OLS Evaluated Configuration for Oracle9*i* Release 2 (9.2.0)

March 2003

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

OLS Evaluated Configuration for Oracle9*i*
Release 2 (9.2.0)

March 2003

Author: Saad Syed

Contributors: Duncan Harris, Peter Goatly, Daniel Elliott

This document is based on the equivalent document for Oracle8i for OLS Release 8.1.7.3.0. The contributions of the many authors of the precursors to this document are acknowledged.

Contents

Contents

CHAPTER

1 Introduction

The Target of Evaluation (TOE) is the Oracle9*i* Release 2 (9.2.0.1.0) Object-Relational Database Management System (O-RDBMS) with Oracle Label Security.

The TOE is hosted on two operating system platforms:

- Sun Solaris 8;
- Microsoft Windows NT Version 4.0 with Service Pack 6a, configured to C2 specification.

This *OLS Evaluated Configuration for Oracle9i* document explains the manner in which the TOE must be configured along with the host operating system 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. The Protection Profile used for the evaluation of the TOE is the Database Management System Protection Profile [DBPP]. 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 sections:

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, 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	details the password management controls that must be implemented in all user profiles;
Annex B	lists the software components installed as per Section 5.2 and
Annex C	lists the references that are used in this document.

1.3 Format

Assertions for the physical, host, and Oracle configurations are given identifiers to the left of each evaluation configuration requirement in bold Helvetica font, e.g. **[A-1]**. References to sections of documents listed in Annex C 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

This chapter describes the physical and procedural requirements for maintaining the security of the TOE.

2.1 Physical Environmental Assumptions

[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 DBA or operator users (i.e. users who are allowed corresponding SYSDBA or SYSOPER access rights within the database) shall have physical access to the server machines.

[A-2] The processing resources of the underlying operating system required to support the TOE shall be located within controlled access facilities which will prevent unauthorised physical access.

[A-3] The processing resources of the network services required to support the TOE shall be located within controlled access facilities which will prevent unauthorised physical access.

[A-4] The media on which authentication data for the underlying operating system data resides shall not be physically removable from the underlying operating system by unauthorised users.

[A-5] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorised users.

[A-6] 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, and [NTC2] and [SRN]. In particular procedures shall be established such

that:

- users must not disclose their operating system passwords to other individuals;
- operating system or database 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;
- the on-line and off-line storage media on which security related data (such as operating system backups, database backups and transaction logs, and audit trails) are 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 database-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 for any non-database purpose;
- the predefined normal users SYS, SYSTEM, LBACSYS and users who connect as SYSDBA or SYSOPER are highly trusted users, who are required by the architecture of the TOE to be able to perform privileged database operations for which the TOE records only limited information. It is assumed that appropriate personnel and procedural measures (such as procedural two-person control) will be provided to ensure that operations performed under these trusted user accounts conform to the system security policy. (Note that the TOE records accounting information for operations performed by SYS, DBA and OPER to the OS audit trail, but only if the `audit_sys_operations` initialization parameter is set to TRUE).

  For more routine administration tasks it is recommended that alternative, less privileged, database user accounts are configured and used to perform a more restricted set of privileged database operations.
- a user who grants the REFERENCES privilege on one or more columns of a table shall understand the possible interactions between database referential integrity controls and access controls. Specifically, a referential constraint has the following implications:
  - if the referential constraint specifies DELETE RESTRICT then a user will not be able to delete referenced parent rows even though the user has DELETE access on the parent table;
  - if the referential constraint specifies SET TO NULL or SET TO DEFAULT then when a parent row is deleted from the parent table the corresponding child row(s) will be updated regardless of whether the deleting user has UPDATE access on that child table.
  - if the referential constraint specifies DELETE CASCADE then when a parent row is deleted from the parent table the corresponding child row(s) will be deleted from the child table regardless of whether the deleting user has DELETE access on that child table.
- Administrators shall understand the limitations of resource limits. The TOE can control certain resources such as user sessions and connect time directly, but 'system' resources such as CPU time and logical reads can only be controlled in relation to statements that the database has to process (i.e. SQL and PL/SQL statements). For example, the O-RDBMS can run Java code internally, but as this is a separate server mechanism the program code itself is not subject to resource

limits. However any database calls (SQL) made from the Java code are sent from the Java Engine to the database SQL engine, then processed in the normal way and are subject to all applicable resource limits.

- Administrators, through the use of password limits in profiles, 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, when creating new profiles or when changing the default profile, of the factors influencing the strength of user passwords. **[DB.IA-18]** ensures that certain limits are set in every profile (although it does offer a choice to administrators), however the other password controls available can both strengthen and weaken the TOE's overall password mechanism strength. In general, any further elaboration of the complexity check function (beyond that suggested in this document) will **weaken** the strength of passwords since it would narrow the choice available. The other controls are however generally strengthening measures. A password_lock_time in conjunction with failed_login_attempts will delay any password-guessing attacks (although a lockout time of at least 1 minute, and a failed logins count of <10 is recommended). Setting a password_life_time (in conjunction with password_grace_time) will limit the opportunity of an attacker to guess a particular password. Also, using the password_reuse_time limit will enforce the use of different passwords, again limiting the opportunity for a particular password to be guessed. To prevent the same password being supplied at the end of a password life-time period, administrators should set password_reuse_time greater than password_life_time.
  Note that "password_reuse_time" should be interpreted as the time between the last successful user password change to a given value and the next attempt to change the user's password to that same value.
- Administrators shall not open databases in read-only mode. The read-only database open feature provides the ability for users to query an open database without the potential for on-line data contents modification. This mode of operation deactivates some security features including password changing, account lockout, and database auditing.

This Page Intentionally Blank

CHAPTER

3 Host Configuration

This chapter describes the configuration requirements for the Windows NT and Solaris server platforms, the network services, and the client platforms. It also covers the use of operating system facilities to protect the TOE.

3.1 Windows NT Operating System

The TOE was evaluated and tested on two Compaq Deskpro EN Pentium 3 machines, one used as server and one used as client. These machines were connected by a Local Area Network (LAN).

The TOE was evaluated and tested on Microsoft Windows NT 4.0 Server (build 1381 with Service Pack 6a) operating system running on the server machine, and on Microsoft Windows NT 4.0 Workstation (build 1381 with Service Pack 6a) operating system running on the client machine. Both Server and Workstation were configured in accordance to the requirements of the TCSEC C2 specification [NTC2].

[NT-1] The underlying operating system shall be the Microsoft Windows NT Version 4.0 Server operating system, build 1381, with Service Pack 6a.

[NT-3] The underlying operating system identified in **[NT-1]** should be installed and operated in accordance with [NTC2].

[NT-5] The operating system administrator shall ensure that only users in the `ADMINISTRATORS` and/or `DOMAIN ADMINS` groups are able to perform administrative tasks in the operating system.

This should be achieved by editing the System Policy Editor of Windows NT to reflect the privileges for administrative and normal operating system users.

3.1.1 Identification and Authentication

[NT.IA-5] The operating system shall only allow the `ADMINISTRATOR` group to access the operating system registry. This should be accomplished by ensuring that only the operating system administrator belongs to the `ADMINISTRATORS` operating system group. The operating system administrator may also belong to the `DOMAIN ADMINS` group to create and administer user accounts on other machines within a domain.

[NT.IA-6] No other users (existing or newly created) shall belong to either the ADMINISTRATORS or DOMAIN ADMINS groups on either the host machine on which the TOE is installed, or on their local (client) machines from which they will connect to the TOE.

[NT.IA-8] All normal operating system users shall belong to either the USERS or other (non-administrator) domain level operating system group such as DOMAIN USERS.

[NT.IA-9] The administrator shall only configure a single domain of identification for all normal users of the TOE.

[NT.IA-11] The operating system administrator shall delete the DBA_AUTHORIZATION parameter (if present) from the NT registry.

[NT.IA-13] Command shell and other logical access (either locally or remotely) to machines hosting the database server shall be restricted to users holding SYSDBA or SYSOPER level access to the database. Unless otherwise required by this document no user level network shares are to be established to the server machines.

