Security Target

for Oracle Identity and Access Management 10*g* (10.1.4.0.1)

March 2008

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

Security Target for Oracle Identity and Access Management 10*g* (10.1.4.0.1)

March 2008

Authors: Julian Skinner and Peter Goatly.

Contributor: Adam O’Brien.

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.

Contents

CHAPTER

1 Introduction

This document is the security target for the Common Criteria evaluation of Oracle Identity and Access Management 10*g* (10.1.4.0.1). For this evaluation of Oracle Identity and Access Management, the products that are in the Target of Evaluation are Oracle Access Manager (OAM), Oracle Virtual Directory (OVD) and Oracle Internet Directory (OID).

Identification and CC Conformance

Title: Security Target for Oracle Identity and Access Management 10*g* (10.1.4.0.1).

Target of Evaluation (TOE):
Oracle Access Manager with Patch 5912931, Oracle Virtual Directory and Oracle Internet Directory.

Release: 10*g* (10.1.4.0.1).

Operating System Platform:
Red Hat Enterprise Linux AS Version 4 Update 5.

Database Platform: Oracle Database 10*g* (10.1.0.5.0).

Web Server Platform: Oracle HTTP Server 10*g* (10.1.3.1.0).

CC Conformance:
This Security Target conforms to CC Part 2 Extended and CC Part 3. All SFRs in the Security Target are derived from [CC], although several SFRs are extended. ALC_FLR.3 is the only augmented assurance criterion specified.

Assurance: EAL4 augmented with ALC_FLR.3[1].

Keywords: Oracle Identity and Access Management, OAM, OVD, OID, EAL4.

[1] ALC_FLR.3 provides assurance at the highest defined component level that there are flaw remediation procedures for the TOE by which discovered security flaws can be reported to, tracked and corrected by the developer, and by which corrective actions can be issued to TOE users in a timely fashion.

Version of the Common Criteria [CC] used to produce this document: 2.3.

TOE Overview

Oracle Identity and Access Management (Oracle IAM) is a suite of products that allows enterprises to manage and automate the end-to-end lifecycle of user identities, and provides users with secure, fine-grained access to enterprise resources and assets.

For this evaluation of Oracle Identity and Access Management, the products that are in the Target of Evaluation are Oracle Access Manager, to which Patch 5912931 has been applied, Oracle Virtual Directory and Oracle Internet Directory.

Oracle Access Manager provides Web-based identity administration, as well as access control to Web applications and resources running in a heterogeneous environment.

Oracle Virtual Directory is an LDAPv3-enabled service that provides virtualised abstraction of one or more enterprise data sources into a single directory view.

Oracle Internet Directory is a general purpose directory service that enables fast retrieval and centralised management of information about dispersed users and network resources. It combines LDAPv3 with the high performance, scalability, robustness, and availability of the Oracle Database server. Oracle Internet Directory 10*g* (10.1.4.0.1) is currently in evaluation at Common Criteria EAL4+.

The security functionality in the TOE includes:

- user identification and authentication with password management, for which OVD provides OAM with access to user security attributes;
- resource access control imposed by OAM, whereby Policy Domains held via OID are used to control who can access resources such as Web content; and
- auditing.

The Lightweight Directory Access Protocol (LDAP) is a standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate. LDAP Version 3 is defined in [LDAP3].

TOE Product Components

The Oracle Identity and Access Management products which constitute the TOE are Oracle Access Manager 10*g* (10.1.4.0.1), Oracle Virtual Directory 10*g* (10.1.4.0.1) and Oracle Internet Directory 10*g* (10.1.4.0.1).

The WebGate component of Oracle Access Manager 10*g* (10.1.4.0.1) runs as a module under Oracle HTTP Server 10*g* (10.1.3.1.0).

Oracle Internet Directory relies on the Oracle 10*g* Database Server Enterprise Edition 10.1.0.5.0 for the storage of directory data and uses Oracle Net Services 10.1.0.5.0 for communication interfaces.

Oracle Process Manager and Notification Server (OPMN) is installed and configured with every Oracle Application Server installation type and is used to start, monitor and stop OID's processes in the TOE's evaluated configuration.

[ECD] defines how the TOE products must be installed in the evaluated configuration and defines the requirements for setting up the TOE environment.

Document Overview

Change bars indicate changes since the previous issue.

Chapter 2 of this security target provides a high-level overview of the security features of the TOE. Chapter 3 identifies the assumptions, threats, and security policies of the TOE environment. Chapter 4 describes the security objectives for the TOE and for the environment needed to address the assumptions, threats, and security policies identified in Chapter 3. Chapter 5 identifies the Security Functional Requirements (SFRs), the Security Assurance Requirements (SARs) and the security requirements for the IT environment. Chapter 6 summarises each Security Function (SF) provided by the TOE to meet the security requirements. Chapter 7 covers the topic of protection profile conformance by the TOE and Chapter 8 provides the rationale for the security claims made within this security target.

Annex A contains a list of references and Annex B provides a glossary of the terms.

This Page Intentionally Blank

CHAPTER

2 TOE Description

This chapter describes the product features that provide security mechanisms and contribute to the security of a system using the TOE. For this evaluation, the Oracle Identity and Access Management products which constitute the TOE are Oracle Access Manager (OAM), Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD).

The major elements of the OAM, OID and OVD security architecture are described below, and the TOE is defined in terms of this architecture. The TOE's mechanisms for identification and authentication, access control, and accountability and auditing are summarised. Additional OAM, OID and OVD security features that are not addressed by the security functional requirements of Chapter 5 are also briefly discussed.

Oracle Identity and Access Management

Oracle Identity and Access Management is a suite of products that allows enterprises to manage and automate the end-to-end lifecycle of user identities, and provides users with secure, fine-grained access to enterprise resources and assets.

Oracle Access Manager

Oracle Access Manager provides Web-based identity administration, as well as access control to Web applications and resources running in a heterogeneous environment. It provides the user and group management, delegated administration, password management and self-service functions necessary to manage large user populations in complex, directory-centric environments.

Access Manager supports all popular authentication methods including browser forms, digital certificates and smart cards, and integrates seamlessly with most application servers and portals. User identities and credentials can be accessed from a number of LDAP-based repositories including Oracle Internet Directory, Microsoft Active Directory and Sun Java System Directory. With Access Manager, user access policies can be defined and enforced with a high degree of granularity through centralised management. Please note that only the limited set of authentication methods that are relevant to the secure network in the TOE's evaluated configuration are included in the TOE scope and that Oracle Virtual Directory is used as the LDAP-based repository for user security attributes in the evaluated configuration.

Oracle Internet Directory

Oracle Internet Directory is a general purpose directory service that enables fast retrieval and centralised management of information about dispersed users and network resources. It combines Lightweight Directory Access Protocol (LDAP) Version 3 with the high performance, scalability, robustness and availability of an Oracle database.

In the TOE, OID is used to store the policy data and configuration data required by Oracle Access Manager.

Oracle Virtual Directory

Oracle Virtual Directory is an LDAPv3-enabled service that provides virtualised abstraction of one or more enterprise data sources into a single directory view. Oracle Virtual Directory provides the ability to integrate LDAP-aware applications into diverse directory environments while minimizing or eliminating the need to change either the infrastructure or the applications.

In the TOE, Oracle Virtual Directory combines the user data required by OAM from multiple data sources to create an aggregated, virtual directory. From the point of view of OAM, the virtual directory looks and behaves just like any other LDAP directory.

Typical Configuration

The figure on the next page illustrates a typical configuration of the various products and systems deployed when using the TOE.

This configuration is based around Oracle Access Manager. Oracle Virtual Directory has also been included in the TOE because experience has shown that most systems that deploy OAM also deploy OVD. Finally, Oracle Access Manager has to directly use an LDAP directory for its policy and configuration data, so Oracle Internet Directory has been included in order to complete the typical TOE configuration.

This typical configuration is the basis for the TOE's evaluated configuration illustrated in the 'TOE Definition' later in this chapter.

