ORACLE APPLICATION SERVER 10*g*

Evaluated Configuration
for Oracle Internet Directory 10*g* (9.0.4)

September 2005

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Evaluated Configuration for Oracle Internet Directory 10*g* (9.0.4)

September 2005

Author: Arfan Latif.

Contributors: Peter Goatly, Shaun Lee, Paula Burgess.

Contents

Contents

jCHAPTER

1 Introduction

The Target of Evaluation (TOE) is Oracle Internet Directory 10*g* (9.0.4.0.0).

The TOE is hosted on the Sun Solaris 8-2/02 operating system platform and uses the Oracle9*i* Release 2 (9.2.0.1.0) Object-Relational Database Management System to hold its directory data.

This *Evaluated Configuration for Oracle Internet Directory 10g (9.0.4)* document explains the manner in which the TOE must be configured along with the host operating system, Oracle9*i* database, and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

The Evaluation Assurance Level for the TOE is EAL4 augmented with ALC_FLR.3. The Security Target used for the evaluation of the TOE is [ST].

1.1 Intended Audience

The intended audience for this document includes evaluators of the TOE, system integrators who will be integrating the TOE into systems, and accreditors of the systems into which the TOE has been integrated.

1.2 Organization

This document is composed of the following chapters:

Chapter 1 contains the introduction to the document;

Chapter 2 describes the physical environment of the TOE and the network services required to support the TOE;

Chapter 3 describes the host operating system, database server, network services, and client application configurations required to support the TOE;

Chapter 4 describes the configuration of the TOE, and all TOE-related network services and applications;

Chapter 5 contains a step by step guide to installation of the TOE in its evaluated configuration;

Annex A lists the software components installed as per Section 5.2; and

Annex B lists the references that are used in this document.

Change bars indicate changes since the previous issue of this document.

1.3 Format

Assertions about the configuration actions that are required to be performed are given identifiers to their left in bold Helvetica font, e.g. **[A-1]**. References to sections of documents listed in Annex B are in the format [*document, section*].

Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configuration requirements use the words “should” in each assertion.

CHAPTER

2 Physical Configuration

The physical and procedural requirements for maintaining the security of the database system underlying the TOE are given in [DBECD, 2]. This chapter describes additional physical and procedural requirements for maintaining the security of the TOE.

2.1 Physical Environmental Assumptions

[DI.A-1] The processing resources of the TOE shall be located within controlled access facilities which will prevent unauthorized physical access to the TOE by unprivileged users. Only authorised administrators for the system hosting the TOE shall have physical access to that system. Such administrators include the Operating System Administrators, Database Administrators and OID Directory Administrators.

[DI.A-2] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorised users.

[DI.A-3] Any on-line and/or off-line storage media on which security relevant data resides shall be located within controlled access facilities which will prevent unauthorised physical access.

2.2 Supporting Procedures

Procedures for the administration of TOE security shall be established based on the contents of this document, the Security Target [ST], any site security policy that may be in force, [DBECD] and [SRN]. In particular, procedures for the TOE shall be established as follows:

- The directory administrator shall instruct users not to disclose their directory passwords to other individuals.
- The directory administrator shall advise users of the restrictions on the passwords they can use as a result of the settings in the directory password policy.
- Directory user passwords generated by the system administrator shall be distributed in a secure manner.

- Procedures and/or mechanisms shall assure that, after system failure or other discontinuity, recovery without a protection (i.e. security) compromise is obtained. Such procedures shall include steps to be taken so that the Oracle9*i* database that the TOE uses to hold its directory data can be protected against data loss. The subject of database backup and recovery is covered in [OBRC].
- The on-line and off-line storage media on which security related data (such as audit trails) is held shall be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related data;
- The media on which directory-related files (including database files, export files, redo log files, control files, trace files, and dump files) have been stored shall be purged prior to being re-used.
- The directory super user is a highly trusted user, who is required by the architecture of the TOE to be able to perform privileged directory adminisration operations such as setting of the audit level and setting access control permissions for users. It is necessary that appropriate personnel and procedural measures (such as procedural two-person control) will be provided to ensure that operations performed under this trusted user account conform to the system security policy.
- For more routine administration tasks it is recommended that alternative, less privileged, directory user accounts are used. These accounts should be configured as members of administrative groups and should be used to perform a set of resticted administrative operations for the directory.
- Administrators, through the use of password policies, shall ensure that password controls for all users (including trusted administrative users) are strong enough to satisfy the TOE's CC Strength of Function rating of SOF-*high.*
- Administrators should be aware of the factors influencing the strength of user passwords when creating or updating password policies. **[DI.POST-4]** ensures that certain limits are set in every password policy. However, suitable use of the other available password controls normally strengthens the TOE's overall password mechanism strength.
  For example, setting `pwdMaxAge` (Password Expiry Time) in conjunction with `pwdExpireWarning` (Password Expiration Warning) will limit the opportunity of an attacker to guess a particular password. In addition, using `pwdInHistory` (Number of Password History) will ensure passwords held in the history store cannot be re-used, again limiting the opportunity for a particular password to be guessed. To prevent the same password being supplied again at the end of a password lifetime period, administrators should set `orclpwdToggle` (Old Password Can Be New Password) to 0.
  Note that Password policies are described in [OIDAG, 15]. The password policy attributes are defined in [OIDAG, Appendix B: Password Policy Schema Elements].

