4 Support for Oracle Management Agent

Release 3.3.4 introduces support for Oracle Management Agent. It continues to provide support for the following Oracle resources:

- Oracle Database
- Oracle Intelligent Agent (release 9.2 and earlier)

See "Software Compatibility" for details about the supported version of each of these resources.

> **See Also:** Chapter 9, *Oracle Fail Safe Concepts and Administration Guide* for details on configuring Oracle Management Agent for high availability

3.5 Support for Oracle Application Server Components for Microsoft Windows (32-Bit)

Prior to release 3.3.4, to configure Oracle Application Server components for high availability, you had to configure them as generic services. With this release, custom support for configuring Oracle Application Server components is provided. The following components are included:

- Oracle Process Manager and Notification Server (OPMN)
- Application Server Control service
- The metadata repository, if it is in the Oracle home where Oracle Application Server was installed

> **See Also:** Chapter 10, *Oracle Fail Safe Concepts and Administration Guide* for details on configuring Oracle Application server components for high availability

3.6 Oracle HTTP No Longer Supported

Unlike previous releases, this release of Oracle Fail Safe does not include support for configuring Oracle HTTP Server for high availability.

4 Software Errors Fixed

This section describes software errors that have been fixed in this release of Oracle Fail Safe.

4.1 Oracle Services for MSCS Security Setup Fails On Non-English Systems

On systems that do not have English as the default language, if the Microsoft local culture definition did not recognize the string "`Self`" as representing the current user, then the Oracle Services for MSCS Security Setup tool (`FsSecurity.exe`) would fail to correctly update the DCOM security settings on the system. When this problem was encountered, a message would be entered into the Windows Application event log with the text:

```
Failed to look up user account SELF with error: 1332
Unable to add SELF to DCOM access ACL.
```

The problem was due to the `FsSecurity.exe` application attempting to use the string "`Self`" for the generic self user ID. That string may not be meaningful on non-English cultures.

This problem can be avoided by temporarily removing the DefaultAccessPermission ACL from the windows registry (`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole`), running the MSCS Security Setup tool, and then adding back the DefaultAccessPermission ACL. This operation must only be executed by system administrators that understand the risks of manually editing the Windows registry and know how to backup and recover it.

`FsSecurity.exe` has been changed to build the security identifier (`SID`) in binary form using predefined constants rather than attempting to use the string "`Self`". This change allows `FsSecurity.exe` to be culture independent when adding SIDs to the DCOM DefaultAccessPermission ACL.

4.2 Standby Database Would Not Stay Online

A database that was configured as a Data Guard standby database would not stay online when brought online, instead, it would cycle continuously between the online and offline states.

The problem was due to Oracle Fail Safe not properly noting the role and open mode of the database. Different database queries are utilized for Is Alive processing, depending on the database role (primary or standby) and open mode (mounted or read only). Fail Safe was not always issuing the correct query when polling the standby database, which resulted in unexpected results from the query and thus a forced shutdown of the database.

The Fail Safe Is Alive query code has been corrected to properly note the database role and always use the correct query when doing Is Alive polling.

4.3 Verify Cluster Fails with No Error Message Reported

Executing a `Verify Cluster` would result in the command terminating before completing with no specific error message. For example, the output from the command may look like the following:

```
FS-10660: NODE1 : Gathering cluster information
The clusterwide operation failed !
```

A pop-up box would be created that contained no text; only an "`X`" error image and an "**OK**" button. No errors would be reported in the Windows application event log and Oracle Fail Safe trace logs would show no errors.

This problem was caused by incorrect DCOM security settings; the remote node could not establish a communication link back to the node running the Oracle Fail Safe server and thus could not report any errors to the server and client. Correcting the DCOM Access Permissions using the Microsoft Component Services administrative tool resolved the problem.

To determine if there are problems with DCOM follow the instructions in this Microsoft Knowledge Base article:

`http://support.microsoft.com/kb/892500/en-us`

Oracle Fail Safe has been enhanced to log DCOM errors in the Windows application event log and Oracle Fail Safe trace log.

4.4 Verify Cluster Fails After Installing Oracle Fail Safe Release 3.3.4 and then Reinstalling Release 3.3.3

If Oracle Fail Safe Release 3.3.4 was installed, then deinstalled using the Oracle Universal Installer, and a previous release, such as 3.3.3 was installed, a `Verify Cluster` operation would fail with errors similar to the following:

```
FS-10665: Checking DLLs for resource provider
** WARNING : FS-10669: The  resource provider DLL
D:\ORACLE\OFS333\FS\FSSVR\BIN\ was not found on node NUMBERONE
```

This problem occurred because the deinstallation neglected to remove new registry entries that were introduced in release 3.3.4.