3.1.2 Protection of Resources

[NT.PR-1] The administrator shall ensure that all of the installed TOE-related files and directories are protected by means of the operating system's Discretionary Access Control mechanisms to ensure that they are accessible to authorised users only.

Oracle Universal Installer, Database Configuration Assistant and Database Upgrade Assistant set file permissions for TOE-related files when Oracle software is installed, so no further action is required.

[INST_NT_9*i*, 6-2: About NTFS File System and Windows Registry Permissions] describes the permissions automatically set by the Oracle Universal Installer, the Database Configuration Assistant and the Database Upgrade Assistant and the steps to set these permissions manually.

There are no mandatory requirements for specific access permissions to be set on the client machine as this is not part of the TOE.

[NT.PR-4] To maintain the integrity of the audit timestamp, only operating system administrators shall have access to the operating system clock configuration. Access permissions for all other users should be set to NO ACCESS for the operating system clock.

3.1.3 Accounting and Auditing

[NT.AA-1] The administrator shall protect operating system audit trails or any other audit trails used by the O-RDBMS against unauthorized modification and deletion by means of operating system Discretionary Access Control mechanisms.

[NT.AA-2] The directory containing operating system audit trail files shall be set to FULL CONTROL permissions for users in the local TOE administrator operating group, and NO ACCESS for all other users.

[NT.AA-3] The operating system administrator shall implement procedures that support the archiving of operating system audit trails prior to audit trail exhaustion.

3.2 Sun Solaris Operating System

The TOE was evaluated and tested on two Sun Ultra 60 server machines, one was used as a server and one as a client. These machines were connected by a Local Area Network (LAN).

The TOE was evaluated and tested on Sun Solaris 8 operating system, which has met Common Criteria security requirements for assurance level EAL4.

[SS-3] Solaris 8 shall be installed and operated in a manner as described in [SRN].

[SS-4] The UNIX filesystem (ufs) shall be used on all host machines supporting the TOE.

[SS-5] The operating system administrator shall ensure that only designated users are able to perform administrative tasks in the operating system.

This should be achieved using AdminSuite (or directly editing the /etc/group file) to ensure that normal users are not given membership of the *oinstall* group, or any OS group used to give administrative rights e.g. *root*, *bin*, *sys*, *adm*, *sysadmin*. Also, the *root* and *oracle* user accounts should be available only to administrators.

In addition the only local operating system user accounts on the server shall be those for the DBA administrators and OS administrators.

3.2.1 Identification and Authentication

[SS.IA-6] No non-administrative users (existing or newly created) shall belong to the administrative groups on either the host machine on which the TOE is installed, or on their local (client) machines from which they will connect to the TOE.

See **[SS-5]** for guidance about such administrative groups.

[SS.IA-8] All normal operating system users shall have a non-administrative primary group set, such as `USERS` or `ORA_USERS`.

3.2.2 Protection of Resources

[SS.PR-1] The operating system shall protect all of the installed TOE-related files and directories by means of its Discretionary Access Control mechanisms to ensure that they are accessible to authorised users only.

Oracle Universal Installer, Database Configuration Assistant and Database Upgrade Assistant set file permissions when Oracle software is installed, so no further action is required.

[INST_SS_9*i*, 4-2: Verifying Database File Security] describes the permissions automatically set by the Oracle Universal Installer, the Database Configuration Assistant and the Database Upgrade Assistant and the steps to set these permissions manually.

[SS.PR-4] To maintain the integrity of the audit timestamp, only operating system administrators shall have access to the operating system clock configuration. All other users shall have no access permissions for the operating system clock configuration.

3.2.3 Accounting and Auditing

[SS.AA-1] The operating system shall protect operating system audit trails or any other audit trails (e.g. audit log files) used by the O-RDBMS against unauthorized modification and deletion by means of its Discretionary Access Control mechanisms.

[SS.AA-2] The directory containing the TOE-generated audit log files shall have permissions set for only the local TOE administrator operating group, and no access for all other users. Note: this is located by default in the *$ORACLE_HOME/rdbms/audit* directory.

[SS.AA-3] The operating system administrator shall include procedures that support the archiving of operating system audit trails and audit log files prior to audit trail or disk space

exhaustion.

3.3 Network Services

[OS.NS-3] In a distributed environment, the underlying network services shall be based on the available secure communication protocols which ensure the authenticity of the operating system users.

[OS.NS-4] Only administrative users shall be able to modify the network services configuration parameters.

3.4 Client Applications

[OS.CA-1] No applications shall be permitted to run on any client or server machines which access the network, unless they have been shown not to compromise the TOE's security objectives stated in the [DBPP] and the [ST].

CHAPTER

4 Oracle 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.

The TOE shall be installed, configured, and maintained in accordance with this document and with the instructions provided in [INST_SS_9*i*] and [INST_NT_9*i*].

4.1 O-RDBMS Server

4.1.1 Identification and Authentication

In the evaluated configuration for the Windows NT platform, the TOE supports two different modes of Identification and Authentication - OS mode and O-RDBMS mode. These two modes can operate concurrently for any database instance, and individual database users can be configured to have either OS I&A (identified externally), or O-RDBMS I&A (database password).

In the evaluated configuration for the Sun Solaris platform, only the O-RDBMS mode of Identification and Authentication is supported. OS Authentication should not be enabled on the Solaris platform as this operating system does not have the concept of domain controllers (as Windows NT) to verify usernames against. On Solaris it would be possible to create spoof OS users on individual machines which could bypass this method of authentication.

[DB.IA-1] For the Windows NT platform, the TOE shall be configured to use either OS I&A or O-RDBMS I&A for all users connecting to the TOE, i.e. all database users must either be *identified externally*, or have a *database password*. For the Sun Solaris platform, the TOE shall be configured to use O-RDBMS I&A for all users connecting to the TOE, i.e. all database users must have a *database password*

[DB.IA-2] Administrators that create normal users within the O-RDBMS shall create appropriately privileged accounts for those users in the operating system as well. See **[NT.IA-5]**, **[NT.IA-8]** and **[SS.IA-8]** for details.

[DB.IA-3] Database administrators shall set the initialization parameter as follows:

```
o7_dictionary_accessibility = FALSE
```

This ensures that if you need to access objects in the SYS schema, explicit object privilege must be granted to you. System privileges that allow access to objects in "any schema" do not allow access to objects in SYS schema.

[DB.IA-4] After creating and setting up a database, all database user accounts must be configured as per **[DB.IA-1]**. All pre-defined accounts (such as SYS, MDSYS, SYSTEM etc.) and any demonstration accounts (such as SCOTT) created during installation should have their passwords changed, or (on Windows NT only) be altered to use OS I&A.

[DB.IA-7] Database administrators shall set the initialization parameter as follows

```
sql92_security = TRUE
```

This ensures that the user must have `SELECT` privilege on a table when executing an `UPDATE` or `DELETE` statement that references table column values in a `WHERE` or `SET` clause.

[DB.IA-8] (Windows NT platform only). To additionally permit operating system authentication of users in each of the O-RDBMS instances, the following initialization configuration parameters shall be set:

```
remote_os_authent = TRUE
os_authent_prefix = " "
```

[DB.IA-11] Normal database users may belong to one or more of the following operating system local groups.

```
ora_user
ora_<sid>_user
```

This step is discretionary, it may help distinguish database users from other users, however it is not necessary for users to belong to this user group in order to connect to the database.

[DB.IA-14] To connect to the O-RDBMS as a privileged database user such as a database administrator, the following parameter shall be set in the appropriate initialization file:

```
remote_login_passwordfile = EXCLUSIVE
```

This allows two types of privileged connection. Privileged connections (i.e. AS SYSDBA, AS SYSOPER) are permitted either by having an entry in the password file (having been granted the appropriate permissions in the database), or by membership of an OS group (having been granted membership by an OS administrator). See **[DB.NS-6]** for an additional parameter required to be initialized to permit such connections.

[DB.IA-15] Database administrators who are required to use the `CONNECT / AS SYSOPER` syntax to connect to an O-RDBMS shall belong to one or more of the following operating system local groups:

Windows NT platform

```
ora_oper
ora_<sid>_oper
```

Sun Solaris platform

```
dba
```

Note that on Solaris the *dba* group gives both sysdba and sysoper privileges.