The dotted line in the figure indicates the mechanism whereby Access Server can cause Identity Server to be entered via WebPass to enforce the TOE's password policy when an end user has requested access to a resource. To achieve this, Access Server redirects the end user's HTTP request to a Web page that causes WebPass to be entered. This occurs, for example, when the user's password has expired and the user has to supply a new one before the access request can be processed.

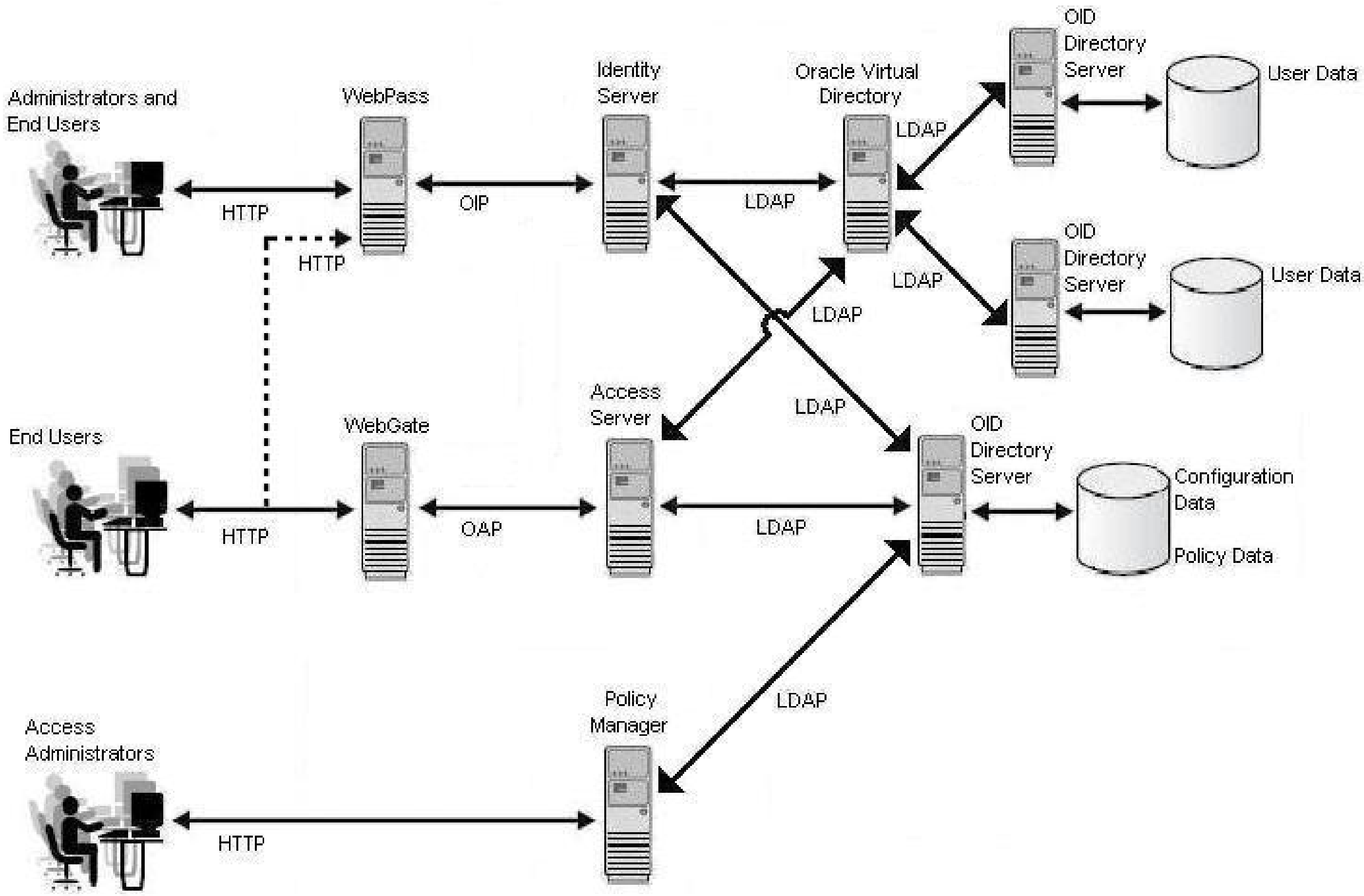

Figure 1: Typical configuration

Oracle Access Manager

The following sections describe the components of Oracle Access Manager.

Access Server

The Access Server is a stand-alone component that provides dynamic policy evaluation services for both Web-based and non-Web resources and applications. The Access Server receives requests from an access client, queries the LDAP directory for authentication, authorization and auditing rules and validates credentials, authorizes users, and manages user sessions for Oracle Access Manager.

- Authentication involves determining what authentication method is required for a resource, gathering credentials from the directory server and returning an HTTP response to the access client based on the results of credential validation.
- Authorization involves gathering access information, and granting access based on a policy domain stored in the directory and the identity established during authentication.

Access Client

An *Access Client* is an Access System component that monitors attempts to access a Web site and uses the Access Server to provide authorization and authentication services prior to completing the access requests. It can be either the client provided by the

Access System (see *WebGate*) or a client that is built into an application server or standalone application by using the Access Manager API.

WebGate

A WebGate is an out-of-the-box Access Client for HTTP-based resources. It is a Web server plug-in access client that intercepts HTTP requests for resources and forwards them to the Access Server for authentication and authorization.

Oracle HTTP Server

Oracle HTTP Server is the web server component of Oracle Application Server. In this evaluation it is used as a platform for the WebGate and does not form part of the TOE. Oracle HTTP Server 10*g* (10.1.2) has been certified under the Common Criteria at EAL4+.

OAP

The Oracle Access Protocol enables communication between Access System components during user authentication and authorization.

Policy Manager

The Policy Manager provides a Web-based interface that allows administrators to create and manage access policies. The Policy Manager also communicates with the directory server to write policy data, and communicates with the Access Server over OAP to update the Access Server when certain policy modifications are made. The Policy Manager is primarily used during the initial installation and configuration of the TOE.

Access System Console

The Web-based Access System Console provides a login interface to the tabs and functions that allow Administrators to perform specific configuration and reporting operations.

Identity Server

The Identity Server is a standalone server that is used to manage identity information about users, groups, organizations, and other objects. Applications within the server are accessed through a web-based interface. The Identity Server is primarily used during the initial installation and configuration of the TOE. Once the TOE is in its operational state the Identity Server is only used if Access Server causes it to be entered via WebPass to enforce the TOE's password policy.

WebPass

A WebPass is an OAM Web server plug-in that passes information back and forth between a Web server and the Identity Server. Depending upon its configuration, the Identity Server processes the request either as an XML or HTML file.

OIP

The Oracle Identity Protocol facilitates communication between the Identity Server and its associated WebPass instance.

Oracle Internet Directory

The following sections describe the components of Oracle Internet Directory.

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate. LDAP Version 3 is defined in [LDAP3].

Directory

A *directory* stores and retrieves information about organisations, individuals and other resources. It acts as the policy and configuration data repository for OAM in the configuration for this evaluation.

Directory Entries

In a directory, a collection of information about an object is called an *entry*. Each entry is uniquely identified by a *distinguished name* (DN), which defines exactly where in the directory's hierarchy the entry resides.

Each entry contains information stored in *attributes*. An *object class* is a group of attributes that define the structure of an entry.

Each directory has a *Directory-Specific Entry* (DSE), which holds information that relates to the whole directory, such as the audit log.

Oracle Directory Server Instance

Each *Oracle Directory Server instance* services LDAP requests through a single OID dispatcher process listening at a specific TCP/IP port number. There can be more than one directory server instance on a node, each listening on a different port.

One instance comprises one dispatcher process and one or more server processes. By default there is one server process for each instance.

Oracle Database 10*g*

OID runs as an Oracle Database 10*g* application. An Oracle database stores the directory data. The database can reside on the same node as the directory server processes or on a separate node.

Oracle Net Connections

OID communicates with the database using Oracle Net Services, Oracle's operating system-independent database connectivity solution. Oracle Net Services is used for all connections between the Oracle Database Server and the OID Control utility (`oidctl`), the directory server instance, and the OID Monitor (`oidmon`).