This problem can be resolved by removing the following registry entries from the Windows registry key `\HKEY_CLASSES_ROOT\OracleFailSafe\Resources`:

- `Oracle10gAgent`
- `OracleAS`

The product deinstallation procedure for release 3.4.1 has been corrected and will now properly remove those registry keys entries. Also, the `Verify Cluster` command has been changed to ignore unrecognized resource names in the registry.

4.5 Oracle Fail Safe Installation Corrupts DCOM ACLs in Microsoft Windows Server 2003 R2

If a system had an explicit definition for the DCOM (OLE) DefaultAccessPermission ACL, when the "Oracle Services for MSCS Security Setup" tool (`FsSecurity.exe`) was executed DCOM applications could fail to open windows. The system event log would contain error messages that said, "`Invalid value for registry`".

This problem was due to a new ACL format being introduced in Microsoft Windows Server 2003 R2, which was incompatible with the format being generated by `FsSecurity.exe`. The problem is described in this Microsoft article:

`http://msdn2.microsoft.com/en-us/library/ms693364.aspx`

This problem can be avoided by temporarily removing the DefaultAccessPermission ACL from the windows registry (`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole`), running the MSCS Security Setup tool, and then adding back the DefaultAccessPermission ACL. This operation should only be executed by system administrators that understand the risks of manually editing the Windows registry and know how to backup and recover it.

`FsSecurity.exe` was adding an `ACE` for user `SELF` using the old style access rights but the existing ACL contained an `ACE` that had the new style. In this release, ACLs created by `FsSecurity.exe` will use the new, post Windows Server 2003 SP2 format.

4.6 Cannot Create Sample Database After Upgrading Oracle Database

Creating a standalone database fails with ORA-1219 errors after upgrading to Oracle Database release 10.2.0.2 or higher. Errors similar to the following would be displayed:

```
FS-10356:  Validating the database for service name OFS3
ORA-1219: database not open: queries allowed on fixed tables/views only
FS-10260: The attempt to create standalone sample database OFS3 failed
```

This problem was caused by changes in the Database Configuration Assistant seed database templates introduced within Oracle Database 10g Release 2. The template files that were shipped in prior Oracle Fail Safe kits were not compatible with the new Database Configuration Assistant.

This problem can be worked around by updating the template files in the Oracle Fail Safe template folder. The steps are listed below. This procedure needs to be executed on each node that has Oracle Fail Safe installed.

1. On each node, edit the sample database template file and update the compatible version element. That is, using a text editor, edit the following file:

   OFS_home\fs\fssvr\sample\Oracle_Fail_Safe_Sample_102.dbc

   Search for the line that contains the following string:

   ```
   <initParam name="compatible" value="10.2.0.1.0"/>
   ```

   Change the version number in the string to match the new Oracle RDBMS version.

   For example:

   ```
   <initParam name="compatible" value="10.2.0.3.0"/>
   ```

2. Preserve an old copy of the OFS sample database DFB template by renaming it. That is, rename this file:

   OFS_home\fs\fssvr\sample\Oracle_Fail_Safe_Sample_102.dfb

   to some other name, such as:

   OFS_home\fs\fssvr\sample\Oracle_Fail_Safe_Sample_102.dfb_old

3. Then copy the seed database template provided by the new Oracle RDBMS kit to the OFS sample directory. That is, copy this file:

   ORACLE_HOME\assistants\dbca\templates\Seed_Database.dfb

   to this location and rename it to use the OFS name:

   OFS_home\fs\fssvr\sample\Oracle_Fail_Safe_Sample_102.dfb

After performing the above procedure it should be possible to create a sample database.

In this release of Oracle Fail Safe the sample database creation functionality has been revamped as described in Section 3.2.

4.7 Various Errors When Verifying Standalone Database

When attempting to verify a standalone database Oracle Fail Safe could return various Fail Safe errors, such as: 10916, 10341,10342, 10496, 10491, 10343, 10347, 10999, 10989, 10795, 10890. When examing the Windows application event log the entries would typically mention module `FsDdbsUpi.c`. For example:

The request is aborted due to internal error when calling `OpenOdbsHst()` in module `.\FsDdbsUpi.c`, line 5932.

These errors were more prevalent on 64-bit platforms, but could also occur on 32-bit platforms. There is no workaround for these problems. A number of corrections have been made to the database interface module, `FsDdbsUpi.c`, to prevent these errors from occurring.