[DB.IA-16] Database administrators who are required to use the `CONNECT / AS SYSDBA` syntax to connect to an O-RDBMS shall belong to one or more of the following operating system local groups:

Windows NT platform

```
ora_dba
ora_<sid>_dba
```

Note that an O-RDBMS privileged user who belongs to an operating system local group (on the host machine itself) having a particular O-RDBMS <SID> as defined above, can connect as a privileged user only to that database. When the <SID> is not specified for a particular operating system local group, then a user belonging to such a local group can connect as a privileged user to all instances of the O-RDBMS.

Sun Solaris platform

```
dba
```

Note that on Solaris the *dba* group gives both sysdba and sysoper privileges.

[DB.IA-18] After creating and setting up a database, the default profile must be changed as described in Annex A of this document. Annex A provides a choice of two profiles, which implement password limits that enable the TOE to satisfy its CC Strength of Function claim. 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 section 2.2 should be followed when modifying or creating profiles.

[DB.IA-19] Administrators wishing to limit password reuse (for example to prevent the same password being supplied at the end of a password life-time period), should use the profile setting password_reuse_time, perhaps in conjunction with password_life_time and password_grace_time (with password_reuse_time being set greater than password_life_time). The profile setting password_reuse_max should not be used.

[DB.IA-20] In the evaluated configuration, roles shall not be protected by an associated password.

4.1.2 Accounting and Auditing

[DB.AA-2] In the evaluated configuration for a specific O-RDBMS, the `audit_trail` parameter in the appropriate initialization parameter file for that O-RDBMS shall be assigned in one of the following two ways:

```
audit_trail = OS
```

```
audit_trail = DB
```

[DB.AA-3] When OLS has been installed, the database audit trail is a SYSTEM-owned table, SYSTEM.AUD$. Only users connected as AS SYSDBA or SYSTEM can directly read and write all rows in SYSTEM.AUD$ (provided that **[DB.AC-10]** has been complied with).

[DB.AA-5] Database administrators shall create database audit trail views for all other appropriately privileged O-RDBMS users to be able to read and analyse database audit trail data.

Pre-defined database audit trail views are automatically created during the installation and creation of the database.

Only highly trusted users shall have the privilege which allows them to:

- set or alter the audit trail configuration for the database;
- alter or delete any audit record in the database audit trail.

[DB.AA-6] Database administrators shall perform regular archiving of database and operating system audit trails before audit trail exhaustion to ensure sufficient free space for continued auditing operations. See Section 3.1.3 or 3.2.3 for details.

[DB.AA-7] Database administrators shall ensure that session auditing is enabled at all times by issuing the statement

```
audit session;
```

By enabling session auditing at all times, all user sessions are recorded with their sessionid and method of authentication. This information can then be used to identify whether actions in a particular session were undertaken by a proxy user.

[DB.AA-9] Database administrators shall ensure that changes to the database audit trail are audited, by issuing the statement

```
audit insert, update, delete
on system.aud$
by access;
```

[DB.AA-10] Since fine-grained auditing is supported only with cost-based optimization, database administrators shall ensure that the cost-based optimization mode is used when using fine-grained auditing. This can be achieved by setting the `optimization_mode` parameter in the appropriate initialization parameter file in one of the following ways:

`optimizer_mode = first_rows_n` (where n = 1,10,100 or 1000), or
`optimizer_mode = all_rows`

4.1.3 Availability and Reliability

[DB.AR-1] Only privileged O-RDBMS users such as database administrators shall be permitted to perform privileged O-RDBMS operations such as backup and recovery, and enforce tablespace quotas and resource profiles.

[DB.AR-2] **[DB.AR-1]** should be accomplished by ensuring that only privileged O-RDBMS users have the necessary administrative system privileges to perform these types of operations.

[DB.AR-3] Administrative system privileges shall not be granted to normal O-RDBMS users directly or through the use of database roles. See Section 4.1.5 for details.

For example, a normal O-RDBMS user must not be granted the `ALTER PROFILE` system privilege either directly or through a database role.

[DB.AR-4] Each user of the TOE must be configured with appropriate tablespace quotas that are

- sufficiently permissive to allow the user to perform the operations for which the user has access rights;

- sufficiently restrictive that the user cannot abuse the access rights and thereby waste or monopolise resources.

4.1.4 DAC Access Controls

[DB.AC-5] If the UTL_FILE PL/SQL package is used to provide database access to host OS files the configuration parameter `UTL_FILE_DIR` must not be set to "*", but to explicit values so as to protect against overriding the operating system DAC mechanisms.

[DB.AC-6] Each database link must be defined such that users who refer to the link are connected to an identically named normal user account in the secondary or remote database, that is the database link must be defined without reference to a single normal user account to which all users referencing the link would otherwise be connected.

[DB.AC-7] The EXECUTE privilege on the DBMS_JOB, UTL_SMTP, UTL_TCP, UTL_HTTP, UTL_FILE, DBMS_RANDOM PL/SQL packages is granted to PUBLIC by default. This should be revoked by executing the following SQL statements from an administrative connection to the database:

```
revoke execute on <package_name> from public;
```

[DB.AC-8] The EXECUTE privilege on the SA_COMPONENTS, SA_USER_ADMIN, SA_LABEL_ADMIN, SA_POLICY_ADMIN and SA_AUDIT_ADMIN OLS packages shall only be granted to OLS policy administrators.

[DB.AC-9] The EXECUTE privilege on the SA_SYSDBA OLS package shall only be granted to database administrators.

[DB.AC-10] Normal users shall not be granted access to objects in the SYSTEM or LBACSYS schemas.

4.1.5 Security Administration and Management

In the evaluated configuration, the TOE supports and implements Security Administration and Management by the use of over ninety distinct and separately managed object and system privileges. When OLS is installed, OLS policy privileges are also available.

System privileges which are administrative in nature such as those which allow database-wide object, role, user, privilege, and profile manipulation shall not be granted to normal O-RDBMS users either directly or through database roles.

[DB.SAM-1] Only highly trusted O-RDBMS users and database administrators should be allowed to posses system privileges which are administrative in nature.

Examples of such privileges are the `ALTER PROFILE` and `ALTER USER` system privileges which can be used to alter any user profile, or any user in the O-RDBMS. The latter gives full access to other users' accounts, either through altering their passwords or through the ability to proxy as them.

[DB.SAM-2] Object privileges and other system privileges (which are non-administrative in nature) are required by normal O-RDBMS users to perform their tasks under the *Principle of Least Privilege.*

The privileges described above should be grouped together into database roles and granted to normal O-RDBMS users.

An example of these types of privileges is the `CREATE TABLE` privilege which by default allows O-RDBMS users to create and modify tables within their own schema, but

not in any other user schema.

[DB.SAM-3] The system privileges of SYSDBA and SYSOPER shall not be granted to any normal O-RDBMS user, including the user SYSTEM.

Database administrators are authenticated as described by DB.IA-14 above. Only database administrators should be granted these system privileges, or given membership of the OS groups described in DB.IA-15 and DB.IA-16.

[DB.SAM-5] The CREATE LIBRARY and CREATE ANY LIBRARY system privileges shall not be granted to any user of the TOE.

This restriction is imposed so as to prevent the use of libraries which would enable callouts to external C programs which could be misused against the TOE's security features.

[DB.SAM-6] The CREATE SNAPSHOT, CREATE MATERIALIZED VIEW, CREATE ANY SNAPSHOT, CREATE ANY MATERIALIZED VIEW, ALTER ANY SNAPSHOT or ALTER ANY MATERIALIZED VIEW privileges shall only be assigned to trusted (e.g. DBA) users.

[DB.SAM-7] In the evaluated configuration the use of Java packages is not supported. Database Administrators shall make regular checks to ensure that users do not use Java packages.

[DB.SAM-8] LBAC user authorisations and OLS policy privileges are required by normal O-RDBMS users to perform their tasks under the *Principle of Least Privilege.*

[DB.SAM-9] The OLS FULL policy privilege shall not be granted to normal users of the TOE.

