



OLS Evaluated Configuration for Oracle8i Release 3 (8.1.7)

April 2002

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

April 2002

Authors: Daniel Elliott,

Contributors: Duncan Harris, Peter Goatly.

This document is based on the equivalent document for Oracle8i Release 8.1.7. The contributions of the many authors of the precursors to this document are acknowledged.

Copyright © 2002, 2001, 2000, 1999 Oracle Corporation. All rights reserved. This documentation contains proprietary information of Oracle Corporation; it is protected by copyright law. Reverse engineering of the software is prohibited. If this documentation is delivered to a U.S. Government Agency of the Department of Defense, then it is delivered with Restricted Rights and the following legend is applicable:

RESTRICTED RIGHTS LEGEND

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of DFARS 252.227-7013, Rights in Technical Data and Computer Software (October 1988).

Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. Oracle Corporation does not warrant that this document is error free.

Oracle, SQL*Loader, and SQL*Net are registered trademarks of Oracle Corporation.

Oracle8i, PL/SQL, and Oracle Label Security are trademarks of Oracle Corporation.

All other products or company names are used for identification purposes only, and may be trademarks of their respective owners.

Contents

April 2002

1 Introduction.....	1
1.1 Intended Audience.....	1
1.2 Organization	1
1.3 Format	2
2 Physical Configuration	3
2.1 Physical Environmental Assumptions.....	3
2.2 Supporting Procedures	3
3 Host Configuration	7
3.1 Sun Solaris Operating System.....	7
3.2 Network Services	8
3.3 Client Applications.....	9
4 Oracle Configuration.....	11
4.1 O-RDBMS Server	11
4.2 Oracle Network Services.....	16
4.3 Oracle Client Applications	17
5 Step by Step Guide.....	19
5.1 Operating System Installation / Configuration.....	19
5.2 Installation of Oracle8i Server with OLS.....	19

Contents

April 2002

- 5.3 Configuration of Oracle 8i RDBMS 21
- 5.4 Configuration of Oracle Label Security..... 22
- 5.5 Client Installation..... 22

- A Password Profile Controls 25**

- B TOE Components 31**

- C References 39**

Introduction

The Target of Evaluation (TOE) is Oracle Label Security installed on top of the Oracle8i Release 3 (8.1.7) Object-Relational Database Management System (O-RD-BMS).

The TOE is hosted on one platform :

- Sun Solaris 8 (SunOS 2.8 Unix) Operating System.

This *OLS Evaluated Configuration for Oracle8i* 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 DBMS PP [DBPP]. The Security Target used for the evaluation of the TOE is the [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:

- | | |
|------------------|---|
| <i>Chapter 1</i> | contains the introduction to the document; |
| <i>Chapter 2</i> | describes the physical environment of the TOE and the network services required to support the TOE; |
| <i>Chapter 3</i> | describes the host operating system, network services, and client application configurations required to support the TOE; |
| <i>Chapter 4</i> | describes the configuration of the TOE, and all TOE-related network |

	services and applications;
<i>Chapter 5</i>	contains a step by step guide to installation of the TOE in its evaluated configuration;
<i>Annex A</i>	details the password management controls that must be implemented in all user profiles;
<i>Annex B</i>	lists the software components installed as per [ECD, 5.1.2] and
<i>Annex C</i>	lists the references that are used in this document.

1.3 Format

Assertions for the physical, host, and Oracle configurations are enumerated to the left of each evaluation configuration requirement in bold Helvetica font, e.g., **[A-1]**.

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.

Physical Configuration

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

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 the evaluated configuration document for the Sun platform [SUN-

INST]. 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. (In general the TOE does not record accounting information for operations performed by SYS, DBA and OPER. However, in certain restricted circumstances, such as instance start-up and shut-down, the TOE does write accounting information for these users to the OS audit trail only. This helps to support reliability and availability by avoiding any possibility that these users could be locked out of the TOE in the event that the database audit trail should become completely full.).

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 (for which the TOE will record accounting information in full).

- 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

Host Configuration

This chapter describes the configuration requirements for the Solaris server platform, the network services, and the client.

3.1 Sun Solaris Operating System

The TOE was evaluated and tested on one (1) Sun UltraSparc 1 server machine and one(1) Sun Sparcstation 20 client machine. These machines were connected by a Local Area Network (LAN).