LDAP Clients

LDAP Clients send LDAP requests to an OID listener/dispatcher process listening for LDAP commands at its port.

The following command-line tools can be used to send LDAP commands to the Oracle Directory Server which is in the TOE's evaluated configuration:

```
ldapadd, ldapaddmt, ldapbind, ldapcompare, ldapdelete,
ldapmoddn, ldapmodify, ldapmodifymt, and ldapsearch.
```

Oracle Virtual Directory

The following sections describe the components of Oracle Virtual Directory.

Oracle Virtual Directory Server

Oracle Virtual Directory Server can integrate multiple directories by using its ability to talk to multiple directory sources through its *adapter* and *mapper* architecture and through the provision of full schema and namespace translation services. This ensures that data presented to applications from multiple proxied sources have a common and consistent format.

Adapters

OVD supports an unlimited number of directory data connection components known as *adapters*. Each adapter is responsible for managing a particular namespace that is represented by a specific parent distinguished name (DN). Multiple adapters can be combined and overlapped to present a customised directory tree. OVD supports the following adapter types:

- LDAP Adapter - provides proxied access to LDAPv2/LDAPv3 directory servers.
- Database Adapter - provides LDAP virtualization of relational database data.
- Storage Adapter - This adapter will form the base of the directory and will hold entries that are not proxied.

- Join View Adapter - provides real-time join capabilities between entries located in other OVD adapters.

Mappers

Oracle Virtual Directory includes a bi-directional mapping system based on the Python scripting language. A *mapper* is a special Python script that processes inbound and outbound transactional data flow within Oracle Virtual Directory. A mapping script can adjust requests as they enter the system on the way to data sources, and transform responses on the return path to the client.

OVD Listeners

Oracle Virtual Directory provides services to clients through two types of connections: LDAP and HTTP. LDAP is used to provide LDAPv3 based services while HTTP can provide one or more services such as DSMLv2, or basic white page functions provided by an XSLT enabled *Web Gateway*. The Web Gateway is not in the TOE's evaluated configuration.

TOE Definition

For this evaluation of Oracle Identity and Access Management the products which constitute the TOE are Oracle Access Manager, Oracle Internet Directory and Oracle Virtual Directory. Thus the TOE is a resource access control system that uses LDAP directories to hold its security credentials.

The Oracle Access Manager components included in the TOE are:

- Access Server;
- WebGate
- WebPass; and
- Identity Server.

The Identity Server and WebPass are primarily used during the initial installation and configuration of the TOE. Once the TOE is in its operational state the Identity Server and WebPass are only used if Access Server causes them to be entered to enforce the TOE's password policy.

The Oracle Virtual Directory components included in the TOE are:

- the OVD listener;
- the OVD server;
- Adapters; and
- Mappers.

The Oracle Internet Directory components included in the TOE are:

- the Oracle Directory Server; and
- the command line directory administration tools that are essential for the directory to be maintained and administered securely. Further details on these tools can be found in [OIDST, 2].

The software platforms for the TOE are listed in the 'Identification and CC Conformance' section of Chapter 1. These are:

- the Red Hat Enterprise Linux operating system;
- the Oracle Database system under which Oracle Internet Directory runs; and
- the Oracle HTTP Server under which WebGate and WebPass run.

The external interfaces into the TOE are:

- the call to the WebGate module from the OHS httpd daemon,
- the call to the WebPass module from the OHS httpd daemon to enforce the TOE's password policy when an end user has requested access to a resource, and
- access via the operating system command line to the directory administration tools that are essential for the OID directory to be maintained and administered securely.

The figure below illustrates the configuration of the TOE.

As in Figure 1 above, the dotted line in Figure 2 indicates the mechanism whereby Identity Server can be entered via WebPass to enforce the TOE's password policy. This happens as a result of Access Server redirecting the end user's HTTP request to a Web page that causes WebPass to be entered. An example of this redirection is when the user's password has expired and the user has to supply a new one before the access request can be processed.

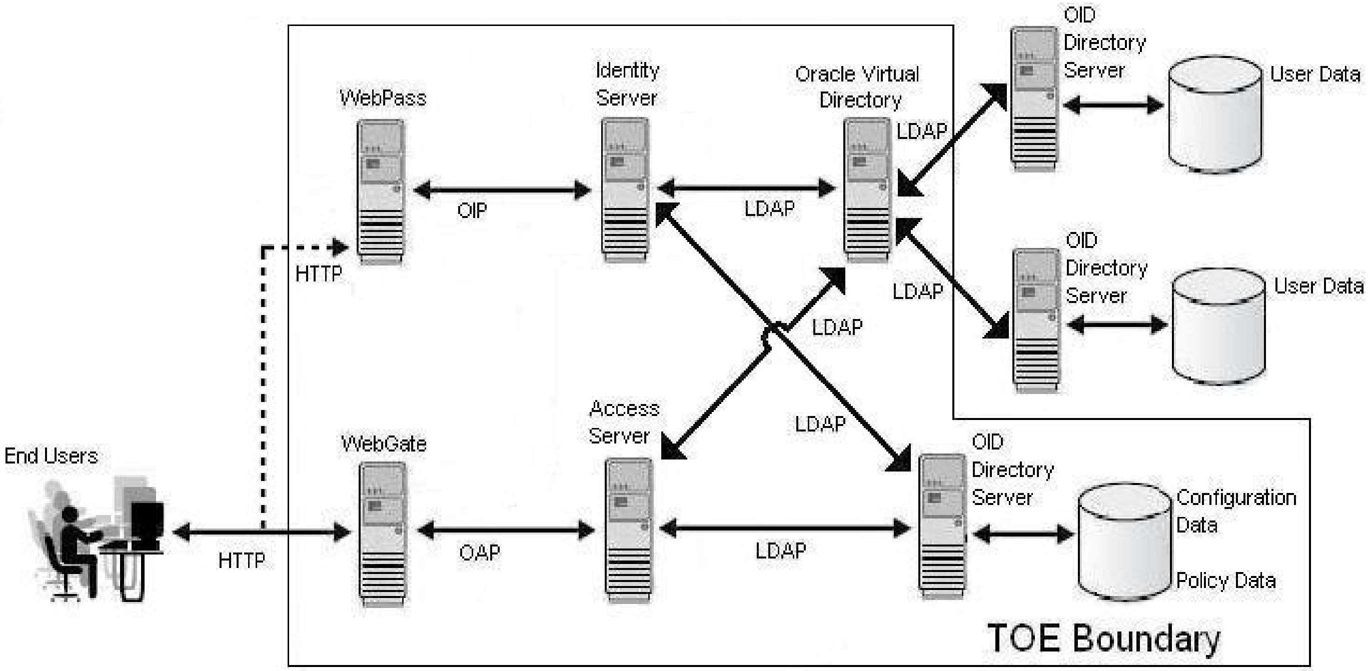

Figure 2: TOE configuration

TOE Modes of Operation

Modes

The TOE has the following modes of operation:

- startup;

- operational mode.

In startup mode, the various components constituting the TOE are being started up in readiness for the TOE to reach operational mode.

In operational mode, the TOE receives requests that have originated from an access client, queries the LDAP directories for authentication, authorization and auditing rules, validates credentials, authorizes users to access resources, and manages user sessions.

The use of Oracle Identity and Access Management administration tools to set up the LDAP directories to hold the authentication, authorization and auditing rules and credentials is outside the scope of the TOE.

The Oracle Identity and Access Management products have other modes of operation, such as for debugging, but these features are outside of the scope of this evaluation.

Operational Assumptions

The ‘Assumptions’ section of Chapter 3 provides assumptions about the use of the TOE. This includes the assumption that the processing resources of the TOE and the underlying system are to be located within controlled access facilities which prevent unauthorized physical access and the assumption that any other IT components with which the TOE communicates are under the same management control and operate under the same security policy as the TOE.

These operational assumptions are compatible with a secure environment in which Oracle Access Manager is used to serve resources to authorized users over a secure network.