[DB.SAM-10] The OLS PROFILE_ACCESS policy privilege shall not be granted to normal users of the TOE. This is a very powerful privilege, since the user can potentially become a user with FULL privileges.

[DB.SAM-11] When OLS has been installed, the CREATE TRIGGER system privilege shall not be granted to any normal user of the TOE. This is because CREATE TRIGGER allows a user to set a trigger on one of his tables which can potentially run with FULL privileges if another user accesses that table.

[DB.SAM-12] The roles CONNECT and RESOURCE shall not be granted to normal users of the TOE. These roles are only provided to maintain compatibility with previous versions of Oracle and may not be provided in future versions of Oracle. Instead, the privileges which make up these roles should individually be granted to users or to a role as needed by the user. See [DAG, 25: User Roles (Table 25-1)].

[DB.SAM-13] The EXEMPT ACCESS POLICY system privilege shall only be given to users who have legitimate reasons for by-passing fine-grained security enforcement of VPD or OLS policies.

[DB.SAM-14] Because system privileges are so powerful, administrators must take great care when granting ANY system privileges to non-DBA users (such as UPDATE ANY TABLE). Such privileges shall only be given to users who have legitimate reasons for their use.

In particular, CREATE ANY TRIGGER shall not be granted to non-DBA users. This is because it allows a user to create a trigger on any database table and hence to capture data from any transaction performed on that table.

[DB.SAM-15] [ADG, 7: Setting Up the Database for Flashback Query] describes how DBAs should set up a database for flashback queries. DBAs should only grant the FLASHBACK ANY TABLE privilege or EXECUTE on the DBMS_FLASHBACK package to trusted users who

have legitimate reasons for their use, because this allows such users to access data that existed in the past in tables that they can currently access. This would be a problem if the owner of a table had deleted rows that held sensitive information before granting other users privileges to access the table.

For the same reason, DBAs should refuse requests from normal users to be granted the `FLASHBACK` privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the `FLASHBACK` privilege.

[DB.SAM-16] As described in **[DB.SAM-15]**, DBAs should refuse requests from normal users to be granted the `FLASHBACK` privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the `FLASHBACK` privilege. The owner of a table which is protected by VPD policies should refuse requests from normal users to be granted the `FLASHBACK` privilege on the table unless the administrators for these VPD policies have given their approval. The reason for this is that otherwise there would be a problem if a row in a table protected by a VPD policy has had data in a column updated to make access to the row via the policy more restricted, because a flashback query could allow a user access to the row when the VPD policy should not permit it.

[DB.SAM-17] As described in **[DB.SAM-15]**, DBAs should refuse requests from normal users to be granted the `FLASHBACK` privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the `FLASHBACK` privilege. The owner of a table which is protected by OLS policies should refuse requests from normal users to be granted the `FLASHBACK` privilege on the table unless the administrators for these OLS policies have given their approval. The reason for this is that otherwise there would be a problem if a row in a table protected by an OLS policy has had its label updated to be more restrictive, because a flashback query could allow a user access to the row when his label authorisations should not permit it.

4.1.6 Secure Data Exchange

[DB.SDE-1] Database administrators shall ensure that any system privilege (directly or through the use of roles) required to implement database import and export be only granted to O-RDBMS users who are trusted to perform these operations, and who normally do not have the appropriate privileges for read and write access to such data.

4.1.7 Secure Distributed Processing and Databases

The TOE can be operated in standalone, client/server and server/server configurations. Database links may be used to connect between different O-RDBMS servers over a network. The TOE provides site autonomy which implies that each server participating in a distributed environment is administered independently from other servers in the distributed system.

[DB.SDD-1] Database administrators should implement a site-specific security policy according to their security requirements.

When distributed databases are employed, OLS Policy administrators should use the same label tags for each database. If this is not possible then users should ensure that they convert labels to character strings upon retrieval (using LABEL_TO_CHAR) and use CHAR_TO_LABEL when storing labels. This ensures that labels are consistent even if the corresponding label tags are different on the remote database.

In a distributed environment, the OLS policy administrator should ensure the same relative ranking of the numeric form of the level component, in order to ensure proper dominance of the labels.

[DB.SDD-2] In the evaluated configuration for a specific O-RDBMS, the `dblink_encrypt_login` parameter, in the appropriate initialization parameter file for that O-RDBMS, shall be assigned in the following way:

```
dblink_encrypt_login = TRUE
```

4.1.8 Multi-tier environments

[DB.MT-1] To ensure accountability in multi-tier environments, any middle-tier(s) must pass the original client ID through to the TOE.

4.2 Oracle Network Services

[DB.NS-3] Only operating system or database administrators shall be able to modify the installed network services configuration parameters.

[DB.NS-4] No other user should be permitted to modify any network services configuration parameter in the O-RDBMS network configuration files such as `TNSNAMES.ORA`, `LISTENER.ORA` and `SQLNET.ORA`.

[DB.NS-5] The network services configuration files specified in DB.NS-4 are located in *$ORACLE_HOME*`\NETWORK\ADMIN`. Permissions on this directory should be restricted so that administrative users have full access, but all other operating system users have read-only access.

[DB.NS-6] The *$ORACLE_HOME*`\NETWORK\ADMIN\SQLNET.ORA` parameter required to support operating system authentication of privileged database users shall be set as follows:

```
sqlnet.authentication_services = (NTS)
```

[DB.NS-7] The parameters in the network configuration files specified in DB.NS-4 shall use a consistent O-RDBMS naming convention, this helps ensure database uniqueness throughout the domain.

CHAPTER

5 Step by Step Guide

This chapter contains a step by step guide to installing the TOE in its evaluated configuration.

Readers unfamiliar with Oracle products should read this section in conjunction with [STARTED]. Note that in some cases changes are not effective until the database is restarted or, for membership of an OS user group, until the user has logged out and logged in again.

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 section 2.1 of this document.

Installation instructions for the two platforms, Windows NT and Sun Solaris, are given separately below.

5.1.1 Installation of Windows NT 4.0

Install Microsoft Windows NT 4.0 Server and Service Pack 6a in accordance with [NTC2] and Chapter 3 of this document.

5.1.2 Installation of Sun Solaris 8

Install Sun Solaris 8 in accordance with [SRN], and Chapter 3 of this document.

5.2 Oracle9*i* Server Installation / Configuration

5.2.1 Step by Step Installation of Oracle 9*i* Release 2 (9.2.0)

This section outlines the steps needed to duplicate the Evaluated configuration on Windows NT 4.0 and Sun Solaris 8 for the Oracle9*i* Database. Those steps which are essential towards achieving the Evaluated configuration are highlighted in **bold**.

This section should be used in conjunction with the relevant installation manuals.

Step No.	Action	Result
1	Insert Oracle9*i* Database CD-ROM. Follow the instructions given in [STARTED] to start Oracle Universal Installer.	Oracle Universal Installer: Welcome window appears.
2	Click Next.	File Locations page opens.
3	Ensure the Oracle Home and full path are suitable for the installation. Click Next.	Available Products page opens.
4	**Select Oracle9*i* Database 9.2.0.1.0 and click Next.**	Installation Types page opens.
5	**Select Custom and click Next.**	Available Product Components page opens.
6	**Deselect all components except the following:** **Oracle9*i* Database 9.2.0.1.0** **Oracle9*i* 9.2.0.1.0** **Enterprise Edition Options 9.2.0.1.0** **Oracle Label Security 9.2.0.1.0** **Oracle Net Services 9.2.0.1.0** **Oracle Net Listener 9.2.0.1.0** **Oracle Intelligent Agent 9.2.0.1.0** **Oracle Call Interface 9.2.0.1.0** **Oracle9*i* Windows Documentation 9.2.0.1.0** **Click Next.**	Component Locations page opens.
7	Click Next.	Oracle Universal Installer: Create Database window opens.
8	Select Yes and click Next.	Summary window opens.