The TOE was evaluated and tested on Sun Solaris 8 (SunOS 5.8) operating system running on both machines.

[SS-1]

The underlying operating system shall be Sun Solaris 8, which has met Common Criteria security requirements for assurance level EAL4.

[SS-3]

The underlying operating system identified in [SS-] should be installed and operated in a manner as described in the [SRN] Solaris 8.0 Security Release Notes.

[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 Admin Suite (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.

3.1.1 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`.

3.1.2 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 authorized users only.

These TOE directories containing all TOE executables and parameter and control files are located in the `$ORACLE_HOME` directory and its subdirectories.

[SS.PR-3]

The operating system shall protect system clocks against unauthorized modification so as to maintain the integrity of audit timestamps.

[SS.PR-4]

[SS.PR-3] should be accomplished by permitting only operating system administrators to access the operating system clock configuration. All other users should have no access permissions for the operating system clock.

3.1.3 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 shall include procedures that support the archiving of operating system audit trails and audit log files prior to audit trail or disk space exhaustion.

[SS.AA-4]

The operating system shall support the audit of TOE generated audit records of all TOE privileged connections and TOE start-up & shutdown operations in either its audit trail or into audit log files, irrespective of whether or not auditing is turned on in the TOE.

3.2 Network Services

[OS.NS-1]

The underlying network services should satisfy the requirements of the [ITSEC] Functionality Class F-C2 or greater, the requirements of the [TCSEC] Class C2 or greater, or the requirements of the [CC] Evaluation Assurance Level EAL3 or greater.

[OS.NS-2]

The underlying network services should be installed, and operated in a manner as described in the [ITSEC] or [CC] Certification Report, or the [TCSEC] Final Evaluation Report, and in accordance with their evaluated configuration and operational documentation, if available.

[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.

[OS.NS-5]

No other user shall be permitted to modify any network services configuration parameter.

3.3 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].

This Page Intentionally Blank

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 the [IUG-SS], [8IP_README], [OLS_INST] and [OLSP_README].

4.1 O-RDBMS Server

4.1.1 Identification and Authentication

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.

[DB.IA-1]

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.

[DB.IA-3]

System privileges that allow access to objects in “any schema” do not allow access to objects in SYS schema. Database administrators shall set the `INIT<SID>.ORA` 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.

[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.

[DB.IA-7]

Database administrators shall set the `INIT<SID>.ORA` 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-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 `INIT<SID>.ORA` file:

```
remote_login_passwordfile = EXCLUSIVE
```

This allows two types of privileged connection. Privileged connections (i.e. `AS SYSDBA`, `AS SYSOPER`, `INTERNAL`) 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:

Sun Solaris platform

```
dba
```

Note, on Solaris there are not separate OS groups for giving `sysdba` and `sysoper` privileges; the `dba` group gives both 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:

Sun Solaris platform

```
dba
```

Note, on Solaris there are not separate OS groups for giving `sysdba` and `sysoper` privileges; the `dba` group gives both 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 into 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 also 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 `INIT<SID>.ORA` 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 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, i.e. 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-8]

To ensure that all privileged connections to the TOE are audited, trusted users shall use Oracle Server Manager for all privileged connections to the TOE.

[DB.AA-9]

Database administrators shall ensure that changes to the database audit trail by are audited, by issuing the statement

```
audit insert, update, delete
on system.aud$
```

by access;