Identification and Authentication

User Identification

Each TOE user entry is uniquely identified by its distinguished name (DN) attribute. The distinguished name indicates exactly where the entry resides in the directory hierarchy (represented by the *Directory Information Tree* (DIT)). A DN for a user could look like this:

```
cn=Alice Smith,ou=Server Technologies,c=UK,o=oracle
```

Within a distinguished name, the lowest component is called the *relative distinguished name* (RDN). In the example above the RDN is `cn=Alice Smith`.

To uniquely identify a particular entry within the overall DIT, the full DN must be used. This allows for user entries for two different Alice Smiths to exist within the same DIT.

Some of the attributes of a user entry relevant to identification and authentication include:

- `uid` - the attribute normally used by the user to login to the TOE (although a different attribute could be configured to identify the user); and
- `UserPassword` - the password to be used for authenticating the user to the TOE.

Master Administrator/ super user

The OAM *Master Administrator* is specified during installation. A user holding this role has access to all areas of OAM.

In OID this user account is known as the *super user* and is the administrator for a directory that holds TOE security attributes. The super user normally has full access to all directory information. The actual name and the password for the Master Administrator/super user are held in the DSE (by default the super user's name is `orcladmin`).

User Authentication

Authentication is the process of proving that a user is who he or she claims to be. To authenticate a user, a WebGate presents the user's browser with a request for authentication credentials in the form of a challenge. The challenge is referred to as a *challenge method*. Only Form-based and Anonymous challenge methods will be within the scope of this evaluation of the TOE.

For remote directories accessed through adapters, Oracle Virtual Directory supports the security inherent in those systems. Depending on the adapter used and its capabilities, a passcredentials option can be set to determine if end-user binding credentials should be passed to the remote directory for authentication and access control enforcement (see *Pass-through Authentication*).

Pass-through Authentication

When an adapter has pass-through enabled (via the passcredentials option) and a user is to be authenticated to the TOE via OVD, OVD will use the received user identification and password credentials to login to the remote directory on the user's behalf. If the authentication (bind) to the remote directory fails, OVD will fail the attempted bind by the user. In this mode, the remote directory is responsible for confirming the user's credentials.

Password Policies

Password policies consist of a set of rules that govern the characteristics of passwords that users can set and the validity period for passwords. Password policies also govern how users are notified of password expiry, how users reset expired passwords, and how users retrieve lost passwords.

These policies apply to users who try to login to the Identity and Access Systems. These policies also apply to users who try to access resources protected by the Access System.

Different password policies can be configured for different areas of the directory tree. A user can qualify under more than one policy in a domain. In this situation, password policies are evaluated in a bottom-to-top order.

Password policies control the characteristics and life cycle of a password, including the following aspects:

- rules for legal passwords e.g the minimum number of characters that can be used in a password and what types of characters must be used;
- challenge phrases and responses for lost password management;
- the minimum number of characters a password must contain;
- settings for password expiry and password reset;
- account lockout after incorrect password entry;
- unique password policies for individual sub-trees in the directory.

Guidance covering the different password controls and instructions to administrators to enable SOF-*high* to be achieved will be provided in the TOE's Evaluated Configuration Document [ECD].

Resource Access Control

The Access System enables administrators to control who can access resources such as Web content and traditional applications by defining *Policy Domains*.

Policy Domains and Policies

Policy domains are typically one or more URL prefixes that identify resources on the Web, along with authentication and authorization rules that determine who can access the resources, and at what time.

Administrators can also create *Policies* within a policy domain to define finer-grained protection for resources, for example, to protect a specific Web page or set of pages.

If a resource is not covered by a policy, the default rules of the domain apply.

A resource may fit the definition of more than one policy domain. The Access Server checks all policy domain definitions to find the policy domain with the most specific URL prefix that matches the resource. The policy domain that a resource belongs to is always the more specific one for the resource's URL.

Unlike the way that the Access Server checks policy domains, the Access Server checks policies in the order they are specified when they were configured. It then uses the first matching policy regardless of how many more policies there are.

Resource Types

A *resource type* describes the kind of resource to be protected, including its associated operations. Before resources can be added to a policy domain administrators must define their types and the operations associated with them that require protection.

By default the Access System defines resource types for HTTP and EJB resources.

Authentication Rules

For each policy domain, administrators must provide one default *authentication rule*. They can also create one authentication rule for each of a policy domain's policies. Authentication rules include *authentication schemes*.

Authentication Schemes

An *authentication scheme* includes the method used to challenge the user for credentials (see *challenge methods*). It also includes one or more steps consisting of one or more *plug-ins* used to perform different parts of the authentication process.

Only Master Administrators can create authentication schemes.

Authentication Plug-ins

Authentication *plug-ins* are a set of instructions for performing authentication. The Access System provides default plug-ins that implement certain methods used to challenge the user for credentials. For example, the Access System provides a credential mapping plug-in to map credentials obtained from a user requesting access to a resource to a user entry in the LDAP directory. Administrators can also create custom plug-ins.

Challenge Methods

The *challenge method* specifies how authentication is to be performed and the information required to authenticate the user. A challenge method must be included in every authentication scheme. The Access System supports the following five challenge methods:

1. Anonymous: Users are not prompted to provide any credential information.
2. Basic: Users must enter a user name and password in a window supplied by the Web server.

3. Client Cert (X509): X.509 digital certificates over SSL.
   A user's browser must supply a certificate.
4. Form: users enter information in the custom HTML form.
5. Ext: An external challenge method (outside of Oracle Access Manager) is used.
   This enables administrators to use their own authentication challenge method.

Only the Anonymous and Form-based challenge methods are allowed in the evaluated configuration of the TOE because they are the methods that are relevant to the secure network in the TOE's evaluated configuration.

ObSSOCookie

The ObSSOCookie is a single sign-on cookie that is generated by the Access Server when a user requests access to a resource and authenticates successfully. The ObSSOCookie is a session-based cookie that stores user identity information. This cookie is passed back to the user's browser in the response to the user's HTTP request, and is included in all subsequest HTTP requests sent by the user's browser to the Access Server. [RFC2965] has further details on cookies.

This cookie is the mechanism by which the TOE can be used for single sign-on.

Authorization Expressions

A policy domain and a policy can each contain only one *authorization expression*. An authorization expression includes:

- one or more *authorization rules;*
- operators (e.g. AND or OR) used to combine the rules.

Authorization Rules

An *authorization rule* specifies information that identifies who can access a resource the rule protects. It also specifies who is explicitly denied access to the resource. One or more authorization rules are included in an authorization expression for a policy domain or policy.

The result of evaluation of an authorization rule—in conjunction with other authorization rules, if more than one is included in the authorization expression—determines whether a user is granted access to the requested resource. Users who do not qualify for any of the conditions of the rule and who request access to a resource protected by the rule are, by default, denied access to the resource.

Authorization Schemes

An *authorization scheme*, which is included in an authorization rule, defines a method to be used to authorize a user. The Access System provides a default authorization scheme called Oracle Authorization Scheme. Authorization schemes for custom plug-ins that perform authorization tasks can also be created. Only a Master Administrator can create and manage authorization schemes.

Access Control Lists

Access Control Lists, often referred to as ACLs, are lists of Access Control Items or ACIs. ACLs govern the way directory entries and attributes are accessed, specifying which clients and which parts of the directory tree(s) may be accessed. The main purpose for ACLs, therefore, is to occupy a role in providing a secure environment where users who need access to data are granted it, and those who should not have access are denied it.

Oracle Virtual Directory enforces access control across its entire virtual directory namespace. Oracle Virtual Directory does this by storing access control information in a configuration file. This information is maintained automatically by intercepting modify requests to the entryACI and subtreeACI attributes. Similarly, it presents these attributes as part of the appropriate entries when queried.

Security Attributes

User Representation

The attributes of a user that are relevant to the identification and authentication of users by the TOE are:

- user identifier (which is normally the uid attribute);
- password; and
- Distinguished Name (DN).

The IP address of the machine that originated the user's request and time of access are further attributes of the user that may be taken into account when the TOE is mediating access to the requested resource.