Step No.	Action	Result
9	**Ensure Summary list of installation components is identical with the Server components listed in Appendix B of this document.**	Lists are indentical.
10	Click Install	Install page opens and installation begins.
11	Insert CD-ROMs 2 and 3 as required by Oracle Universal Installer.	Oracle Net Configuration Assistant opens.
12	Click Next.	Directory Usage Configuration page opens.
13	Select No, I want to complete the configuration at another time and click Next.	Listener Configuration, Listener Name page opens.
14	Select a Listener name and click Next.	Listener Configuration, Select Protocols page opens.
15	Select TCP only and click Next.	Listener Configuration, TCP/IP protocols page opens.
16	Select Use the standard port number of 1521 and click Next.	Listener Configuration, More Listeners? page opens.
17	Select No and click Next.	Listener Configuration Done page opens.
18	Click Next.	Naming Methods Configuration page opens.
19	Select No, I do not want to change the naming methods configured.	Oracle Net Configuration Assistant: Done page opens. Oracle Net Configuration ends.
20	Click Finish.	Database Configuration Assistant: Welcome window opens.
21	Click Next.	Step 1 of 8 : Operations page opens.
22	Select Create a database then click Next.	Step 2 of 8 : Database Templates page opens.
23	Select New Database and click Next.	Step 3 of 8 : Database Identification page opens.

Step No.	Action	Result
24	Choose a Global Database Name e.g. ols1.test and click Next.	Step 4 of 8 : Database Features page opens.
25	**De-select all features and select Oracle Label Security. Click on Standard Database Features and deselect all. Click OK then Click Next.**	Step 5 of 8 : Database Connection Options page opens.
26	**Select Dedicated Server Mode and click Next.**	Step 6 of 8 : Initialization Parameters page opens.
27	Select appropriate data storage options. Click Next.	Step 7 of 8 : Database Storage page opens.
28	Click Next.	Step 8 of 8 : Creation Options page opens
29	Select Create Database and click Finish.	Summary window opens.
30	Click OK.	Database Configuration Assistant creates database.
31	Choose new passwords for SYS and SYSTEM. Click Exit.	Configuration Tools page opens.
32	Click Next.	End of Installation page opens to confirm Oracle9i Database installation was successful.
33	Click Exit.	Oracle Universal Installer closes.

5.2.2 Exclusions

This document implicitly excludes certain components by specifying the installation options that comprise the TOE boundary. Additionally, the guidance and configuration steps contained in this document prohibit the use of certain other facilities.

Administrators should also be aware of facilities that should not be used during development of database applications in the evaluated configuration. These are the iFS (internet File System), the OCI internet cache, the KG platform (which implements PL/SQL metadata sharing in applications), the Thin JBDC driver (which provides java applets with a non-OCI interface to the database), the Oracle Intelligent Agent and the new Java RepAPI protocol for snapshots (which is similar to the thin Java client inter-

face).

5.3 Configuration of Oracle9*i* RDBMS

5.3.1 Protection of database files

Protect the database files from unauthorised access as per **[SS.PR-1]** and **[NT.PR-1]** of section 3.2.2. Network files shall be protected as per **[DB.NS-3]** to **[DB.NS-5]** of section 4.2.

5.3.2 Setting up the Evaluated Configuration

The following steps must be completed to comply with the Evaluated Configuration.

5.3.2.1 As required for **[DB.IA-3]**, database administrators shall set the following initialization parameter:

```
o7_dictionary_accessibility = FALSE
```

5.3.2.2 As required for **[DB.IA-7]**, database administrators shall set the following initialization parameter:

```
sql92_security = TRUE
```

5.3.2.3 As required for **[DB.IA-14]**, database administrators shall set the following initialization parameter:

```
remote_login_passwordfile = 'EXCLUSIVE'
```

5.3.2.4 As required for **[DB.AA-2]**, the `audit_trail` parameter in the appropriate initialization parameter file for that O-RDBMS shall be assigned in one of the following two ways:

```
audit_trail = OS
audit_trail = DB
```

5.3.2.5 As required for **[DB.AA-10]**, if fine-grained auditing is in use then database administrators shall set the `optimizer_mode` initialization parameter in set in one of the following ways:

```
optimizer_mode = first_rows_n (where n =
1,10,100,1000), or
optimizer_mode = all_rows
```

5.3.2.6 As required for **[DB.AA-7],** database administrators shall ensure that session auditing is enabled at all times, by issuing the following statement from an administrative connection to the database:

```
audit session;
```

5.3.2.7 As required for **[DB.AC-7]**, the following SQL statements shall be executed from an administrative connection to the database:

```
revoke execute on dbms_job from public;

revoke execute on utl_smtp from public;

revoke execute on utl_tcp from public;

revoke execute on utl_http from public;

revoke execute on utl_file from public;
```

```
revoke execute on dbms_random from public;
```

5.3.2.8 As required for **[DB.IA-1]**, on Solaris systems, the administrator shall ensure OS authentication is not configured for any user connecting to the TOE, i.e. all database users must be configured to have a *database password.* This can be checked at any time by executing:

```
select username from dba_users where password='EXTERNAL';
```

If no records are selected, then all users are authenticating via a database password.

5.3.2.9 As required for **[DB.IA-4]**, all pre-defined accounts (such as SYS, MDSYS, LBACSYS, SYSTEM etc.) and any demonstration accounts (such as SCOTT) created during installation shall have their passwords changed.

If the account is not to be used, then it shall be locked and expired. To prevent inappropriate access to the data dictionary tables or other tampering with the database, the passwords set for SYS, LBACSYS and SYSTEM shall be divulged only to the group of administrators who are intended to use them.

5.3.2.10 As required for **[DB.IA-4]**, the following SQL statements shall be executed from an administrative connection to the database:

```
alter user dbsnmp account lock password expire;
```

5.3.2.11 As required for **[DB.IA-18]**, after creating and setting up a database, the default profile must be changed as described in Annex A.

5.3.2.12 As required for **[DB.SDD-2]**, the `dblink_encrypt_login` initialization parameter should be set as follows:

```
dblink_encrypt_login = TRUE
```

5.3.3 Enabling OS Authentication (Windows NT only)

If OS authentication is to be used, then it shall be enabled in accordance with [NT_START] and in addition the following parameters shall be set as described below.

As required for **[DB.IA-8],**. database administrators shall set the following initialization parameters.

```
remote_os_authent = TRUE
```

```
os_authent_prefix = " "
```

As required for **[DB.NS-6],**.the operating system administrator shall set the *$ORACLE_HOME*`\NETWORK\ADMIN\SQLNET.ORA` parameter required to support operating system authentication of privileged database users as follows:

```
sqlnet.authentication_services = (NTS)
```

In order to make privileged connections to the database, users may belong to the OS user groups described in assertions **[DB.IA-15]** and **[DB.IA-16]**.

Note: OS Authentication should not be enabled on the Solaris platform, see 4.1.1.

5.3.4 Maintaining the Evaluated Configuration

The above steps are necessary for achieving an initial evaluated configuration. The remaining configuration requirements in this document (Sections 4.1.2, 4.1.3, 4.1.4,

4.1.5, 4.1.6, 4.1.7, 4.1.8, **[DB.NS-7]** and **[NT.IA-13]**) cover the general administration of the TOE in order that the evaluated configuration is maintained.

5.4 Configuration of Oracle Label Security

No further configuration of Oracle Label Security is required upon installation.

5.5 Client Installation

Client installation is completed as follows:

- Install the host operating system as described in and section 5.1.2 above;
- Install the client Oracle software as described in section 5.6 above;
- Configure Oracle Net authentication as laid out in **[DB.NS-6]**;
- Configure the network services configuration parameters as described in **[DB.NS-2]** to **[DB.NS-4]**;
- Protect the client applications from unauthorised use by setting the access control permissions as described in **[SS.PR-2]**.

Note that untrusted users of the TOE are not expected to be administrators of their local machines.

5.6 Oracle Client Applications

[DB.CA-1] The client applications shall be installed using the Oracle Universal Installer 2.2.0.12.0. The following software components shall be installed using the Custom Installation option:

- Oracle9*i* client 9.2.0.1.0

  - Oracle Network Utilities
    Oracle Database Utilities
    SQL*Plus 9.2.0.1.0
    Oracle Call Interfaces 9.2.0.1.0
    Oracle9*i* Windows Documentation 9.2.0.1.0
    Oracle Universal Installer 2.2.0.12.0

Annex B contains a complete list of all the software components that are then installed by the Oracle Installer.