CHAPTER

3 Host Configuration

This chapter describes the configuration requirements for the systems which unlerly the TOE.

[DBECD, 3] describes the configuration requirements for the Solaris server platforms and the network services. [DBECD, 3] also covers requirements for client platforms that are to be used in the same secure network as the Oracle9*i* database, and covers the use of operating system facilities to protect the database.

[DBECD, 4] covers the configuration requirements for the Oracle9*i* database that the TOE uses to hold its directory data.

3.1 Further Database Configuration Requirement

The following requirement replaces **[DB.IA-18]** in [DBECD, 4] when configuring the database underlying the TOE.

[DB.IA-18x] After creating and setting up a database, the default profile must be changed to ProfileB, which is described in Annex A of [DBECD]. Database administrators must also employ this change to all new profiles created, to ensure that all users (including administrative users) are subject to strong password controls at all times. The guidance in [DBECD, 2.2] should be followed when modifying or creating profiles.

This Page Intentionally Blank

CHAPTER

4 TOE Configuration

The TOE consists of software only. The TOE contains no hardware or firmware components and there are no hardware or firmware dependencies which affect the evaluation.

This chapter describes how the TOE must be configured in its evaluated configuration.

4.1 Pre-Installation Requirements

The actions **[DI.PRE-1]** to **[DI.PRE-5]** listed in this section are required before the installation of the TOE can be carried out as described in chapter 5.

[DI.PRE-1] In order that the Oracle Application Server 10*g* (9.0.4) installation process can install the TOE successfully, the following lines must be present in the file `/etc/system`:

```
set semsys:seminfo_semmni=100
set semsys:seminfo_semmns=256
set semsys:seminfo_semmsl=256
set shmsys:shminfo_shmmax=4294967295
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=10
```

[DI.PRE-2] A Unix group, which will be used by the Oracle software owner and database administrators, must be created before installing the TOE. Any legal name can be used for this group, but the convention is to use “dba”. The dba group can be created via the admintool GUI or with the Unix command:

```
groupadd -g 300 dba
```

[DI.PRE-3] A Unix group, which will be used by the Oracle software owner, must be created before installing the TOE. Any legal name can be used for this group, but the convention is to use “oinstall”. The oinstall group can be created via the admintool GUI or with the Unix command:

```
groupadd -g 301 oinstall
```

[DI.PRE-4] A Unix user that will be the Oracle software owner must be created before installing the TOE. The standard name used is “oracle”. When creating the user a primary and a secondary group are required. The primary group should be oinstall and the secondary group should be dba. The oracle user can be created via the admintool GUI or with the Unix command:

```
useradd -c “Oracle Software Owner” -d /home/oracle
-g oinstall -G dba -m -u 300 -s /bin/ksh oracle passwd or-
acle
```

[DI.PRE-5] The directory `/var/opt/oracle` must be created, with the oracle user as owner. After the installation this directory will contain some text files that briefly describe the Oracle software installations.

The following Unix commands can be used to establish this directory:

```
mkdir /var/opt/oracle
chown oracle:oinstall /var/opt/oracle
chmod 755 /var/opt/oracle
```

4.2 Post-Installation Requirements

[DI.POST-1] The directory administrator must establish Access Control settings for the directory so that anonymous users can only access material which the administrator deems to be “public information” (for example names of administrators and their contact telephone numbers).

The amount of information returned during a null subtree and null base search should be as restrictive as possible whilst still allowing operation.

[DI.POST-2] The directory administrator must establish Access Control settings for the directory so that the guest user and the proxy user can only access data that anonymous users can access. The guest and proxy users are set up with the same privileges as anonymous users during the default installation of the TOE.

[DI.POST-3] The directory administrator must set passwords of at least 8 characters in length for the guest user and the proxy user. These passwords are only to be revealed to administrators. [OIDAG, 5: Managing Super Users, Guest Users and Proxy Users] describes how to set these passwords.