In the evaluated configuration, the users' security attributes are held in data sources that are accessed via OVD.

Resource Security Attributes

The security attributes of a resource are

- its URL; and
- the policy domain or policy that applies to the resource.

In the evaluated configuration, information about policy domains and policies is held in an OID directory.

Audit and Accountability

The auditing feature of Oracle Access Manager collects and presents data pertaining to policy and profile settings, system events, and usage patterns. At the most detailed level, dynamic audit reports reveal when a system event was triggered and who triggered it.

Oracle Virtual Directory normally provides two log files: a general log and an access log. The general log holds information on operational errors and administrative events. The access log is a transaction log that reports on transactions that have occurred through the Oracle Virtual Directory system. Output to these log files can be individually enabled/disabled.

Audit Records

The Access System does not log any audit information to the audit log file until the Master Administrator creates a Master Audit Rule. The Master Audit Rule contains the following information:

- User identity attributes (for example, cn and uid);
- Events to audit (for example, authentication success and failure);
- Selection of a date format;
- Format and event mapping for the audit log.

Auditable Events

For each policy domain and policy, administrators can define audit rules to monitor and record events, including system events, successful and failed user authentications, and successful and failed authorization of users who request access to protected resources.

Audit Log File

An audit rule causes event-based data to be written to the audit log file. There is one audit log for each Access Server. Administrators can configure the size of the audit log file and the rotation interval for each server. Depending on events recorded, the audit log may contain some duplicate audit entries.

Audit records can be output to disk file, to a relational database, or both. In the evaluated configuration, audit records will be output to disk file.

The audit log file names, locations, rotation policies, and record formats for Oracle Vitrtual Directory are all configurable.

Audit Analysis

OAM does not provide audit analysis tools for Unix based operating systems.

Other Oracle Identity and Access Management Security Features

In addition to the security features described above, Oracle Identity and Access Manager provides features which are related to security but do not directly address any of the functional requirements identified in Chapter 5 of this document. These features provide significant security capabilities to support robust and reliable web servers.

The features described below are **not** within the scope of this evaluation.

AccessGate

An *AccessGate* is a custom access client that is specifically developed using the Software Developer Kit (SDK) and Oracle Access Manager APIs. An AccessGate is a form of access client that processes requests for Web and non-Web resources (non-HTTP) from users and applications.

OVD Manager

OVD includes a management and operations system that is based on the Eclipse™ 3.0 platform known as the Oracle Virtual Directory Manager. This system provides an easy way to manage and monitor multiple OVD servers.

Web Gateway

Part of OVD, the *Web Gateway* is an HTTP based gateway servlet that provides DSML and XSLT-rendered directory reporting. This web gateway also provides the ability to serve static web content, allowing the construction of sophisticated directory white page and delegated administration functions.

OVD Plug-ins

Oracle Virtual Directory provides a flexible plug-in framework modeled on Java Servlet Filters. Plug-ins can be used to provide custom logic as part of a transaction or simply to connect to a custom data source.

Other Oracle Identity and Access Management Products

[OIAMI, 1] lists the products which are components of the Oracle Identity and Access Management suite. The TOE only includes OAM, OID and OVD for this evaluation of Oracle Identity and Access Management.

The products described below are in the Oracle Identity and Access Management suite, but are **not** within the scope of this evaluation.

Oracle Identity Manager

The Oracle Identity Manager platform automates user identity provisioning and deprovisioning and allows enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources, both within and beyond the firewall. It provides an identity management platform that automates user provisioning, identity administration, and password management, wrapped in a comprehensive workflow engine.

Oracle Identity Federation

Federated identity management allows companies to operate independently and cooperate for business purposes by enabling cross-domain single sign-on and allowing companies to manage user identities and vouch for them as they access resources managed by another domain.

Oracle Identity Federation provides a self-contained federation solution that enables companies to manage multiple partners and choose from industry standard federated protocols. Identity Federation provides built-in integration with each customer's identity management infrastructure.

CHAPTER

3 Security Environment

This chapter identifies the IT assets protected by the TOE and the operational environment in which there are threats to these IT assets. It also covers the organisational security policies supported by the TOE and the assumptions for secure usage of the TOE.

IT Assets

The IT assets requiring protection consist of the resources that users can access as a result of requests received by Oracle Access Manager (OAM). The primary IT assets are:

- *Resources,* which the TOE can provide access to on receipt of suitable requests from OAM users.

The secondary IT assets, which support the protection of the primary assets are:

- *Security attributes,* which are held in an OID directory and in data sources accessed via OVD.
- *Configuration files,* which are held in filestore to govern the way the TOE products operate.
- *Audit data* generated by the TOE during its operation.

The TOE provides protection for the resources which it serves to users, but the operating system underlying the TOE is also required to provide protection for configuration files etc.

Operational Environment

In the evaluated configuration defined in [ECD], the TOE executes on an operating system that provides identification and authentication of its users, discretionary access controls on filestore items, process isolation and audit functions. In addition, [ECD] requires the administrator to employ physical and procedural controls in a way that provides protection against attacks against the IT assets, the TOE, its underlying system and the network that it is connected to. The requirements for such controls are covered in the Assumptions section below.

Threats

The assumed threats to TOE security, along with the threat agents which might instigate these threats, are specified below. Each threat statement identifies a means by which the TOE and its underlying system might be compromised.

These threats will be countered by:

a) technical security measures provided by the TOE, in conjunction with

b) technical security measures provided by the underlying system, and

c) non-technical operational security measures (personnel, procedural and physical measures) in the environment.

Threat agents

The threat agents are:

- *Outsiders* who are persons that are not authorized users of the IT environment underlying the TOE (operating system and/or database systems and/or web servers and/or network services and/or custom software);
- *Users* who are capable of making requests to access IT assets through the TOE;
- *System Users* who are persons authorized to use the the IT environment (or *system*) underlying the TOE;
- *Operational Interruptors* that cause the operation of the TOE to be interrupted as a result of failures of hardware, power supplies, storage media etc, where the source of the threat may be human (e.g. suppliers of equipment) or non-human (e.g. hardware glitches and natural disasters).

Threat agents can initiate the types of threats against the IT assets that are listed below.

Threats countered by the TOE

The threats in this section are countered by technical security measures provided by the TOE, supported by technical security measures provided by the underlying system and non-technical operational security measures in the environment.

T.DATA *Unauthorized Access to Resources.* A user obtains unauthorized access to resources via an access request to the TOE.

Note that this threat includes a user accessing a resource for which they are not authorized by impersonating another user.

T.ACCESS *Unauthorized Access to Security Attributes.* A user obtains unauthorized access to security attributes via an access request to the TOE.

T.ATTACK *Undetected Attack.* An undetected compromise of IT assets occurs as a result of an attacker attempting to perform actions, which the individual is not authorized to perform, via an access request to the TOE.

Note that this threat is included because, whatever countermeasures are provided to address the other threats, there is still a residual threat of a violation of the *security policy occuring by attackers attempting to defeat these countermeasures (e.g. by attempting to crack a user's password).*

T.ABUSE.USER *Abuse of Privileges.* An undetected compromise of IT assets occurs as a result of a user (intentionally or otherwise) performing actions the individual is authorized to perform.

Note that this threat is included because, whatever countermeasures are provided to address the other threats, there is still a residual threat of a violation of the security policy occuring, or IT assets being placed at risk, as a result of actions taken by authorized users. For example, a user may grant access to a directory object they are responsible for to another user who is able to use this information to perform a fraudulent action.

Threats countered only by the Operating Environment

TE.ACCESS *Unauthorized Access to IT Assets.* An outsider or system user obtains unauthorized access to IT assets other that via an access request to the TOE.

TE.OPERATE *Insecure Operation.* Compromise of IT assets may occur because of improper configuration, administration, and/or operation of the composite system.

TE.CRASH *Abrupt Interruptions.* Abrupt interruptions to the operation of the TOE may cause security related data, such as audit data, to be lost or corrupted. Such interruptions may arise from human error or from failures of software, hardware, power supplies, or storage media.