4.8 Various Errors When Adding a Resource to a Group

Attempts to add a resource to a group could fail with various errors, often with a Fail Safe 10999 error displayed and "unhandled exception" errors listed in the Windows application event log and the Oracle Fail Safe trace files. For example, the Fail Safe Manager may display a message similar to the following:

```
FS-10427: Creating database instance ORCL for Oracle Net service name ORCL
** ERROR : FS-10999: An internal programming error has occurred
** ERROR : FS-10989: The resource provider Oracle Database raised an unhandled
exception
** ERROR : FS-10778: The Oracle Database resource provider failed to configure the
cluster resource ORCL
** ERROR : FS-10890: Oracle Services for MSCS failed during the add operation
```

These errors were caused by incorrect argument passing and insufficient error handling in the database interface module, `FsDdbsUpi.c`. There is no workaround for these problems. The errors have been corrected in this release.

5 Software Compatibility

This section describes software compatibility for this release of Oracle Fail Safe.

> **Note:** Oracle Fail Safe does not support Automatic Storage Management. Also, Oracle Fail Safe Server and Oracle Fail Safe Manager are not supported on Windows Vista.

5.1 Software Compatibility for Microsoft Windows (32-Bit)

Oracle Services for MSCS must be installed on Microsoft Windows 2000 Advanced Server or Datacenter Server. When that condition is met, then:

- Oracle Fail Safe Manager is compatible with the following operating systems:
  - Microsoft Windows 2000
  - Microsoft Windows XP
  - Microsoft Windows Server 2003
  - Microsoft Windows Server 2003 R2
  - Microsoft Windows Server 2008
- Oracle Fail Safe Server is compatible with the software listed in the following table:

Software	Release or Version
Oracle Database (Standard and Enterprise editions)	Oracle9*i* Release 2 (9.2)
	Oracle Database 10*g* Release 1 (10.1)
	Oracle Database 10*g* Release 2 (10.2)
	Oracle Database 11*g* Release 1 (11.1)
Oracle Intelligent Agent	Release 9.2.0

Software	Release or Version
Oracle Management Agent	Release 10.1.0.2
	Release 10.1.0.3
	Release 10.2
	(A Management Agent release for Microsoft Windows only.)
Oracle Enterprise Manager	Release 9.2.0
	Release 10.1.0
Oracle Application Server	Release 10.1.2

5.2 Software Compatibility for Microsoft Windows x64

The 64-bit release of Oracle Fail Safe is a server-only release. It can be used with the 32-bit version of Oracle Fail Safe Manager release 3.3.1, 3.3.2, 3.3.3, 3.3.4, or 3.4.1. Oracle Fail Safe Manager can be found on the Oracle Fail Safe CD-ROM (32-bit) included with the Oracle Database kit.

- Oracle Fail Safe Manager is compatible with the following operating systems:
  - Microsoft Windows 2000
  - Microsoft Windows XP
  - Microsoft Windows Server 2003
  - Microsoft Windows Server 2003 R2
  - Microsoft Windows Server 2008
- Oracle Fail Safe Server is compatible with the software listed in the following table:

Software	Release or Version
Oracle Database (Standard and Enterprise editions)	Oracle Database 10*g* Release 2 (10.2)
	Oracle Database 11*g* Release 1 (11.1)
Oracle Management Agent	Release 10.1.0.2
	Release 10.1.0.3
	Release 10.2
	(A Management Agent release for Microsoft Windows only.)
Microsoft Cluster Server	Version 5.0 or later
Oracle Fail Safe Manager (32-bit)	Release 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.4.1

6 Hardware Compatibility

Consult your hardware vendor to ensure that the hardware you intend to use with Oracle Fail Safe is certified for use with Microsoft Cluster Server software.

7 Installation and Configuration

This section includes topics about Oracle Fail Safe installations.

For complete installation and deinstallation instructions, see *Oracle Fail Safe Installation Guide*.

7.1 MSCS Cluster Administrator Displays Problems with Fail-Safe Resource Types

Sometimes, after completing an Oracle Fail Safe installation, you see problems with the fail-safe resource types (such as databases) in MSCS Cluster Administrator. MSCS Cluster Administrator denotes the problem by displaying an Oslash symbol (Ø) over the resource type name.

If this occurs, follow these steps:

1. If you forgot to reboot the cluster nodes after installing Oracle Fail Safe, do so now.
2. Make sure that the `PATH` environment variable includes the Oracle Services for MSCS path. (In the Command Prompt window, enter `PATH`.) The Oracle Services for MSCS path (*`ORACLE_HOME`*`\fs\fssvr\bin`) should be included. If it is not included, add it, and then reboot the nodes on which the Oracle Services for MSCS path is missing.
3. Make sure that the Oracle Fail Safe resource DLL, `FsResOdbs.dll`, is installed in *`ORACLE_HOME`*`\fs\fssvr\bin`.