[DI.POST-4] The directory administrator must set a password policy which is enabled and has attributes as follows:

- `pwdMinLength` set to 6 (the minimum number of characters that may be used in a password);
- `orclpwdAlphaNumeric` set to 0 (the minimum number of numeric characters in the password);
- `pwdLockout` set to 1 (a value of 1 indicates account lockout is in force);
- `pwdMaxFailure` set to 10 (the number of consecutive failed password checks after which the user is locked out if `pwdLockout` has been set to 1); and
- `pwdLockoutDuration` set to 900 (the number of seconds for which the user is locked out when the number of consecutive failed password checks has reached `pwdMaxFailure` and `pwdLockout` has been set to 1).

[OIDAG, 15: Managing Password Policies] describes how to set password policies. The password policy attributes are defined in [OIDAG, Appendix B: Password Policy Schema Elements]. Password policies are enabled by setting the value of the attribute `orclpwdpolicyenable` to 1.

[DI.POST-5] The directory administrator must ensure that Access Control settings for the super user password attribute of the DSE entry (`orclsupassword`) do not allow users other than the super user to read the value of this attribute.

To do this the directory administrator must edit the default ACP to deny users access to the `orclsupassword` attribute. Using Oracle Directory Manager this can be done by navigating to the Access Control Management Panel, navigating to `Default ACP`, then creating a new ACI for attribute `orclsupassword` for which all users are denied the read, compare, search and modify capabilities.

For example:

access to attr=(orclSuPassword) by dn="cn=orcladmin"(Read, Write, Search, Compare) by * none

[DI.POST-6] The directory administrator shall ensure that the audit level is set to cover auditing of at least super user logins and user logins. The administrator should normally use an audit level that includes all security events (which is represented by a value of 16383). The directory administrator shall perform regular checks of the directory audit trail, looking for evidence of attacks against the TOE's security policy. The administrator shall ensure that the audit trail is kept to a reasonable size by archiving audit material when necessary and by purging the audit trail using `bulkdelete`.
The administrator should note that, if the directory audit trail is not regularly purged, it can cause the database to fill up. Once this has happened no actions will be audited as there will be no space in the database to store audit records. At this point, the database administrator must make space available for the database and the directory administrator must archive audit material if necessary and then purge the directory audit trail using `bulkdelete`, as described in [OIDAG, 4].

Here is a example of using the Bulkdelete command to delete the auditlog:-

Bulkdelete.sh -connect oid -base "cn=auditlog" -size 100 -w password

To ensure that the bulk command tools work correctly the path must be set correctly in the *.profile* file.

DTSOURCEPROFILE=TRUE
ORACLE_SID=oid
ORACLE_HOME=/export/home/oracle/OraHome1
PATH=$ORACLE_HOME/bin:$PATH
export PATH
export ORACLE_SID
export ORACLE_HOME

If the above paths are not set correctly then the bulk tools will not run.

The database administrator can tell whether the database is getting full by examining the DBA_FREE_SPACE data dictionary view.

[OIDAG, 10: Setting the Audit Level] describes how to set the audit level.

[DI.POST-7] The super user for the directory has the privileges necessary to perform all actions on the directory. The initial password for the super user is set by the Application Server

installation process to be the same as the password for the ias_admin user for the Oracle Application Server instance. This password is supplied by the installer during the installation. The super user password should be changed after the installation process because the ias_admin password is the password for many of the Application Server tools, and hence is known by a range of Application Server administrators.
Because of the power of the super user, the directory administrator must set a password with at least 8 characters for it.

[OIDAG, 5: Managing Super Users, Guest Users and Proxy Users] describes how to set the super user password.

[DI.POST-8] The ODS schema is the database schema which holds all of the directory data. The password for the ODS database user is set by the Application Server installation process to be the same as the password for the ias_admin user for the Oracle Application Server instance. This password is supplied during the installation. The ODS database user password should be changed after the installation process because the ias_admin password is the password for many of the Application Server tools, and hence is known by a range of Application Server administrators.

[OIDAG, Appendix A: OID Database Password Utility (`oidpasswd`) Syntax] describes how to change the ODS password.

[DI.POST-9] The directory administrator should provide the directory server's port number to people intending to send LDAP messages to the TOE. Following installation of the TOE, the port configuration details are stored in the file `ORACLE_HOME/install/portlist.ini`. This file defines the port number that is configured to run the Oracle Internet Directory Server in non-SSL mode.

[DI.POST-10] The administrators for the system hosting the TOE shall ensure that operating system accounts and database accounts on that system are only provided for administrators.

[DI.POST-11] The `orclCryptoScheme` attribute in the DSE, which is given an initial value during the installation process, must never be set as No Encryption.