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 4.2.5 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 PL/SQL package is granted to PUBLIC by default. This should be revoked by executing the following SQL statement from an administrative connection to the database:

```
revoke execute on dbms_job 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 possess 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 created 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, Table 23-1].

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

[DB.SDD-1]

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.

Database administrators should implement a site-specific security policy as per their security requirements.

OLS Policy administrator should use the same label tags across multiple databases. 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.

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-1]

The network services that shall be installed using the Oracle Universal Installer 1.7.1.9.0 and by using the Custom Installation option are:

- Net8 Client 8.1.7.0.0
- Net8 Server 8.1.7.0.0

In addition to these network services, the following service is also automatically installed:

- Net8 Configuration Assistant 8.1.7.0.0

[DB.NS-2]

The installed network services shall be configured in the manner described in the [NP-IUG].

[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\NET80\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\NET80\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.

4.3 Oracle Client Applications

[DB.CA-1]

The client applications shall be installed using the Oracle Universal Installer Release 1.7.1.8.0 (for Solaris 8.0). The following software components shall be installed using Custom Installation option :

- Oracle 8i client 8.1.7.0.0
- Net8 Protocols 8.1.7.0.0
 - Net8 client 8.1.7.0.0
 - Oracle Protocol Support 8.1.7.0.0
- Oracle Utilities 8.1.7.0.0
 - SQL*Plus 8.1.7.0.0

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

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 back in again.

5.1 Operating System Installation / Configuration

Installation instructions for Sun Solaris, are given below.

5.1.1 Installation of Sun Solaris 8

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.

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

5.2 Installation of Oracle8i Server with OLS

5.2.1 Installation of Oracle 8i Release 3 (8.1.7)

Install the database using the Oracle Universal Installer in accordance with [8i_INST] and the remainder of this section.

[DB-2]

Oracle8i shall be installed using the Oracle Universal Installer 1.7.1.8.0. The option to install Oracle 8i Enterprise Edition 8.1.7.0.0 should be selected and within it, the Custom Installation option.

The TOE shall be installed using the default Product language of English and NOT English(United Kingdom).

[DB-3]

During installation of the server, ONLY the following software components shall be selected from the list of available products presented on the product installation

screen. All other components must be deselected:

- Oracle8 Enterprise Edition 8.1.7.0.0
 - Oracle 8i Server 8.1.7.0.0
 - Development Tools 8.1.7.0.0
 - Oracle Call Interface (OCI) 8.1.7.0.0
 - Oracle XML SQL Utility 2.0.0.0.0
 - Oracle Installation Products 8.1.7.0.0
 - Oracle Universal Installer 1.7.1.8.0
 - Oracle Configuration Assistants 8.1.7.0.0
 - Oracle Database Configuration Assistant 8.1.7.0.0
 - Oracle Utilities 8.1.7.0.0
 - SQL*Plus 8.1.7.0.0
 - Oracle Database Utilities 8.1.7.0.0
- Net8 Products 8.1.7.0.0
 - Net8 Client 8.1.7.0.0
 - Net8 Server 8.1.7.0.0
 - Oracle Names 8.1.7.0.0
 - Oracle Connection Manager 8.1.7.0.0
 - External Naming NIS
- Oracle Java Products 8.1.7.0.0
 - Oracle JDBC Drivers 8.1.7.0.0
 - Oracle JDBC/OCI Driver for JDK 1.1.8.1.7.0.0
 - Oracle JDBC/OCI Driver for JDK 1.2.8.1.7.0.0
 - Oracle JDBC Thin Driver for JDK 1.1.8.1.7.0.0
 - Oracle JDBC Thin Driver for JDK 1.2.8.1.7.0.0
 - Oracle Java Tools 8.1.7.0.0
- Oracle8i Unix Documentation 8.1.7.0.0

Note that although Java is not part of the evaluated configuration, it is automatically installed (See [DB.SAM-7])

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

5.2.1.1 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 devel-

opment of database applications in the evaluated configuration. These are the iFS (internet File System), the OCI internet cache, the KG platform (implements PL/SQL metadata sharing in applications), the Thin JDBC driver (provides java applets with a non-OCI interface to the database), and the new Java RepAPI protocol for snapshots (similar to the thin Java client interface).

5.2.2 Installation of Oracle8i Patch Set Version 8.1.7.3.0

Install the patch in accordance with the installation instructions provided in the README [8iP_README].

5.2.3 Installation of Oracle Label Security 8.1.7.0.0

OLS shall be installed in accordance with the OLS Installation Notes [OLS_INST].

ENSURE THAT THE LBACSYS PASSWORD IS CHANGED TO A VALUE KNOWN ONLY TO DATABASE ADMINISTRATORS.

5.2.4 Installation of Oracle Label Security 8.1.7.3.0 patch

Install OLS 8.1.7.3.0 patch in accordance with the installation instructions provided in the README [OLSP_README].

5.3 Configuration of Oracle 8i RDBMS

5.3.1 Protection of database files

Protect the database files from unauthorised access using steps [SS.PR-1] and [SS.PR-2] of [section 3.1.2](#). Network files shall be protected as described in steps [DB.NS-3] to [DB.NS-5] of [section 4.2](#).

5.3.2 Completing Installation

These steps must be completed to comply with the Evaluated Configuration.

[Re. DB.IA-3], Database administrators shall set the `INIT<SID>.ORA` parameter as follows:

```
o7_dictionary_accessibility = FALSE
```

[Re. DB.IA-7], Database administrators shall set the `INIT<SID>.ORA` parameter as follows

```
sql92_security = TRUE
```

[Re. DB.IA-14], the following parameter shall be set in the appropriate `INIT<SID>.ORA` file:

```
remote_login_passwordfile = EXCLUSIVE
```

[Re. DB.AA-2], the `audit_trail` parameter in the appropriate `INIT<SID>.ORA` parameter file for that O-RDBMS shall be assigned in one of the following two ways:

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

[Re. DB.AA-7], Database administrators shall ensure that session auditing is enabled at all times, i.e. by issuing the statement from an administrative connection to the database:

```
audit session;
```

[Re. DB.AC-7], This should be revoked by executing the following SQL statement from an administrative connection to the database:

```
revoke execute on dbms_job from public;
```

[Re. 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)
```

[Re. DB.AA-7], Database administrators shall ensure that changes to the database audit trail by are audited, i.e. by issuing the statement

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

5.3.3 Miscellaneous

The following steps are also required:

[Re. DB.IA-1], The administrator must ensure O-RDBMS I&A is configured for all users connecting to the TOE, i.e. all database users must have a *database password*.

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

[Re. DB.IA-4], 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. If the account is not to be used, then it should be locked and expired.

[Re. DB.IA-18], ensures that the default profile is amended to implement password controls for all users.

5.3.4 Completing Installation

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, [DB.NS-7], [NT.IA-13], and [SS.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 5.1.1](#) above;
- Install the client Oracle software as described in [section 4.3](#) above;
- Configure Net8 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.

This Page Intentionally Blank

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. Paragraph [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 a choice to database administrators; both choices 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 by creating a SQL script (or 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](#). Firstly a rationale for the two choices available is provided in [section A.1](#).

ProfileA and ProfileB are merely examples of profiles which could be used; plenty of other profiles could also achieve *SOF-high*. As long as a *SOF* analysis is performed to show *SOF-high* is achieved, any profile with appropriate password controls could be suitable alternatives. Of course, for true CC conformance, such a profile would need formal evaluation.

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 (i.e in 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 Oracle8i Release 3 (8.1.7) 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 :

```
SVRMGR> @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 Oracle8i Release 3(8.1.7) 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 :

```
SVRMGR> @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 Server Manager, connect as a privileged user (e.g. `sys`) and run the script to create the complexity check function as follows:

```
SVRMGR> @profilea.sql
```

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

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

This Page Intentionally Blank

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 Oracle8i RDBMS as per [DB-3].

- Advanced Queueing (AQ) API 8.1.7.0.0
- Agent Required Support Files 8.1.7.0.0
- Assistant Common Files 8.1.7.0.0
- Character Set Migration Utility 8.1.7.0.0
- Database SQL Scripts 8.1.7.0.0
- Database Verify Utility 8.1.7.0.0
- DBUI 1.1.2.0.0
- Development Tools 8.1.7.0.0
- Export/Import 8.1.7.0.0
- Extended Windowing Toolkit 3.3.6.0.0a
- External Naming: NIS 8.1.7.0.0 (Solaris Only)
- Generic Connectivity Common Files 8.1.7.0.0
- Generic Connectivity Using ODBC 8.1.7.0.0
- Installation Common Files 8.1.7.0.0
- Java Runtime Environment 1.1.8.10a
- JDBC Common Files 8.1.7.0.0
- JDBC/OCI Common Files 8.1.7.0.0
- LDAP Required Support Files 8.1.7.0.0