   If the resource DLL is not there, reinstall Oracle Fail Safe.
4. Use Oracle Fail Safe Manager to verify the cluster (on the **Troubleshooting** menu, select **Verify Cluster**), then reboot each cluster node, one at a time. The `Verify Cluster` command automatically verifies registration of Oracle resource DLLs. You may not need to reboot all cluster nodes. After you reboot one node, check MSCS Cluster Administrator to see if the Oslash symbol has been removed from the resource type names. If the Oslash symbol is gone, you do not need to reboot all cluster nodes.

7.2 Using fssvrsec.bat on Windows Server 2008

`fssvrsec.bat` command used to configure Fail Safe service, must be run with full administrative privileges. To run this command with full administrative privileges, you can either start it from the Administrator command prompt or use the Run As Administrator context menu option.

8 Oracle Services for MSCS

This section includes topics about Oracle Services for MSCS.

8.1 DCOM Security Changes on Microsoft Windows 2000

If the list of Access permissions for the default setting of Distributed Component Object Model (DCOM) is empty, the `SYSTEM` and `SELF` accounts have implicit access rights. In Microsoft Windows 2000, if a user or group is added to the list, the implicit rights no longer apply; rights are granted only to explicitly named users or groups. In Microsoft Windows NT, the `SYSTEM` and `SELF` accounts retain their implicit rights.

During the installation of Oracle Services for MSCS, the Oracle Fail Safe user account is added to the default access permissions list. If the access list is not empty, then the `SYSTEM` and `SELF` accounts are automatically added.

After installing Oracle Services for MSCS, if there are problems opening hyperlinks in an HTML file or problems using Microsoft Outlook or Outlook Express, use the `dcomcnfg.exe` tool to add the necessary users to the default list of Access permissions.

See Microsoft Support articles Q274696 and 892500 for more information.

8.2 Oracle Services for MSCS and Microsoft Cluster Server Can Run Under Different Accounts

When your cluster was first configured and Microsoft Cluster Server was first installed, it was installed under a Microsoft Windows user account.

Oracle Services for MSCS runs as a Microsoft Windows service under a domain user account (not the system account) that has Administrator privileges on all cluster nodes. When you install Oracle Services for MSCS, you are instructed to provide a user name and password combination for a user account that has the required privileges. This account does not have to be the same account under which Microsoft Cluster Server was installed.

"Is Alive" polling of Oracle Fail Safe resources is performed by Microsoft Cluster Server, not by Oracle Services for MSCS server. For polling to work properly, the account used for the Microsoft Cluster Server must have the necessary privileges to access the resource being polled.

9 Oracle Database

This section includes information about Oracle databases.

9.1 Errors During Execution of Verify Standalone Database Command

In some cases (perhaps due to another program updating the file), Microsoft Windows may determine that the initialization parameter file for the database is locked by another user and will not allow the file to be temporarily renamed or opened for read/write access. This can cause problems when the `Verify Standalone Database` command is executed and may result in somewhat cryptic error messages being reported. If you encounter error messages that are similar to the following when executing the `Verify Standalone Database` command, check to see if you can temporarily rename the initialization parameter file for the database without getting an operating system error message:

```
FS-10890: Oracle Services for MSCS failed during the Verify Standalone operation
FS-10818: The Oracle Database resource provider failed during preparation for
configuration processing for resource TESTDB1.US.ORACLE.COM
FS-10160: Failed to verify standalone Oracle database TESTDB1.US.ORACLE.COM
FS-10611: Failed to open file d:\oracle\database\initestdb1.ora for read
0xB: An attempt was made to load a program with an incorrect format
```

If another application appears to have control of the file, you can resolve the problem by restarting the cluster node that owns the disk where the file resides (be sure to move any cluster disks that contain database files back to the node that hosts the database after you restart).

9.2 Default Oracle Intelligent Agent Is Stopped and Restarted When the Database Is Shut Down

The default Oracle Intelligent Agent incorrectly discovers fail-safe databases on the node where the default Oracle Intelligent Agent is running, and maintains a connection to the database. (The default Oracle Intelligent Agent listens on the node's host address, and therefore should not discover fail-safe databases because they use a virtual address.) Therefore, when a fail-safe database is taken offline in normal or transactional mode using Oracle Fail Safe Manager, Oracle Fail Safe shuts down the default Oracle Intelligent Agent prior to shutting down the database. Oracle Fail Safe restarts the default Oracle Intelligent Agent after the database shutdown operation is complete.