[DI.POST-12] If the administrator finds that the super user account has become locked, he or she must attempt to find the cause of the lockout before unlocking the account, and must take action to prevent re-occurrence, if possible. The administrator should also take such action if a normal user repeatedly asks the administrator to unlock their user account.

The oidpasswd utility in $ORACLE_HOME/bin may be used to unlock the super user account. For example:

oidpasswd [connect=<OID schema database connect string>] unlock_su_acct=true

When prompted, the ODS password to authenticate to the database must be provided.

[DI.POST-13] The administrator for Oracle9*i* database that the TOE uses to hold its directory data can use the statement:

```
AUDIT SESSION
BY ods;
```

to monitor all of the TOE's database sessions.

[DI.POST-14] Section 2.2 states that users shall be instructed not to disclose their directory passwords to other individuals. This instruction must include the requirement that users must not change the Access Control settings for the `userpassword` attribute of their user entry to allow other non-administrative users to read the value of this at-

tribute.

[DI.POST-15] [OIDAG, 6: Guidelines for Deleting Object Classes] states that object classes cannot be deleted from the base schema, but that Oracle Internet Directory does not enforce this rule. Administrators shall therefore not delete such object classes. If items from the base schema get deleted, administrators shall employ database restore procedures to recover such items (see section 2.2 which requires that steps be taken so that the Oracle9*i* database that the TOE uses to hold its directory data can be protected against data loss).

[DI.POST-16] Password policies are described in [OIDAG, 15]. Changes to a password policy entry only take effect after the directory server instance has next been re-started. Administrators shall therefore ensure that the directory server instance is re-started when it is necessary for an updated password policy entry to take effect.

[OIDAG, Appendix A: Starting, Stopping, Restarting and Monitoring Oracle Directory Servers] describes how to re-start a directory server instance.

[DI.POST-17] The directory administrator must ensure that Access Control settings for the audit log allow only administrative users to access its records.

[DI.POST-18] When a user entry is deleted from a directory, references to this user from Access Control Information and group entries are not automatically removed. The directory administrator must ensure that no new user entry is created with the same DN as the deleted entry to avoid the new user gaining privileges that the deleted user had without being authorised to receive these privileges.
It is recommended that this is achieved by the use of an administration log maintained manually by the directory administrators (perhaps in a file on the server). This log would allow an administrator to record the details of any new user entry they had created. Such details must include the DN of the new directory user. They could also include a record of the justification for the user to be given access to the directory and of the justification when the user is to be given group memberships. This log would have the benefit of communicating information on each directory administrator's actions to the other directory administrators.
As an alternative to deleting the user entry when a user's access to the directory is to be terminated, administrators may choose to disable the user account by setting the attribute `orclisenabled` to `DISABLED`.

[DI.POST-19] The directory administrator must ensure that Access Control settings for the password policy entry allow only administrative users to modify it. Thus all users will be able to access the password policy, but attempts to make modifications will give rise to an error message stating Insuficient Access Rights. All attempts at changing the password policy are auditable.

[DI.POST-20] There may be interactions if an administrator is using a TOE directory administration tool described in [OIDAG, 4: Using Command-Line Tools] to access data which is simultaneously being accessed by a directory server instance executing an LDAP request. Guidance on action to be taken to avoid any such undesirable interactions is given in the documentation for each TOE directory administration tool in [OIDAG, Appendix A]. If administrators are in doubt about possible interactions, they must ensure that the directory server is not running when they use a TOE directory administration tool.

This Page Intentionally Blank

CHAPTER

5 Step by Step Guide

This chapter contains a step by step guide to installing the TOE in its evaluated configuration. It can be read in conjunction with [QUICK, 2], which provides background information on the pre-installation requirements.

5.1 Operating System Installation / Configuration

Ensure that the intended physical environment is in accordance with the assumptions **[A-1]** to **[A-6]** listed in [DBECD, 2.1].

5.1.1 Installation of Sun Solaris 8-2/02

Install Sun Solaris 8-2/02 in accordance with [DBECD, 3] and [SRN].

5.2 Oracle Application Server 10*g* (9.0.4) Configuration

5.2.1 Step by Step Installation of Oracle Internet Directory 10*g* (9.0.4)

This section outlines steps needed to set up the TOE's evaluated configuration on Sun Solaris 8-2/02, including the installation of the Oracle9*i* Database. Those steps which are essential towards achieving the TOE's Evaluated Configuration are highlighted in **bold**.

The information to be supplied by the administrator for each step is indicated on the Universal Installer screen. The items in quotes below are examples of what was supplied for a particular installation of the TOE.

This section should be used in conjunction with the relevant installation manuals and assumes any prior installations of Oracle Application Server have been removed before the new installation starts.