[DB.CA-2] No database applications except those based on OCI (e.g. SQL*Plus) 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 the [DBPP] and the [ST] (see **[OS.CA-1]**).

This Page Intentionally Blank

ANNEX

A

Password Profile Controls

This Annex specifies the password control requirements that must be applied to all profiles in the evaluated configuration of the TOE. Assertion **[DB.IA-18]** states that the password control limits specified in this Annex must be applied to the default profile as part of the installation task, and then to all new profiles created subsequently.

This Annex does however provide database administrators with a choice of two profiles, both of which provide password controls that are strong enough to meet the claimed CC Strength of Function rating of SOF-*high*. Both choices can also be strengthened further, if necessary, however administrators should see the guidance in section 2.2 of this document, and carefully consider their security requirements and the implications of the profile changes before implementing any such changes.

The two profiles suggested below, entitled ProfileA and ProfileB, require creation via a SQL script (which could be achieved by modifying an example script supplied with the TOE), as well as execution of the script and a SQL statement in the database. The steps are explained fully in Sections A.2 and A.3. A rationale for the two choices available is provided in section A.1.

ProfileA and ProfileB were used during the evaluation of the TOE, along with variants of them that added strengthened password controls. Any installation of the TOE can remain within the TOE's Evaluated Configuration provided that ProfileA or ProfileB are used or, if variants of them are used, then it must be possible to show that the changes have added strengthened password controls.

A.1 Rationale

ProfileA specifies a complexity check function that enforces a minimum password length of 8 characters. It is intended that this profile achieves the required strength by enforcement of password length alone, thereby presenting an attacker with an unreasonably large password space to search. This type of profile may be preferred by ad-

ministrators who do not wish to use any type of lockout on user accounts, i.e. for availability reasons.

Profile B specifies a complexity check function that enforces a minimum password length of 6 characters, plus a 1 minute lockout whenever 3 consecutive failed log in attempts are made. The rationale for this profile is that administrators may not want to mandate a length of 8 for user passwords, but by reducing this to a length of 6 the profile is strengthened by introducing a temporary lockout. This type of lockout works extremely effectively against automated attacks by almost nullifying the speed advantage they would have over manual attacks. The temporary nature of the lockout (one minute is suggested as being sufficient, although a longer time would strengthen this profile) counters a denial of service attack, since the accounts automatically re-enable themselves after the lockout time expires.

The complexity check function for both profiles will do the following checks:

- Check that the password supplied is not the same as the username;
- Check the length of the password meets the minimum requirement;
- Raise application errors if either of these two checks fail.

The two sections for ProfileA and ProfileB below both specify in full the `CREATE FUNCTION` statement that will create a PL/SQL function to be the complexity check. This function can either be created by entering the full creation statement into the database, or by putting it into a SQL script and executing this within the database. The ProfileA and ProfileB sections also specify the SQL statement that can then be used to modify or create profiles to incorporate the new complexity check function.

As a further alternative to creating a script from scratch (by using a text editor), the example complexity check function supplied with the TOE can be modified. The example script supplied is called *utlpwdmg.sql*, and instructions for modifying this (as an alternative to using the scripts in Sections A.2 and A.3) are given in section A.4 below.

A.2 ProfileA

To implement ProfileA, the complexity check function needs to be created, and then assigned to the profile.

Section A.2.1 supplies a listing for a SQL script that, when executed, will create the function. Note, the function can also be entered directly into the database if required (omit the `Rem` statements), however a script is recommended as this will preserve the function definition for future use or modification.

A.2.1 Script Listing

```
Rem Oracle9i Release 2(9.2.0) evaluated configuration
Rem Password complexity check (ProfileA)

CREATE OR REPLACE FUNCTION profilea

(username varchar2,

  password varchar2,

  old_password varchar2)

  RETURN boolean IS

n boolean;
```

```
BEGIN
Rem Check if the password is the same as the username
   IF password = username THEN
     raise_application_error(-20001, 'Password same as user');
   END IF;
Rem Check for the minimum length of the password
   IF length(password) < 8 THEN
     raise_application_error(-20002, 'Password length less than
8');
   END IF;
RETURN(TRUE);
END;
/
```

A.2.2 Database commands

To create the function from a script, the script must be executed in the database by an administrator (e.g. *sys*) as follows:

```
sqlplus> @profilea.sql
```

Once the complexity check function (called `profilea`) is created, then the default profile can be amended as follows:

```
alter profile default limit
password_verify_function profilea;
```

A.3 ProfileB

To implement ProfileB, the complexity check function needs to be created, and then assigned to the profile in conjunction with other profile limits.

Section A.3.1 supplies a listing for a SQL script that, when executed, will create the function. Note, the function can also be entered directly into the database if required (omit the `Rem` statements), however a script is recommended as this will preserve the function definition for future use or modification.

A.3.1 Script Listing

```
Rem Oracle9i Release 2(9.2.0) evaluated configuration
Rem Password complexity check (ProfileB)
CREATE OR REPLACE FUNCTION profileb
(username varchar2,
  password varchar2,
  old_password varchar2)
  RETURN boolean IS
   n boolean;
BEGIN
```

```
Rem Check if the password is the same as the username
   IF password = username THEN
     raise_application_error(-20001, 'Password same as user');
   END IF;
Rem Check for the minimum length of the password
   IF length(password) < 6 THEN
     raise_application_error(-20002, 'Password length less than
6');
   END IF;
RETURN(TRUE);
END;
/
```

A.3.2 Database Commands

To create the function from a script, the script must be executed in the database by an administrator (e.g. *sys*) as follows:

```
sqlplus> @profileb.sql
```

Once the complexity check function (called `profileb`) is created, then the default profile can be amended as follows:

```
alter profile default limit
failed_login_attempts 3
password_lock_time 1/1440
password_verify_function profileb;
```

A.4 Modifying utlpwdmg.sql

As an alternative to creating the function using the scripts described above, it is also possible to modify the *utlpwdmg.sql* script as described below.

1. In the check for minimum length of password, modify the value of '4' to either '8' (for ProfileA) or '6' (for ProfileB). Ensure this value is changed in two places - the line commencing `IF length`... and the line commencing `raise_application_error`.

2. Comment out all checks except the first two checks (the code for the first two checks ensures that the password is not the same as the username, and that the minimum length of password is met). Note, all lines of code under every check description should be commented out by placing the word "Rem" at the start of the line.

3. Ensure that having commented out every check underneath the first two, that the following lines at the end of the function remain un-commented out:

```
RETURN(TRUE);
END;
/
```

4. Comment out all the lines of the `ALTER PROFILE` statement at the end of the

script by placing the word “Rem” at the start of each line.

5. Save the modified script (it is recommended that a different filename is used e.g. `profilea.sql` or `profileb.sql`). Then using a tool such as SQL*PLUS, connect as a privileged user (e.g. *sys*) and run the script to create the complexity check function as follows:

```
sqlplus> @profilea.sql
```

6. The default profile can then be modified to include the complexity check function as follows:

```
sqlplus> alter profile default limit
password_verify_function profilea;
```

This Page Intentionally Blank

APPENDIX

B TOE Components

B.1 Server components

The following is a list of all the software components that are installed on the server by the Oracle Universal Installer during the installation of the Oracle9*i* RDBMS as per **[DB-3]**:

- Advanced Queueing (AQ) API 9.2.0.1.0
- Advanced Replication 9.2.0.1.0
- Agent Required Support Files 9.2.0.1.0
- Assistant Common Files 9.2.0.1.0
- Bali Share 1.1.17.0.0
- Character Set Migration Utility 9.2.0.1.0
- Common Files For Generic Connectivity Using OLEDB 9.2.0.1.0 (Windows only)
- DBJAVA Required Support Files 9.2.0.1.0 (Sun Solaris only)
- DB2400V4R5 Plugin 9.2.0.1.0 (Windows only)
- Database Management Services Common Files 9.2.0.1.0
- Database Configuration Assistant 9.2.0.1.0
- Database SQL Scripts 9.2.0.1.0
- Database Upgrade Assistant 9.2.0.1.0
- Database Verify Utility 9.2.0.1.0
- Database Workspace Manager 9.2.0.1.0
- Documentation Required Support Files 9.2.0.1.0
- Enterprise Edition Options 9.2.0.1.0 (Sun Solaris only)