9.3 Create Sample Database

Oracle Fail Safe includes a `Create Sample Database` command that installs a preconfigured sample database on a cluster disk specified by the user. The sample database has limited functions and is intended only for testing purposes and for use with the online Oracle Fail Safe Tutorial; it should not be used for production. To create a database for production, use Oracle Database Configuration Assistant or create the database manually.

9.4 User Name for Database Must Be `SYS`

If your database does not use operating system authentication, then the database user name must be `SYS` to ensure the success of all Oracle Fail Safe release 3.2.1, 3.3.1, 3.3.2, 3.3.3, and 3.4.1 operations. If operating system authentication is used, then Oracle Fail Safe does not use the `SYS` account.

10 Disk Resources

Oracle Fail Safe allows the use of EMC SRDF/CE disks, formerly known as EMC GeoSpan. However, if you attempt to add a resource to a group and an EMC SRDF/CE disk used by the resource is not already in that group, then Oracle Fail Safe returns the error FS-10203 and rolls back the operation.

If this occurs, add the resource to the group that already contains the EMC SRDF/CE disk that the resource requires.

11 Virtual Addresses

If an MSCS network name contains trailing spaces and you attempt to have Oracle Fail Safe Manager add a virtual address to a group, the operation fails and the following error is returned:

```
NT-5045: The cluster network was not found
```

The workaround to this problem is to rename the network name using MSCS Cluster Administrator to remove the trailing spaces.

12 Oracle Enterprise Manager Integration

This section includes information about integrating Oracle Fail Safe with Oracle Enterprise Manager.

12.1 Partial Support of JobOut Subdirectory

Oracle Intelligent Agent release 8.1.7 deposits its jobs output files into a subdirectory called `JobOut`. For highly available Intelligent Agents, the `JobOut` subdirectory is under the agent's `ConfigPath` directory on the cluster disk. The Intelligent Agent requires the `JobOut` subdirectory to run jobs.

When creating an Oracle Intelligent Agent and adding it to a group, Oracle Fail Safe creates the `JobOut` subdirectory on the cluster disk. However, when verifying a group with a highly available Intelligent Agent in it, Oracle Fail Safe does not verify that the `JobOut` subdirectory exists. In addition, when changing a highly available Intelligent Agent's cluster disk, Oracle Fail Safe does not create a `JobOut` subdirectory on the new disk, nor does it remove the `JobOut` subdirectory from the old disk.

12.2 Oracle Fail Safe Manager Lists Incorrect Oracle Enterprise Manager Agent During Cluster Verification

Oracle Fail Safe Manager lists the 10.2.0.4 Oracle Enterprise Manager Agent incorrectly as 10.1.0.2 Oracle Enterprise Manager Agent during the Verify Cluster process.

12.3 Oracle Enterprise Manager Agent Does Not Start

Oracle Enterprise Manager Management Agent does not start in a secured configuration after being deployed by Oracle Fail Safe through the Add Resource to Group process.

The workaround is to run `emctl secure agent` command manually while the agent is being deployed.

13 Documentation Updated for This Release

See the following documentation, which was updated for this release, which is included in the kit, for additional information:

- *Oracle Fail Safe Concepts and Administration Guide*
- *Oracle Fail Safe Installation Guide*
- *Oracle Fail Safe Error Messages*

Oracle Fail Safe Tutorial, which is included with the kit for this release has not been updated. Specific references to release 3.3.3 in the previous list of documents are also applicable to release 3.4.1 with the exception of references to Oracle HTTP Server. Configuring Oracle HTTP Server for high availability is not supported in this release of Oracle Fail Safe.

The documentation that comes with the kit is provided in HTML and PDF online formats. Viewing the PDF files requires Adobe Acrobat Reader 3.0 or later. You can download the latest version from the Adobe Web site at

`http://www.adobe.com/prodindex/acrobat/readstep.html`

14 Additional Information About Oracle Fail Safe

Refer to the following Web sites for more information about Oracle Fail Safe:

- Oracle Fail Safe on the Oracle Technology Network

http://www.oracle.com/technology/documentation/failsafe.html

Updated software compatibility information, white papers, and so on are posted on the Oracle Technology Network Web site.

- Oracle Enterprise Manager on the Oracle Technology Network

  http://www.oracle.com/technology/documentation/oem.html

- Oracle Support Services

  http://www.oracle.com/support/

  Contact your Oracle support representative for technical assistance and additional information, or visit the Oracle Support Services Web site to find out about other available resources.

15 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, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Oracle Fail Safe Release Notes, Release 3.4.1 for Microsoft Windows
E10719-04