Step No.	Action	Result
1	Insert Oracle Application Server CD-ROM 1. Follow the instructions given in [QUICK, 2.11] to start Oracle Universal Installer.	Oracle Universal Installer: Welcome window appears.
2	Click Next.	
3	Ensure the Inventory path is suitable for the installation. example: "`export/home/oracle/oraInventory`" Click Next.	File Locations page opens. This is the default path supplied on screen.
4	Unix Group Name: example: "`oinstall`"	Enter operating system group name.
5	Execute oraInstRoot.sh script as **root user** from the following directory: `export/home/oracle/oraInventory` The command to run theoraInstRoot.sh script is: **`sh oraInstRoot.sh`**	This script is run only if this is the first installation on this computer.
6	Ensure the Oracle Home and full path are suitable for the installation. example: "`export/home/oracle/OraHome1`" Click Next.	This is the default option provided by the Universal Installer.
7	Select Product to Install: **Oracle Infrastructure 10*g*** Click Next	
8	Installation Type: **Identity Management and OracleAS Metadata Repository.** Click Next.	
9	Infrastructure Installation Screen. Click Next	
10	Confirm Pre-Installation Requirements. Click on the **Root Privileges box**. Click Next.	This is required so that some of the installation scripts can be run as the root user.

Step No.	Action	Result
11	Configurable Options **Click on Oracle Internet Directory and deselect everything else.** Click Next	
12	Namespace in Oracle Internet Directory: example: "`dc = reliant, dc = com`" Note: reliant is the name of the host in this example. Click Next	
13	**Privileged Operating System Groups** Database Administrator (OSDBA) Group: example: "`oinstall`" Database Operator (OSOPER) Group: example: "`oinstall`" Click Next	
14	Database Identification: **Global Database Name**: example: "**`OID.CLEF`**" **SID**: example: "**`OID`**"	
15	**DBA Passwords:** **Sys Password:** example: "`oracle`" **System Password**: example: "`oracle`" Click Next	These will be the database administrator passwords for the Sys and System user.
16	Database File Location example: "`export/home/oracle/OraHome1/oradata`" Click Next	This is the default option provided by the Universal Installer.
17	Database Character Set Click on the Default option Click Next	

Step No.	Action	Result
18	Specify Instance Name and ias_admin password: **Instance Name**: example: "`OID`" i**as_admin password**: example: "`oracle10g`" **Confirm Password**: example: "`oracle10g`" **Click Next**	The ias_admin password stated here will be the default password for the Super User and the ODS user.
19	There should be a list of products which are selected to be installed. These are listed in Annex A.1. **Click Install**	This will run the installation process. Inserts CD's 2 and 3 when asked on screen.
20	During the installation process the user will be asked to run the **root.sh** script. Oracle Universal Installer will display a screen prompting the administrator to run **root.sh**. In a different window login as the root user and run the **root.sh** script.	This script will create all the Oracle Internet Directory file permissions.

5.2.2 Exclusions

Section A.1 lists the software components that are installed on the server by the Oracle Universal Installer during the installation of Oracle Internet Directory 10*g* (9.0.4) as per section 5.2.1. Because this is an Application Server installation process, many of these components are not part of the TOE. Section A.2 lists the components that actually constitute the TOE. The other components are not for use with the TOE in its evaluated configuration.

5.3 Client Installation

The TOE scope does not include any Oracle Application Server client software. During the evaluation of the TOE, client software can be used to send LDAP messages to the TOE in order to test its security features.

[DI.CA-1] No applications, other than those which communicate with the TOE by sending LDAP messages, shall be permitted to run on any client or server host machines which access the network, unless they have been shown not to compromise the TOE's security objectives as stated in [ST] (the equivalent restriction for the database underlying the TOE is **[OS.CA-1]** in [DBECD]).

ANNEX

A TOE Components

A.1 Server components

The following is a summary of all the components that are installed on the server by the Oracle Universal Installer during the installation of Oracle Internet Directory 10*g* (9.0.4) as per section 5.2.1:

- Advanced Queueing (AQ) API 9.0.1.5.0
- Advanced Replication 9.0.1.5.0
- Agent Required Support Files 9.0.4.0.0
- Apache Configuration for EJB 9.0.1.0.1
- Apache Configuration for Oracle Java Server Pages 9.0.4.0.0
- Apache Configuration for Oracle XML Developers Kit 9.0.4.0.0
- Apache Jserv 1.1.2.0.2a
- Apache Module for Oracle Distributed Authoring and versioning 9.0.4.0.0
- Assistant Common Files 9.0.4.0.0
- Authentication and Encryption 9.0.1.5.0
- Bali Share 1.1.18.0.0
- BC4J Config Assistant 9.0.4 1304.0
- BC4J Config Assistant for Agent 9.0.4 1304.0
- BC4J Runtime Library 9.0.4 1304.0
- Character Set Migration Utility 9.0.1.5.0
- Configure ldap.ora Config file 9.0.4.0.0
- Database Management Services Common Files 9.0.4.0.0
- Database Configuration Assistant 9.2.0.1.0