Organisational Security Policies

P.ACCOUNT Users will be held accountable for their actions within the TOE**.**

Assumptions

The TOE is dependent upon both technical IT and operational aspects of its environment.

TOE Assumptions

A.TOE.CONFIG The TOE is installed, configured, and managed in accordance with its evaluated configuration described in [ECD].

Note that, as stated in OE.INSTALL, [ECD] defines the evaluated configuration in detail. It states requirements for the installation and configuration of the underlying system, describes how to install the TOE from its issue media and specifies actions that must be taken by the administrator to ensure the security of the evaluated configuration. Examples of such actions are the setting of restrictive permissions on operating system files and the generation of strong passwords and their secure communication to users.

Underlying System Assumptions

A.PHYSICAL The security-critical parts of the TOE and the underlying system (including processing resources and network services) are located within controlled access facilities which prevent unauthorized physical access.

A.SYS.CONFIG The underlying system (operating system and/or secure network services) is installed, configured, and managed in accordance with its secure configuration documentation.

A.ACCESS The underlying system is configured such that only the approved group of system users may obtain access to the system.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the underlying system and the security of the information it contains who can be trusted not to abuse their privileges.

A.PEER Any other IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.

CHAPTER

4 Security Objectives

This chapter describes the IT security objectives for the TOE and the IT and non-IT security objectives for the TOE's operational environment that are needed to support the TOE IT objectives.

TOE Security Objectives

This section defines the IT security objectives that are to be satisfied by the TOE in combination with the IT security environment. Table 5 in chapter 8 correlates the TOE security objectives to each of the threats and security policies, showing that each threat is countered by at least one IT security objective, and that each security policy is satisfied by at least one IT security objective.

O.ACCESS The TOE must prevent unauthorized access to resources protected by OAM, TOE security attributes and OID audit data.

O.I&A The TOE must provide the means of identifying and authenticating users of the TOE. Users who do not identify themselves are to be given sessions with the TOE that only allow access to IT assets that are authorized for access by anonymous users.

O.AUDIT.GEN The TOE must provide the means of generating records of security relevant events in sufficient detail to help an administrator of the TOE to:

a) detect attempted security violations, or potential misconfiguration of the TOE security features that would leave the directory open to compromise; *and*

b) hold individual directory users accountable for any actions they perform that are relevant to the security of the directory.

O.AUDIT.RECORD The TOE must provide the means of storing and maintaining records of security relevant events generated by OID.

O.ADMIN The TOE, where necessary in conjunction with the underlying system, must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators can access such functionality.

Environmental Security Objectives

The following IT security objectives are to be satisfied by the environment in which the TOE is used.

OE.ADMIN The underlying system must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators can access such functionality. In particular, to enable the effective management of the TOE's audit functions the underlying operating system's functions must include the provision of reliable timestamps for use in audit records.

OE.AUDIT.SYSTEM The underlying system must maintain a protected audit trail for OAM and OVD so that administrators can use it to detect and investigate security incidents.

OE.FILES The underlying system must provide access control mechanisms by which all of the TOE related files (including executables, run-time libraries, database files, export files, redo log files, control files, audit files, trace files and dump files) and directory related database tables may be protected from unauthorized access.

OE.SEP The underlying operating system must provide the means to isolate the TOE Security Functions (TSF) and assure that the TSF components cannot be tampered with.

The following non-IT security objectives are to be satisfied by procedural and other measures taken within the TOE environment.

OE.INSTALL Those responsible for the TOE must ensure that:

a) The TOE is delivered, installed, managed and operated in accordance with the operational documentation of the TOE, and in particular its evaluated configuration as defined in [ECD], and

b) The underlying system is installed and operated in accordance with its operational documentation. If the system components are certified under the Common Criteria they should be installed and operated in accordance with the appropriate certification documentation.

Note that [ECD] defines the evaluated configuration of the TOE in detail. It states requirements for the installation and configuration of the underlying system, describes how to install the TOE from its issue media and specifies actions that must be taken by the administrator to ensure the security of the evaluated configuration. Such specified actions may emphasise items already documented in the TOE's administrator guidance documentation or may provide additional instructions to avoid potential security problems that relate to the evaluated configuration.

OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE that are critical to the security policy are protected from physical attack.

OE.AUDITLOG Administrators must ensure that audit facilities are used and managed effectively. These procedures shall apply to the TOE's audit trail and the audit trail for the underlying operating system and the database servers and/or secure network services. In particular:

a) Appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space;

b) Audit logs must be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future;

c) The system clocks must be protected from unauthorized modification (so that the integrity of audit timestamps is not compromised).

OE.RECOVERY Those responsible for the TOE must ensure that procedures are in place to ensure that, after system failure or other discontinuity, recovery without security compromise is obtained.

OE.TRUST Those responsible for the TOE must ensure that only users, who can be trusted to perform administrative duties with integrity, have privileges which allow them to:

a) set or alter the configuration directives affecting audit record generation by the TOE;

b) set or alter the configuration of the audit trail maintenance system;

c) modify the contents of the audit trail;

d) create any user account or modify any security attributes of users other than themselves;

e) set or alter security attributes that affect the ability of users other than themselves to access resources; or

f) set administrative permissions on files.

Note that one user would not normally simultaneously hold all of these privileges. Thus an audit administrator would normally be given the privileges for items a), b) and c) while a system administrator would be given the privileges for d) e) and f).

OE.AUTHDATA Those responsible for the TOE must ensure that the authentication data for each user account for the TOE and for each user account for the underlying system is held securely and not disclosed to persons not authorized to use that account. In particular:

a) The media on which the authentication data for the underlying operating system is stored shall not be physically removable from the underlying platform by unauthorized users;

b) Users shall not disclose their passwords to other individuals;

c) Passwords generated by the system administrator shall be distributed in a secure manner;

d) The network of computers that includes the TOE will be installed and maintained as specified in [ECD] so that unencrypted passwords being transmitted through this network cannot be captured by malicious software or hardware and passed to users.

OE.MEDIA Those responsible for the TOE must ensure that the confidentiality, integrity and availabilty of IT assets held on storage media is adequately protected. In particular:

a) The on-line and off-line storage media on which IT assets and security related data (such as operating system backups, database backups and transaction logs, and audit trails) must not be physically removable from the underlying platform by unauthorized users;

b) The on-line and off-line storage media must be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related-data;

c) The media on which TOE-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-directory purpose.

Table 6 in chapter 8 illustrates how each of the above objectives counters a threat, supports a policy, or maps to a secure usage assumption.

CHAPTER

5 IT Security Requirements

TOE Security Functional Requirements

Table 1 below lists the Security Functional Requirements (SFRs) for the TOE included in this Security Target. These TOE SFRs are listed in the order in which they are covered in this chapter and the table gives the section headings of the logical groupings of SFRs. This table identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have been applied to each requirement relative to Part 2 of [CC]. The text for such completed operations is highlighted with *ITALICISED CAPITAL LETTERS* within each requirement. SFRs that are extended relative to Part 2 of [CC] are indicated by adding the letter "T" after the component identifier.

The remainder of this section details the TOE SFRs for this Security Target. The functional requirements for the IT Environment to support the TOE SFRs are given in the section below entitled "Support for SFRs". Annex B provides definitions for various terms used in the functional requirements. Note that the phrase "suitably authorized users", which is used in the SFRs listed below, refers to users who are permitted by the Directory Access Control SFP to perform the operation in question.