- Migration Utility 8.1.7.0.0
- Net8 Assistant 8.1.7.0.0
- Net8 Client 8.1.7.0.0
- Net8 Configuration Assistant 8.1.7.0.0
- Net8 Products 8.1.7.0.0
- Net8 Required Support Files 8.1.7.0.0
- Net8 Server 8.1.7.0.0
- NLS Required Support Files 8.1.7.0.0
- Oracle Call Interface (OCI) 8.1.7.0.0
- Oracle Client Required Support Files 8.1.7.0.0
- Oracle Configuration Assistants 8.1.7.0.0
- Oracle Connection Manager 8.1.7.0.0
- Oracle Core Required Support Files 8.1.7.0.0
- Oracle Database Configuration Assistant 8.1.7.0.0
- Oracle Database Demos 8.1.7.0.0
- Oracle Database Utilities 8.1.7.0.0
- Oracle Enterprise Java Beans and CORBA Tools 8.1.7.0.0
- Oracle help For Java 3.1.8.0.0a
- Oracle Installation Products 8.1.7.0.0
- Oracle Internet Directory Client 2.1.1.0.0
- Oracle Java Products 8.1.7.0.0
- Oracle Java Server Pages 1.1.0.0.1
- Oracle Java Tools 8.1.7.0.0
- Oracle JDBC Drivers 8.1.7.0.0
- Oracle JDBC Thin Driver for JDK 1.1 8.1.7.0.0
- Oracle JDBC Thin Driver for JDK 1.2 8.1.7.0.0
- Oracle JDBC/OCI Driver for JDK 1.1 8.1.7.0.0
- Oracle JDBC/OCI Driver for JDK 1.2 8.1.7.0.0
- Oracle JServer 8.1.7.0.0
- Oracle Names 8.1.7.0.0
- Oracle Starter Database 8.1.7.0.0
- Oracle Trace 8.1.7.0.0
- Oracle Trace Required Support Files 8.1.7.0.0
- Oracle Universal Installer 1.7.1.8.0
- Oracle Utilities 8.1.7.0.0

- Oracle Wallet Manager 8.1.7.0.0
- Oracle XML SQL Utility 2.0.0.0.0
- Oracle8i Enterprise Edition 8.1.7.0.0
- Oracle8i Server 8.1.7.0.0
- Oracle8i Unix Documentation 8.1.7.0.0
- Parser Generator Required Support Files 8.1.7.0.0
- PL/SQL 8.1.7.0.0
- PL/SQL Embedded Gateway 8.1.7.0.0
- PL/SQL Required Support Files 8.1.7.0.0
- Platform Required Support Files 8.1.7.0.0
- Precompiler Required Support Files 8.1.7.0.0
- RDBMS Required Support Files 8.1.7.0.0
- Recovery Manager 8.1.7.0.0
- Replication API 8.1.7.0.0
- Required Support Files 8.1.7.0.0
- Secure Socket Layer 8.1.7.0.0
- Server Manager 8.1.7.0.0
- SQL*Loader 8.1.7.0.0
- SQL*Plus 8.1.7.0.0
- SQLJ Runtime 8.1.7.0.0
- SSL Required Support Files 8.1.7.0.0
- Utilities Common Files 8.1.7.0.0
- Visigenics ORB 3.4
- XML 8.1.7.0.0
- XML Class Generator for Java 1.0.2.0.0
- XML Parser for Java 2.0.2.9.0
- XML Parser for PL/SQL 1.0.2.0.0
- XML Transviewer Beans 1.0.3.0.0
- XSQL Servlet 1.0.0.0.0

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 RDBMS 8.1.7.3.0 patch [DB-3].

Oracle8i Patch Set 8.1.7.3.0

- JDBC Common Files Patch 8.1.7.3.0
- JDBC/OCI Common Files Patch 8.1.7.3.0

- Oracle JDBC Thin Driver for JDK 1.1 Patch 8.1.7.3.0
- Oracle JDBC Thin Driver for JDK 1.2 Patch 8.1.7.3.0
- Oracle Connection Manager Patch 8.1.7.3.0
- Oracle Names Patch 8.1.7.3.0
- Net8 Configuration Assistant Patch 8.1.7.3.0
- Net8 Client Patch 8.1.7.3.0
- Net8 Server Patch 8.1.7.3.0
- External Naming: NIS Patch 8.1.7.3.0
- Secure Socket Layer Patch 8.1.7.3.0
- Oracle8i Server Patch 8.1.7.3.0
- Advanced Queuing (AQ) API Patch 8.1.7.3.0
- Database SQL Scripts Patch 8.1.7.3.0
- Database Verify Utility Patch 8.1.7.3.0
- Oracle Database Demos Patch 8.1.7.3.0
- Export/Import Patch 8.1.7.3.0
- PL/SQL Embedded Gateway Patch 8.1.7.3.0
- Generic Connectivity Using ODBC Patch 8.1.7.3.0
- Migration Utility Patch 8.1.7.3.0
- Oracle Call Interface (OCI) Patch 8.1.7.3.0
- PL/SQL 8.1.7.3.0
- Recovery Manager Patch 8.1.7.3.0
- SQL*Loader 8.1.7.3.0
- Server Manager Patch 8.1.7.3.0
- Oracle Client Required Support Files Patch 8.1.7.3.0
- LDAP Required Support Files Patch 8.1.7.3.0
- Net8 Required Support Files Patch 8.1.7.3.0
- PL/SQL Required Support Files Patch 8.1.7.3.0
- Precompiler Required Support Files Patch 8.1.7.3.0
- RDBMS Required Support Files Patch 8.1.7.3.0
- SSL Required Support Files Patch 8.1.7.3.0
- Oracle Database Utilities Patch 8.1.7.3.0
- Utilities Common Files Patch 8.1.7.3.0
- Oracle JServer Patch 8.1.7.3.0
- Generic Connectivity Common Files Patch 8.1.7.3.0
- Net8 Assistant Patch 8.1.7.3.0