- Database SQL Scripts 9.0.1.5.0
- Database Verify Utility 9.0.1.5.0
- Database Workspace Manager 9.0.1.0.0
- Documentation Required Support Files 9.2.0.1.0
- Enterprise Edition Options 9.0.1.5.0
- Enterprise Manager Agent 4.0.1.0.0
- Enterprise Manager Base Classes 9.0.2.0.0
- Enterprise Manager Common Files 4.0.1.0.0
- Enterprise Manager Minimal Support Files 9.2.0.0.0
- Enterprise Manager Process Utility 9.0.4.0.0
- Enterprise Manager Translated Files 9.2.0.1.0
- Export/Import 9.0.1.5.0
- Extending Windowing Toolkit 3.3.18.0.0a
- Generic Connectivity Common Files 9.0.1.5.0
- Generic Connectivity Using ODBC 9.0.1.5.0
- HTTP Server Files 1.3.28.0.0
- Infrastructure Schema and Instance Configuration Assistants 9.0.4.0.0
- Installation Common Files 9.0.4.0.0
- Installer SDK Component 2.3.0.10.0
- JDBC Common Files 9.0.1.5.0
- JDBC/OCI Common Files 9.0.1.5.0
- JSDK 2.0.0.0d
- Java Naming and Directory Interface Libraries 1.2.1.0.0
- Java Runtime Environment 1.1.8.16.0c
- Java Runtime Environment 1.4.1.3.0
- Java Security Configuration Assistant 9.0.4.0.0
- LDAP Required Support Files 9.0.4.0.0
- Migration Utility 9.0.1.5.0
- OC4J for Oracle Enterprise Manager 9.0.4.0.0
- Object Type Translator 9.0.1.5.0
- Oracle Advanced Security 9.0.1.5.0
- Oracle Application Server Instance 9.0.4.0.0
- Oracle Application Server Management and Integration 9.0.4.0.0
- Oracle Application Server UIX Configuration
- Oracle Application Server Mod osso registration 9.0.4.0.0

- Oracle Call Interface (OCI) 9.0.1.5.0
- Oracle Client Required Support Files 9.0.1.5.0
- Oracle Data Migration Assistant 9.0.4.0.0
- Oracle Database Configuration Assistant 9.0.4.0.0
- Oracle Database User Interface 2.2.13.0.0
- Oracle Database Utilities 9.0.1.5.0
- Oracle Delegated Administration Service 9.0.4.0.0
- Oracle Display Fonts 9.0.2.0.0
- Oracle Distributed Configuration Management 9.0.4.0.0
- Oracle Dynamic Motoring Service 9.0.4.0.0
- Oracle Dynamic Services Core 9.0.4.0.0
- Oracle Dynamic Services Midtier 9.0.4.0.0
- Oracle Dynamic Services Server 9.0.4.0.0
- Oracle EM Agent 9.0.4.0.99
- Oracle Enterprise Java Beans and Cobra Tools 9.0.1.1.1
- Oracle Enterprise Manager Common Files 9.0.2.0.0
- Oracle Enterprise Manager Database Applications 9.0.2.0.0
- Oracle Extended Windowing Toolkit 3.4.28.0.0
- Oracle HTTP Server 9.0.4.0.0
- Oracle Help for Java 4.2.5.0.00
- Oracle Help for the Web 1.1.7.0.oa
- Oracle Ice Browser 5.2.3.3.0
- Oracle Internet Directory 9.0.4.0.0
- Oracle Internet Directory Client 9.0.4.0.0
- Oracle Internet Directory Client Common Files 9.0.4.0.0
- Oracle Internet Directory Client Configuration Assistant 9.0.4.0.0
- Oracle Internet Directory Server 9.0.4.0.0
- Oracle Internet Directory Tools 9.0.4.0.0
- Oracle JDBC Thin Driver for JDK 1.1.9.0.1.5.0
- Oracle JDBC Thin Driver for JDK 1.2.9.0.1.5.0
- Oracle JDBC/OCI Driver for JDK 1.1.9.0.1.5.0
- Oracle JDBC/OCI Driver for JDK 1.2.9.0.1.5.0
- Oracle JFC Extended Windowing Toolkit 4.1.11.0.0
- Oracle JFC Extended Windowing Toolkit 4.2.18.0.0
- Oracle JVM 9.0.1.5.0