Table 1: List of Security Functional Requirements

Element	Name	A	S	R	I
	SFRs under the heading "Identification and Authentication":				
FIA_AFL.1.1	Authentication Failure Handling	X			
FIA_AFL.1.2	Authentication Failure Handling	X			
FIA_ATD.1.1	User Attribute Definition	X			
FIA_SOS.1.1	Verification of Secrets	X			

Element	Name	A	S	R	I
FIA_UAU.1.1	Timing of Authentication	X			
FIA_UAU.1.2	Timing of Authentication				
FIA_UAU.6.1	Re-authenticating	X			
FIA_UID.1.1	Timing of Identification	X			
FIA_UID.1.2	Timing of Identification				
FIA_USB.1.1	User-subject Binding	X			
FIA_USB.1.2	User-subject Binding	X			
FIA_USB.1.3	User-subject Binding	X			
	SFRs under the heading “Resource Access Control SFP”:				
FDP_ACC.1.1	Subset Access Control	X			
FDP_ACF.1.1	Security Attribute Based Access Control	X			
FDP_ACF.1.2	Security Attribute Based Access Control	X			
FDP_ACF.1.3	Security Attribute Based Access Control	X			
FDP_ACF.1.4	Security Attribute Based Access Control	X			
	SFRs under the heading “Security Management”:				
FMT_MSA.1.1	Management of Security Attributes	X	X		
FMT_MSA.3.1	Static Attribute Initialisation	X	X		
FMT_MSA.3.2	Static Attribute Initialisation	X			
FMT_MTD.1.1	Management of TSF Data	X	X		
FMT_REV.1.1	Revocation	X	X		
FMT_REV.1.2	Revocation	X			
FMT_SMF.1.1	Specification of Management Functions	X			
FMT_SMR.1.1	Security Roles	X			
FMT_SMR.1.2	Security Roles				
	SFRs under the heading “Protection of the TSF”:				
FPT_RVM.1.1	Non-Bypassability of the TSP				
	SFRs under the heading “TOE Access”:				
FTA_TSE.1.1	TOE Session Establishment	X			
	SFRs under the heading “Security Audit”:				
FAU_GEN.1T.1	Audit Data Generation	X	X		

Element	Name	A	S	R	I
FAU_GEN.1T.2	Audit Data Generation	X			
FAU_GEN.2.1	User Identity Association				
FAU_SAR.1T.1	Audit Review	X		X	
FAU_SAR.1T.2	Audit Review			X	
FAU_SAR.3T.1	Selectable Audit Review	X	X		
FAU_STG.1T.1	Protected Audit Trail Storage			X	
FAU_STG.1T.2	Protected Audit Trail Storage		X	X	

Identification and Authentication

The TOE SFRs under class FIA in this Security Target relate to the identification and authentication of users when the Resource Access Control SFP has been invoked to control access by users to resources via HTTP requests sent over the network to the web server hosting the TOE's WebGate software. In addition, some FIA SFRs are used to cover the rules for the association of user security attributes with subjects acting on behalf of a user.

FIA_AFL.1.1 The TSF shall detect when *AN ADMINISTRATOR CONFIGURABLE POSITIVE INTEGER WITHIN THE RANGE 1 TO 999,999,999* unsuccessful authentication attempts occur related to *CONSECUTIVE INSTANCES OF A USER ATTEMPTING TO AUTHENTICATE THEMSELVES WITHIN AN ADMINISTRATOR CONFIGURABLE PERIOD OF TIME*.

Note that an administrator can set the maximum number of unsuccessful authentication attempts to be any positive integer up to 999,999,999, but [ECD] defines a specific value to be used in the TOE's evaluated configuration..

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *LOCK THE USER'S ACCOUNT*.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) *USER IDENTIFIER;*
b) *AUTHENTICATION DATA;*
c) *ROLES;*
d) *GROUP MEMBERSHIPS.*

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet *REUSE, LIFETIME, AND CONTENT METRICS AS DEFINED BY A SUITABLY AUTHORIZED ADMINISTRATOR*.

FIA_UAU.1.1 The TSF shall allow *ACCESS TO MATERIAL AUTHORIZED FOR ACCESS BY THE ANONYMOUS USER* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions

a) *THE ADMINISTRATOR CONFIGURABLE MAXIMUM SESSION TIME HAS BEEN EXCEEDED;*
b) *THE ADMINISTRATOR CONFIGURABLE MAXIMUM SESSION INACTIVITY PERIOD HAS BEEN EXCEEDED*.

FIA_UID.1.1 The TSF shall allow *ACCESS TO MATERIAL AUTHORIZED FOR ACCESS BY THE ANONYMOUS USER* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:

a) *IP ADDRESS OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS THE RESOURCE;*
b) *USER IDENTIFIER;*
c) *ROLES HELD BY THE USER;*
d) *GROUP MEMBERSHIPS HELD BY THE USER;*
e) *USER AUTHENTICATION DATA.*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users:

a) *AT THE START OF A SESSION WITH THE TSF, THE IP ADDRESS OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS THE RESOURCE IS ASSOCIATED WITH EACH SUBJECT ACTING ON BEHALF OF THE USER;*
b) *IF THE FORM-BASED AUTHENTICATION SCHEME IS CONFIGURED FOR THE POLICY PROTECTING THE RESOURCE THAT THE USER IS REQUESTING TO ACCESS, THEN, PROVIDED THAT THE USER IS A VALID USER FOR THE RESOURCE, THE USER IDENTIFIER WILL BE ASSOCIATED WITH EACH SUBJECT ACTING ON BEHALF OF THAT USER;*
c) *IF RULE b) APPLIES, THEN THE AUTHENTICATION DATA FOR THE USER AND ANY ROLES AND GROUP MEMBERSHIPS HELD BY THE USER WILL BE ACCESSIBLE TO EACH SUBJECT THAT IS RESPONSIBLE FOR CHECKING THE AUTHENTICATION AND AUTHORIZATION OF THE USER TO ACCESS THE RESOURCE.*
d) *IF THE ANONYMOUS AUTHENTICATION SCHEME IS CONFIGURED FOR THE POLICY PROTECTING THE RESOURCE THAT THE USER IS REQUESTING TO ACCESS, THEN THE USER IDENTIFIER FOR THE ANONYMOUS USER WILL BE ASSOCIATED WITH EACH SUBJECT ACTING ON BEHALF OF THAT USER;*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users:

a) *ONCE THE VALUE OF A PARTICULAR SECURITY ATTRIBUTE HAS BEEN ASSOCIATED WITH A SUBJECT ACTING ON BEHALF OF A USER, THIS VALUE MAY BE USED FOR THE SECURITY ATTRIBUTE FOR THE*

REMAINDER OF THE SESSION WITH THE TSF EVEN IF THE STORED VALUE OF THE ATTRIBUTE HAS BEEN CHANGED OR DELETED.

Resource Access Control SFP

The TOE SFRs in this section relate to the Resource Access Control Security Function Policy. This SFP controls access by users to resources via HTTP requests sent over the network to the web server hosting the TOE's WebGate software.

FDP_ACC.1.1 The TSF shall enforce the *RESOURCE ACCESS CONTROL SFP* on:

a) *USERS*;
b) *RESOURCES; AND*
c) *OPERATIONS PROVIDING THE TYPES OF ACCESS IN THE FOLLOWING LIST:*
GET
POST
PUT
TRACE
HEAD
CONNECT
OPTIONS.

FDP_ACF.1.1 The TSF shall enforce the *RESOURCE ACCESS CONTROL SFP* to objects based on the following:

a) *THE IP ADDRESS OF THE COMPUTER ORIGINATING THE USER'S REQUEST TO ACCESS THE RESOURCE,*
THE TIME AT WHICH THE USER REQUESTED TO ACCESS THE RESOURCE,
THE USER IDENTIFIER, ROLES AND GROUP MEMBERSHIPS ASSOCIATED WITH THE USER; AND
b) *THE URL AND POLICY OR POLICY DOMAIN THAT APPLY TO THE RESOURCE THE USER IS REQUESTING TO ACCESS.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *THE AUTHORIZATION RULES DEFINED IN THE POLICY OR POLICY DOMAIN THAT APPLY TO THE RESOURCE THE USER IS REQUESTING TO ACCESS.*

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *NONE.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *NONE*.

Security Management

The TOE SFRs in this section relate to the general requirements for the TSF to manage the security attributes, TSF data and security management roles that are under its control. The TOE uses LDAP directories, which are accessed via its OID and OVD software, to hold its security attributes.

Please note that "security management role" is a Common Criteria term for which SFR FMT_SMR.1 is used to state requirements for the security management roles that are to be used for the TSF, whereas the TSF's term "role" refers to a way of grouping users according to their organisational roles.