- Enterprise Login Assistant 9.2.0.1.0 (Sun Solaris only)
- Enterprise Manager Base Classes 9.2.0.1.0
- Enterprise Manager Minimal Integration 9.2.0.1.0
- Enterprise Manager Translated Files 9.2.0.1.0
- Export/Import 9.2.0.1.0
- External Naming: NIS (Sun Solaris only)
- Generic Connectivity Common Files 9.2.0.1.0
- Generic Connectivity Using ODBC 9.2.0.1.0
- Generic Connectivity Using OLEDB-FS 9.2.0.1.0 (Windows only)
- Generic Connectivity Using OLEDB-SQL 9.2.0.1.0 (Windows only)
- Informix Plugin 9.2.0.1.0 (Windows only)
- Installation Common Files 9.2.0.1.0
- JDBC Common Files 9.2.0.1.0
- JDBC/OCI Common Files 9.2.0.1.0 (Windows only)
- Java Runtime Environment 1.1.8.16.0
- Java Runtime Environment 1.3.1.1.0a
- LDAP Required Support Files 9.2.0.1.0
- Microsoft Access Plugin 9.2.0.1.0 (Windows only)
- Microsoft SQL Server 2000 Plugin 9.2.0.1.0 (Windows only)
- Microsoft SQL Server 6.5 Plugin 9.2.0.1.0 (Windows only)
- Microsoft SQL Server 7.0 Plugin 9.2.0.1.0 (Windows only)
- Migration Utility 9.2.0.1.0
- MySQL Plugin 9.2.0.1.0
- New Database ID 9.2.0.1.0
- Object Type Translator 9.2.0.1.0
- Oracle Application Extensions 9.2.0.1.0 (Sun Solaris only)
- Oracle Call Interface (OCI) 9.2.0.1.0
- Oracle Client Required Support Files 9.2.0.1.0
- Oracle Code Editor 1.2.1.0.0A
- Oracle Common Schema Demos 9.2.0.1.0
- Oracle Complete DSS Starter Database 9.2.0.1.0
- Oracle Complete OLTP Starter Database 9.2.0.1.0
- Oracle Core Required Support Files 9.2.0.1.0
- Oracle Database Demos 9.2.0.1.0
- Oracle Database User Interface 2.2.11.0.0

- Oracle Database Utilities 9.2.0.1.0
- Oracle Display Fonts 9.0.2.0.0
- Oracle Dynamic Services Server 9.2.0.1.0
- Oracle EMD Agent Extensions 9.2.0.1.0 (Sun Solaris only)
- Oracle Enterprise Manager Products 9.2.0.1.0 (Sun Solaris only)
- Oracle Extended Windowing Toolkit 3.4.13.0.0
- Oracle Forms Extensions 9.2.0.1.0 (Sun Solaris only)
- Oracle Help For Java 3.2.13.0.0
- Oracle Help For Java 4.1.13.0.0
- Oracle Intype File Assistant 9.2.0.1.0 (Windows only)
- Oracle Ice Browser 5.06.8.0.0
- Oracle Intelligent Agent 9.2.0.1.0
- Oracle Intelligent Agent Base Component Files 9.2.0.1.0
- Oracle Intelligent Agent Configuration Tool 9.2.0.1.0
- Oracle Intelligent Agent Extensions 9.2.0.1.0 (Sun Solaris only)
- Oracle Internet Directory Client 9.2.0.1.0
- Oracle Internet Directory Core Common Files 9.2.0.1.0 (Sun Solaris only)
- Oracle Internet Directory Tools 9.2.0.1.0 (Sun Solaris only)
- Oracle JDBC Thin Driver for JDK 1.1.9.2.0.1.0
- Oracle JDBC Thin Driver for JDK 1.2.9.2.0.1.0
- Oracle JDBC/OCI Driver for JDK 1.1.9.2.0.1.0 (Windows only)
- Oracle JFC Extended Windowing Toolkit 4.1.10.0.0
- Oracle JVM 9.2.0.1.0
- Oracle Java Tools 9.2.0.1.0
- Oracle Label Security 9.2.0.1.0
- Oracle Message Gateway Common Files 9.2.0.1.0
- Oracle Migration Workbench 9.2.0.1.0 (Windows only)
- Oracle Net 9.2.0.1.0
- Oracle Net Configuration Assistant 9.2.0.1.0
- Oracle Net Listener 9.2.0.1.0
- Oracle Net Manager 9.2.0.1.0
- Oracle Net Required Support Files 9.2.0.1.0
- Oracle Net Services 9.2.0.1.0
- Oracle Remote Configuration Agent 9.2.0.1.0 (Windows only)
- Oracle SNMP Agent 9.2.0.1.0 (Windows only)

- Oracle Starter Database 9.2.0.1.0
- Oracle Text 9.2.0.1.0
- Oracle Trace 9.2.0.1.0
- Oracle Trace Required Support Files 9.2.0.1.0
- Oracle UIX 2.0.20.0.0
- Oracle Ultra Search Common Files 9.2.0.1.0
- Oracle Ultra Search Middle-Tier 9.2.0.1.0
- Oracle Ultra Search Server 9.2.0.1.0
- Oracle Universal Installer 2.2.0.12.0
- Sun Wallet Manager 9.2.0.1.0
- Oracle XML SQL Utility 9.2.0.1.0
- Oracle Intermedia 9.2.0.1.0
- Oracle Intermedia Annotator 9.2.0.1.0
- Oracle Intermedia Audio 9.2.0.1.0
- Oracle Intermedia Client Compatibility Files 9.2.0.1.0
- Oracle Intermedia Client Demos 9.2.0.1.0
- Oracle Intermedia Client Option 9.2.0.1.0
- Oracle Intermedia Common Files 9.2.0.1.0
- Oracle Intermedia Image 9.2.0.1.0
- Oracle Intermedia Java Advanced Imaging 9.2.0.1.0
- Oracle Intermedia Java Client 9.2.0.1.0
- Oracle Intermedia Java Media Framework Client 9.2.0.1.0
- Oracle Intermedia Locator 9.2.0.1.0
- Oracle Intermedia Video 9.2.0.1.0
- Oracle Intermedia Web Client 9.2.0.1.0
- Oracle9*i* 9.2.0.1.0
- Oracle9*i* Database 9.2.0.1.0
- Oracle9*i* Development Kit 9.2.0.1.0
- Oracle9*i* Globalization Support 9.2.0.1.0
- Oracle9*i* Syndication Server 9.2.0.1.0
- Oracle9*i* for Unix Documentation 9.2.0.1.0 (Sun Solaris only)
- Oracle9*i* Windows Documentation 9.2.0.1.0 (Windows only)
- PL/SQL 9.2.0.1.0
- PL/SQL Embedded Gateway 9.2.0.1.0
- PL/SQL Required Support Files 9.2.0.1.0

- Parser/Generator Required Support Files 9.2.0.1.0
- Platform Required Support Files 9.2.0.1.0
- Precompiler Common Files 9.2.0.1.0
- Precompiler Required Support Files 9.2.0.1.0
- RDBMS Required Support Files 9.2.0.1.0
- Recovery Manager 9.2.0.1.0
- Required Support Files 9.2.0.1.0
- SQL*Loader 9.2.0.1.0
- SQL*Plus 9.2.0.1.0
- SQL*Plus Required Support Files 9.2.0.1.0
- Secure Socket layer 9.2.0.1.0
- SSL Required Support Files 9.2.0.1.0
- Sun JDK 1.3.1.0.1a
- Sun JDK Extensions 9.2.0.1.0
- Sybase Adaptive Server 11 Plugin 9.2.0.1.0 (Windows only)
- Sybase Adaptive Server 12 Plugin 9.2.0.1.0 (Windows only)
- Utilities Common Files 9.2.0.1.0
- Visigenics ORB 3.4.0.0.0
- XDK Required Support Files 9.2.0.1.0
- XML 9.2.0.1.0
- XML Class Generator for Java 9.2.0.1.0
- XML Parser for Java 9.2.0.1.0
- XML Parser for Oracle JVM 9.2.0.1.0
- XML Parser for PL/SQL 9.2.0.1.0
- XML Transviewer Beans 9.2.0.1.0
- XML Transx 9.2.0.1.0
- XSQL Servlet 9.2.0.1.0
- regexp 2.0.20.0.0

B.2 Evaluated Configuration Boundaries

SQL*Plus Release 9.2.0.1.0 is used by the evaluators for testing the TOE components. However, it is not part of the evaluated configuration.