- Oracle Java Layout E ngine 2.0.2.0.0f
- Oracle Java Object Cache 9.0.4.0.0
- Oracle Java Tools 9.0.1.5.0
- Oracle Java Tools Common Files 9.0.1.5.0
- Oracle Log Loader 9.0.4.0.0
- Oracle Mod PL/SQL Gateway 9.0.4.0.0
- Oracle NET 9.0.4.0.0
- Oracle Net Configuration Assistant 9.0.4.0.0
- Oracle Net Listener 9.0.4.0.0
- Oracle Net Manager 9.0.4.0.0
- Oracle Net Protocol Support 9.0.4.0.0
- Oracle Net Required Support Files 9.0.1.5.0
- Oracle Net Services 9.0.4.0.0
- Oracle Notification Service 9.0.4.0.0
- Oracle OC4J Module 9.0.4.0.0
- Oracle One-Off Patch Installer 2.3.0.10.0
- Oracle Partitioning 9.0.1.5.0
- Oracle Portal CAT 9.0.4.0.99
- Oracle Portal Common Services 9.0.4.0.99
- Oracle Portal Configuration Assistant 9.0.4.0.99
- Oracle Portal Documentation 9.0.4.0.99
- Oracle Portal Images 9.0.4.0.99
- Oracle Portal Monitoring 9.0.4.0.99
- Oracle Portal PLSQL Toolkit 9.0.4.0.99
- Oracle Portal SSO 9.0.4.0.99
- Oracle Portal Utilities 9.0.4.0.99
- Oracle Portal VPD Policy 9.0.4.0.99
- Oracle Process Management Notification 9.0.4.0.0
- Oracle Property Inspector 4.1.15.0.0
- Oracle SMIME 9.0.4.0.0
- Oracle SOAP Client Files 2.2.0.0.2a
- Oracle SOAP Server 2.2.0.0.2a
- Oracle Spatial 9.0.1.5.0
- Oracle Starter Database 9.0.1.0.0
- Oracle Syndication Service 9.0.4.0.0

- Oracle Syndication Services 9.0.4.0.0
- Oracle Syndication Services Midtier 9.0.4.0.0
- Oracle Text 9.0.1.5.0
- Oracle Trace 9.01.0.0
- Oracle Trace Required Support Files 9.0.1.0.1
- Oracle UIX 2.1.21.0.0a
- Oracle Ultra Search Common Files 9.0.4.0.0
- Oracle Ultra Search Extention for EM Agent 9.0.4.0.0
- Oracle Ultra Search Extention for EMD 9.0.4.0.0
- Oracle Ultra Search Server 9.0.4.0.0
- Oracle Universal Installer 2.3.0.10.0
- Oracle Wallet Manager 9.0.1.5.0
- Oracle XML SQL Utility 9.01.5.0
- Oracle Intermedia 9.0.4.0.0
- Oracle Intermedia Annotator 9.0.4.0.0
- Oracle Intermedia Audio 9.0.4.0.0
- Oracle Intermedia Client Compatability Files 9.0.4.0.0
- Oracle Intermedia Client Option 9.0.4.0.0
- Oracle Intermedia Common Files 9.0.4.0.0
- Oracle Intermedia Image 9.0.4.0.0
- Oracle Intermedia Java Advanced Imaging 9.0.4.0.0
- Oracle Intermedia Java Client 9.0.4.0.0
- Oracle Intermedia Java Media Framework Client 9.0.4.0.0
- Oracle Intermedia Locator 9.0.1.5.0
- Oracle Intermedia Video 9.0.4.0.0
- Oracle Intermedia Web Client 9.0.4.0.0
- Oracle 9*i* 9.0.1.5.0
- Oracle 9*i* Globalization Support 9.0.1.5.0
- Oracle 9*i* Real Application Clusters Common Files 9.0.1.5.0
- OracleAS Certificate Authority 9.0.4.0.0
- OracleAS Chart Builder 9.0.4.0.0
- OracleAS Configuration for OC4J 9.0.4.0.0
- OracleAS Containers for J2EE 9.0.4.0.0
- OracleAS Containers for J2EE Common Files 9.0.4.0.0
- Oracle Infrastructure Devkit dialogs 9.0.4.0.0