- Oracle Wallet Manager Patch 8.1.7.3.0
- SQLJ Runtime Patch 8.1.7.3.0
- Character Set Migration Utility Patch 8.1.7.3.0
- Oracle Enterprise Java Beans & CORBA Tools Patch 8.1.7.1.0
- Oracle Java Tools Patch 8.1.7.1.0
- XSQL Servlet Patch 1.0.4.1.1
- XML Parser for Java Patch 2.0.2.9.2
- XML Parser for PL/SQL Patch 1.0.2.2.0

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 OLS 8.1.7.0.0 patch.

- Oracle Military Security 8.1.7.0.0

B.2 Evaluated Configuration Boundaries

[DB-4]

SQL*Plus Release 8.1.7.0.0 is used by the evaluators for testing the TOE components. However, it is not part of the evaluated configuration.

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

- Character Set Migration Utility 8.1.7.0.0 (Character Set Migration Utility Patch 8.1.7.3.0)
- Database SQL Scripts 8.1.7.0.0 (Database SQL Scripts Patch 8.1.7.3.0)
- Database Verify Utility 8.1.7.0.0 (Database Verify Utility Patch 8.1.7.3.0)
- Development Tools 8.1.7.0.0
- Generic Connectivity Common Files 8.1.7.0.0 (Generic Connectivity Common Files Patch 8.1.7.3.0)
- Generic Connectivity Using ODBC 8.1.7.0.0 (Generic Connectivity Using ODBC Patch 8.1.7.3.0)
- JDBC Common Files 8.1.7.0.0 (JDBC Common Files Patch 8.1.7.3.0)
- JDBC/OCI Common Files 8.1.7.0.0 (JDBC/OCI Common Files Patch 8.1.7.3.0)
- Net8 Client 8.1.7.0.0 (Net8 Client Patch 8.1.7.3.0)
- Net8 Server 8.1.7.0.0 (Net8 Server Patch 8.1.7.3.0)
- Net8 Products 8.1.7.0.0
- Net8 Required Support Files 8.1.7.0.0 (Net8 Required Support Files Patch 8.1.7.3.0)
- NLS Required Support Files 8.1.7.0.0
- Oracle Client Required Support Files 8.1.7.0.0 (Oracle Client Required Support Files Patch 8.1.7.3.0)
- Oracle Connection Manager 8.1.7.0.0 (Oracle Connection Manager Patch

8.1.7.3.0)

- Oracle Core Required Support Files 8.1.7.0.0
- Oracle Database Utilities 8.1.7.0.0 (Oracle Database Utilities Patch 8.1.7.3.0)
- Oracle JDBC/OCI Driver for JDK 1.1.8.1.7.0.0
- Oracle JDBC/OCI Driver for JDK 1.2.8.1.7.0.0
- Oracle Call Interface 8.1.7.0.0 (Oracle Call Interface (OCI) Patch 8.1.7.3.0)
- Oracle Utilities 8.1.7.0.0
- Oracle Universal Installer 1.7.1.8.0 (Solaris ONLY)
- Oracle8i Enterprise Edition 8.1.7.0.0
- Oracle8i Server 8.1.7.0.0 (Oracle8i Server Patch 8.1.7.3.0)
- Parser Generator Required Support Files 8.1.7.0.0
- PL/SQL 8.1.7.0.0 (PL/SQL 8.1.7.3.0)
- PL/SQL Embedded Gateway 8.1.7.0.0 (PL/SQL Embedded Gateway Patch 8.1.7.3.0)
- PL/SQL Required Support Files 8.1.7.0.0 (PL/SQL Required Support Files Patch 8.1.7.3.0)
- Platform Required Support Files 8.1.7.0.0
- Precompiler Required Support Files 8.1.7.0.0 (Precompiler Required Support Files Patch 8.1.7.3.0)
- RDBMS Required Support Files 8.1.7.0.0 (RDBMS Required Support Files Patch 8.1.7.3.0)
- Required Support Files 8.1.7.0.0
- Server Manager 8.1.7.0.0 (Server Manager Patch 8.1.7.3.0)
- SQL*Plus 8.1.7.0.0
- Utilities Common Files 8.1.7.0.0 (Utilities Common Files Patch 8.1.7.3.0)