[DB-4] The evaluated configuration of the TOE shall therefore comprise exactly the following software components:

- Assistant Common Files 9.2.0.1.0

- Generic Connectivity Common Files 9.2.0.1.0
- Generic Connectivity Using ODBC 9.2.0.1.0
- Oracle Net 9.2.0.1.0
- Oracle Net Listener 9.2.0.1.0
- Oracle Net Manager 9.2.0.1.0
- Oracle Net Required Support Files 9.2.0.1.0
- Oracle Net Services 9.2.0.1.0
- Oracle Core Required Support Files 9.2.0.1.0
- Oracle Call Interface 9.2.0.1.0
- Oracle9*i* 9.2.0.1.0
- Oracle9*i* Database 9.2.0.1.0
- Oracle9*i* Development Kit 9.2.0.1.0
- Oracle9*i* Windows Documentation 9.2.0.1.0 (Windows only)
- Parser Generator Required Support Files 9.2.0.1.0
- Oracle Label Security 9.2.0.1.0
- PL/SQL 9.2.0.1.0
- PL/SQL Embedded Gateway 9.2.0.1.0
- PL/SQL Required Support Files 9.2.0.1.0
- Platform Required Support Files 9.2.0.1.0
- RDBMS Required Support Files 9.2.0.1.0
- Required Support Files 9.2.0.1.0

B.3 Client components

The following is a list of all the software components that are installed on the client by the Oracle Universal Installer during the installation of the client software as per **[DB.CA-1]**.

- Advanced Queueing (AQ) API 9.2.0.1.0
- Agent Required Support Files 9.2.0.1.0
- Assistant Common Files 9.2.0.1.0
- Bali Share 1.1.17.0.0
- Character Set Migration Utility 9.2.0.1.0
- DB2400V4R5 Plugin 9.2.0.1.0
- DBJAVA Required Support Files 9.2.0.1.0
- Documentation Required Support Files 9.2.0.1.0
- Enterprise Manager Minimal Integration 9.2.0.1.0

- Enterprise Manager Translated Files 9.2.0.1.0
- Export/Import 9.2.0.1.0
- Informix Plugin 9.2.0.1.0
- Installation Common Files 9.2.0.1.0
- JDBC Common Files 9.2.0.1.0
- JDBC/OCI Common Files 9.2.0.1.0
- Java Runtime Environment 1.1.8.16.0
- Java Runtime Environment 1.3.1.1.0a
- LDAP Required Support Files 9.2.0.1.0
- Microsoft Access Plugin 9.2.0.1.0
- Microsoft SQL Server 2000 Plugin 9.2.0.1.0
- Microsoft SQL Server 6.5 Plugin 9.2.0.1.0
- Microsoft SQL Server 7.0 Plugin 9.2.0.1.0
- MySQL Plugin 9.2.0.1.0
- Object Type Translator 9.2.0.1.0
- Oracle C++ Call Interface 9.2.0.1.0
- Oracle Call Interface (OCI) 9.2.0.1.0
- Oracle Client Required Support Files 9.2.0.1.0
- Oracle Code Editor 1.2.1.0.0A
- Oracle Core Required Support Files 9.2.0.1.0
- Oracle Database Utilities 9.2.0.1.0
- Oracle Extended Windowing Toolkit 3.4.13.0.0
- Oracle Help For Java 3.2.13.0.0
- Oracle Help For Java 4.1.13.0.0
- Oracle Intype File Assistant 9.2.0.1.0
- Oracle Ice Browser 5.06.8.0.0
- Oracle JDBC Thin Driver for JDK 1.1.9.2.0.1.0
- Oracle JDBC Thin Driver for JDK 1.2.9.2.0.1.0
- Oracle JDBC/OCI Driver for JDK 1.1.9.2.0.1.0
- Oracle JFC Extended Windowing Toolkit 4.1.10.0.0
- Oracle Migration Workbench 9.2.0.1.0
- Oracle Net 9.2.0.1.0
- Oracle Net Configuration Assistant 9.2.0.1.0
- Oracle Net Manager 9.2.0.1.0
- Oracle Net Required Support Files 9.2.0.1.0

- Oracle Network Utilities 9.2.0.1.0
- Oracle ODBC Driver 9.2.0.1.0
- Oracle Trace Required Support Files 9.2.0.1.0
- Oracle Universal Installer 2.2.0.12.0
- Oracle Workflow Builder 2.6.2.0.0
- Oracle Workflow Client 2.6.2.0.0
- Oracle Workflow Common Files 2.6.2.0.0
- Oracle Workflow Mailer 2.6.2.0.0
- Oracle XML SQL Utility 9.2.0.1.0
- Oracle9*i* Client 9.2.0.1.0
- Oracle9*i* Globalization Support 9.2.0.1.0
- Oracle9*i* Syndication Server 9.2.0.1.0
- Oracle9*i* Windows Documentation 9.2.0.1.0
- PL/SQL Required Support Files 9.2.0.1.0
- Parser/Generator Required Support Files 9.2.0.1.0
- Platform Required Support Files 9.2.0.1.0
- Precompiler Common Files 9.2.0.1.0
- Precompiler Required Support Files 9.2.0.1.0
- RDBMS Required Support Files 9.2.0.1.0
- Recovery Manager 9.2.0.1.0
- Required Support Files 9.2.0.1.0
- SQL*Loader 9.2.0.1.0
- SQL*Plus 9.2.0.1.0
- SSL Required Support Files 9.2.0.1.0
- Sun JDK 1.3.1.0.1a
- Sun JDK Extensions 9.2.0.1.0
- Sybase Adaptive Server 11 Plugin 9.2.0.1.0
- Sybase Adaptive Server 12 Plugin 9.2.0.1.0
- Utilities Common Files 9.2.0.1.0
- Visigenics ORB 3.4.0.0.0
- XDK Required Support Files 9.2.0.1.0
- XML Parser for Java 9.2.0.1.0

APPENDIX

C References

[ADG] *Oracle9i Application Developer's Guide - Fundamentals,* Release 2 (9.2), Part No.: A96590-01, Oracle Corporation.

[CC] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999

[DAG] *Oracle9i Database Administrator's Guide*, Release 2 (9.2), Part No.: A96521-01, Oracle Corporation.

[DBPP] *Database Management System Protection Profile,* Version 2.1, May 2000

[INST_SS_9*i*] *Oracle9i Installation Guide, Release 2 (9.2.0.1.0) for Unix Systems,* Part No.: A96167-01, Oracle Corporation

[INST_NT_9*i*] *Oracle9i Database Installation Guide Release 2 (9.2.0.1.0) for Windows*, Part No.: A95493-01

[NTC2] *Microsoft Windows NT 4.0 C2 Configuration Checklist, Last Updated 05 April 2000*, Available from http://www.microsoft.com/technet/security

[NT_START] *Oracle9i Database Getting Started Release 2 (9.2) for Windows*, Part No.: A95490-01

[ST] *OLS Security Target for Oracle9i, Release 2 (9.2.0),* Oracle Corporation

[STARTED] *How to get Started*, Oracle Corporation, A97375-01.

[SRN] *Solaris 8.0 Security Release Notes, Common Criteria Certification*, Version 1.0, December 2000, Sun Microsystems. Available from: http://www.sun.com/solaris/securitycert

[TCSEC] *Trusted Computer System Security Evaluation Criteria,* 5200 28-STD, December 1985, US Department of Defense