- Oracle Infrastructure 10g 9.0.4.0.0
- Oracle Infrastructure Database 9.0.4.0.0
- Oracle Instance Dialog 9.0.4.0.0
- Oracle JAAS Support 9.0.4.0.0
- Oracle JAAS Support Common Files 9.0.4.0.0
- Oracle Repository API 9.0.4.0.0
- OracleAS Single Sign On 9.0.4.0.0
- OracleAS Single Sign On Registration 9.0.4.0.0
- OracleAS Single Sign On Server 9.0.4.0.0
- OracleAS Web Services 9.0.4.0.0
- OracleAS Web Services Common Files 9.0.4.0.0
- OracleAS Wireless SSO Pages 9.0.4.0.0
- PL/SQL 9.01.5.0
- PL/SQL Embedded Gateway 9.0.1.5.0
- PL/SQL Required Support Files 9.0.1.0.1
- Parser Generator Required Support Files 9.0.1.0.1
- Perl Interpreter 5.6..1.0.2c
- Platform Required Support Files 9.0.1.5.0
- PreCompiler Common Files 9.0.1.5.0
- PreCompiler Required Support Files 9.0.1.5.0
- RDBMS Required Support Files 9.0.1.5.0
- Recovery Manager 9.0.1.5.0
- Replication API 9.0.1.5.0
- Repository Config Assistant 9.0.4.0.0
- Required Support Files 9.0.1.5.0
- SQL* Loader 9.0.1.5.0
- SQL* Plus 9.0.1.5.0
- SQLJ Runtime 9.0.4.0.0
- SSL Required Support Files 9.0.1.5.0
- Secure Socket Layer 9.0.1.5.0
- Secure Socket Layer Files 9.0.1.5.0
- SUN JDK 1.4.1.0.3
- SUN JDK extensions 9.0.4.0.0
- Ultra Search Configuration Assistant for OID 9.0.4.0.0
- Utilities Common Files 9.0.1.5.0

- Visigenics ORB 3.4.0.0.0
- XDK Required Support Files 9.0.4.0.0
- XML 9.0.4.0.0
- XML Class Generator for C++ 9.0.4.0.0
- XML Class Generator for Java 9.0.4.0.0
- XML Parser for C 9.0.4.0.0
- XML Parser for C++ 9.0.4.0.0
- XML Parser for Java 9.0.4.0.0
- XML Parser for Oracle JVM 9.0.4.0.0
- XML Parser for PL/SQL 9.0.4.0.0
- XML Transviewer Beans 9.0.4.0.0
- XSQL Servlet 9.0.4.0.0
- regexp 2.1.9.0.0

A.2 Evaluated Configuration Boundaries

The evaluated configuration of the TOE shall comprise exactly the following software components:

- Oracle Internet Directory 9.0.4.0.0
- Oracle Internet Directory Server 9.0.4.0.0
- Oracle Internet Directory Tools 9.0.4.0.0

A.3 Client components

There are no client components in the TOE.

The following is a list of all the components that were installed on the client by the Oracle Universal Installer during the installation of client software for use in testing the TOE in its evaluated configuration.

- Oracle Internet Directory Client 9.0.4.0.0
- Oracle Internet Directory Client Common Files 9.0.4.0.0
- Oracle Internet Directory Client Configuration Assistant 9.0.4.0.0
- ldap.ora Config file.

This Page Intentionally Blank

ANNEX

B References

[CC] *Common Criteria for Information Technology Security Evaluation,* Version 2.2, ISO/IEC 15408, CCIMB-2004-01, 001, January 2004.

[DBECD] *Evaluated Configuration for Oracle9i, Release 2 (9.2.0),* Oracle Corporation.

[LDAP3] *Lightweight Directory Access Protocol (v3),* Request For Comments (RFC) 2251 of the Internet Engineering Task Force, December 1997, available on the World Wide Web at http://www.ietf.org/rfc.htm

[OIDAG] *Oracle Internet Directory Administrator's Guide 10g (9.0.4),* Oracle Corporation.

[OBRC] *Oracle9i Backup and Recovery Concepts, Release 2 (9.2),* Oracle Corporation.

[QUICK] *Oracle Application Server10g: Quick Installation and Upgrade Guide 10g (9.0.4) for Solaris Operating System(SPARC),* Oracle Corporation.

[RFC2252] *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions,* Request For Comments (RFC) 2252 of the Internet Engineering Task Force, December 1997, available on the World Wide Web at http://www.ietf.org/rfc.htm

[RFC3377] *Lightweight Directory Access Protocol (v3): Technical Specification,* Request For Comments (RFC) 3377 of the Internet Engineering Task Force, September 2002, available on the World Wide Web at http://www.ietf.org/rfc.html

[SRN] *Solaris 8-2/02 Security Testing - Installation Procedure,* Version 0.1, November 5, 2002, Sun Microsystems.

[ST] *Security Target for Oracle Internet Directory 10g (9.0.4)*, Oracle Corporation**.**