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].

- Agent Required Support Files 8.1.7.0.0
- Assistant Common Files 8.1.7.0.0
- Extended Windowing Toolkit 3.3.6.0.0a
- Installation Common Files 8.1.7.0.0
- Java Runtime Environment 1.1.8.10a
- LDAP Required Support Files 8.1.7.0.0
- Net8 Assistant 8.1.7.0.0

- Net8 Client 8.1.7.0.0
- Net8 Configuration Assistant 8.1.7.0.0
- Net8 Products 8.1.7.0.0
- Net8 Required Support Files 8.1.7.0.0
- NLS Required Support Files 8.1.7.0.0
- Oracle8i Client 8.1.7.0.0
- Oracle Client Required Support Files 8.1.7.0.0
- Oracle Core Required Support Files 8.1.7.0.0
- Oracle help For Java 3.1.8.0.0a
- Oracle Protocol Support 8.1.7.0.0
- Oracle Trace Required Support Files 8.1.7.0.0
- Oracle Utilities 8.1.7.0.0
- Parser Generator Required Support Files 8.1.7.0.0
- PL/SQL Required Support Files 8.1.7.0.0
- Platform Required Support Files 8.1.7.0.0
- Precompiler Required Support Files 8.1.7.0.0
- RDBMS Required Support Files 8.1.7.0.0
- Required Support Files 8.1.7.0.0
- SQL*Plus 8.1.7.0.0
- SSL Required Support Files 8.1.7.0.0

This Page Intentionally Blank

C

References

[CC]	<i>Common Criteria for Information Technology Security Evaluation</i> , Version 2.1, August 1999
[DBPP]	<i>Database Management System Protection Profile</i> , Version 2.1, May 2000
[ITSEC]	<i>Information Technology Security Evaluation Criteria</i> , Version 1.2, June 1991, UK IT Security Evaluation and Certification Scheme
[8i_INST]	<i>Oracle 8i Enterprise Edition Installation, Release 8.1.7 for Sun SPARC Solaris</i> , Part No.: A85471-01, Oracle Corporation
[8iP_README]	<i>Oracle 8i Server Patch Set version 8.1.7.3.0.0 for Sun SPARC Solaris (32-bit)</i> , Patch Set Notes, Oracle Corporation
[OLS_INST]	<i>Oracle Label Security Installation Notes, Release 8.1.7 for Sun SPARC Solaris</i> , Part No.: A87348-01, December 2000, Oracle Corporation
[OLSP_README]	<i>Oracle Label Security Patch 8.1.7.3.0 Readme, for Sun SPARC Solaris</i> , Oracle Corporation
[OAR_SSP]	<i>Oracle 8i Enterprise Edition Administrators Reference, Release 3 (8.1.7) for Sun SPARC Solaris</i> , Part No.: A85349-01, August 2000, Oracle Corporation
[ST]	<i>OLS Security Target for Oracle8i, Release 3 (8.1.7)</i> , Oracle Corporation
[TCSEC]	<i>Trusted Computer System Security Evaluation Criteria</i> , 5200 28-STD, December 1985, US Department of Defense
[STARTED]	<i>How to get Started</i> , Release 8.1.7, Oracle Corporation, A90548-01.
[SUN_INST]	<i>Solaris 8.0 Security Release Notes, Common Criteria Certi-</i>

figuration, Version 1.0, December 2000, Sun Microsystems.
Available from: <http://www.sun.com/solaris/securitycert>