FMT_MSA.1.1 The TSF shall enforce the *DIRECTORY ACCESS CONTROL SFP* to restrict the ability to QUERY, *MODIFY, DELETE, CREATE* the security attributes
USER IDENTIFIER, ROLES, GROUP MEMBERSHIPS AND AUTHENTICATION DATA FOR USERS, AND
THE URL AND POLICY OR POLICY DOMAIN FOR RESOURCES
to *SUITABLY AUTHORIZED USERS.*

FMT_MSA.3.1 The TSF shall enforce the *DIRECTORY ACCESS CONTROL SFP* to provide *RESTRICTIVE* default values for security attributes that are used to enforce the SFP.

Note that Section H.2 of Part 2 of [CC] states that FMT_MSA.3.1 applies only to security attributes for objects (which are the URL and policy or policy domain).

FMT_MSA.3.2 The TSF shall allow *SUITABLY AUTHORIZED ADMINISTRATORS* to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1.1 The TSF shall restrict the ability to *QUERY, CLEAR* the *OID AUDIT TRAIL* to *SUITABLY AUTHORIZED ADMINISTRATORS.*

Note that the TSF is only responsible for the management of the OID part of the TSF's audit trail. The IT environment is responsible for the management of the OAM audit trail and the OVD audit trail (as stated in FMT_MTD.1E).

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the *USERS AND OBJECTS* within the TSC to *SUITABLY AUTHORIZED USERS*.

FMT_REV.1.2 The TSF shall enforce the rules:

a) *THE REVOCATION OF A USER'S SECURITY ATTRIBUTES SHALL BE IN EFFECT WHEN THE USER NEXT REQUESTS A SESSION WITH THE TSF;*

b) *THE REVOCATION OF AN OBJECT'S SECURITY ATTRIBUTES SHALL BE IN EFFECT IN SUBSEQUENT SESSIONS WITH THE TSF WHEN A USER ACCESSES THE OBJECT*.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a) *QUERY, CLEAR* the *OID AUDIT TRAIL;*

b) *MODIFY, DELETE, CREATE the SECURITY ATTRIBUTES.*

Note that SFR FMT_MSA.1.1 defines the SECURITY ATTRIBUTES.

FMT_SMR.1.1 The TSF shall maintain the roles:

a) *AUTHORIZED ADMINISTRATOR*;
b) *USER*.

Note that an authorised administrator is a user with the necessary privileges and permissions to perform their administrative duties.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Note that SFR FMT_SMR.1 relates to the roles used in performing the security management functions listed in SFR FMT_SMF.1.1.

Protection of the TOE Security Functions

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

TOE Access

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on *TIME OF ACCESS*.

Security Audit

The TOE SFRs under class FAU in this Security Target relate to the generation of audit data for security relevant TOE events,and the protection and review of audit data generated by OID.

FAU_GEN.1T.1 The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events *AS IDENTIFIED IN TABLE 2 BELOW*.

*Note that the FAU_GEN.1.1 element defined in Section 8.2 of [CC] Part 2 requires that the TSF shall be able to generate an audit record for the start-up and shutdown of the audit functions. Since the TOE does not do this, this SFR has been explicitly stated and the selection operation for the FAU_GEN.1.1 element defined in Section 8.2 of [CC] Part 2 has effectively been completed with "*for the *NOT SPECIFIED* level of audit*". A refinement has been applied to omit these words for the sake of clarity.*

Table 2: Required Auditable Events

Component	Event	Additional Data
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	Object identifier, requested access
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state	None
FIA_SOS.1	Rejection by the TSF of any tested secret	None
FIA_UAU.1	Unsuccessful use of the authentication mechanism	None
FIA_UAU.6	Failure of reauthentication	None
FIA_UID.1	Unsuccessful use of the user identification mechanism	None
FMT_MSA.1	All modifications of the values of security attributes	None
FMT_MSA.3	All modifications of the initial values of security attributes	None
FMT_REV.1	Unsuccessful revocation of security attributes	Security attribute
FMT_SMF.1	Specification of Security Management Functions.	None
FMT_SMR.1	Modifications to the group of users that are part of a role	None

Table 2: Required Auditable Events

Component	Event	Additional Data
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	None

FAU_GEN.1T.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the *SECURITY TARGET AND OTHER AUDIT RELEVANT INFORMATION AS IDENTIFIED IN TABLE 2 ABOVE*.

Note that FAU_GEN.1T.2 is as per FAU_GEN.1.2 defined in section 8.2 of [CC] Part 2.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1T.1 The TSF shall provide *SUITABLY AUTHORIZED ADMINISTRATORS* with the capability to read *ALL AUDIT INFORMATION* from the audit records *GENERATED BY OID*.

FAU_SAR.1T.2 The TSF shall provide the audit records *GENERATED BY OID* in a manner suitable for the user to interpret the information.

FAU_SAR.3T.1 The TSF shall provide the ability to perform *SEARCHES* of audit data *GENERATED BY OID* based on *A FUNCTION OF ONE OR MORE ATTRIBUTE VALUES IN THE AUDIT RECORD*.

FAU_STG.1T.1 The TSF shall protect the stored audit records *GENERATED BY OID* from unauthorized deletion.

FAU_STG.1T.2 The TSF shall be able to *PREVENT* unauthorized modifications to the stored audit records *GENERATED BY OID* in the audit trail.

TOE Security Assurance Requirements

The target assurance level is EAL4 as defined in Part 3 of the CC, augmented with ALC_FLR.3.

Security Requirements for the IT Environment

The TOE is a resource access control system that uses LDAP directories to hold its security credentials. The TOE is built on top of an underlying IT platform. This IT platform, which consists of an operating system, network services and other supporting software (collectively referred to as the *system*) is required to provide controlled access services to ensure the secure operation of the TOE as follows:

- The operating system and database server shall identify and authenticate users prior to providing access to the underlying system.

- The operating system shall provide the discretionary access control mechanisms required to support the TOE and the IT environment in ensuring files can only be accessed by authorized users.
- The operating system shall provide an auditing system to support the TOE and the IT environment by ensuring users can be held accountable for their access to IT assets other than via access requests submitted to OAM.
- The system shall provide backup, restore and other secure recovery mechanisms. Such mechanisms are to be capable of archiving and restoring the TOE's audit trail.

Note that an operating system meeting the functional and assurance requirements defined in [CAPP], or equivalent, will meet the above requirements (although conformance to [CAPP] is not a mandatory requirement).

Support for SFRs

The specific functional requirements for the IT Environment that are needed to support the secure functioning of the TOE SFRs defined earlier in this chapter are listed in Table 3. The IT environment SFRs in Table 3 are listed in the order in which they are covered in this chapter and the table gives the section headings of the logical groupings of SFRs. This table identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have been applied to the requirement relative to Part 2 of [CC]. The text for such completed operations is highlighted with *ITALICISED CAPITAL LETTERS* within each requirement.

All of the elements covered in this section have been refined relative to Part 2 of [CC] so that the elements apply to the IT Environment rather than the TOE. Such elements have been distinguished from the SFRs that apply to the TOE by adding the letter "E" after the component identifier.

After Table 3, the remainder of this section gives the details of the SFRs for the IT Environment and indicates the purpose of these SFRs.

Table 3: List of Security Functional Requirements for the IT Environment

Element	Name	A	S	R	I
	SFRs under the heading "Security Management":				
FMT_MTD.1E.1	Management of TSF Data	X	X	X	X
FMT_SMF.1E.1	Specification of Management Functions	X		X	
	SFRs under the heading "Protection of the TSF":				
FPT_SEP.1E.1	TSF Domain Separation			X	
FPT_SEP.1E.2	TSF Domain Separation			X	
FPT_STM.1E.1	Reliable Time Stamps			X	
	SFRs under the heading "Security Audit":				
FAU_SAR.1E.1	Audit Review	X		X	

Element	Name	A	S	R	I
FAU_SAR.1E.2	Audit Review			X	
FAU_SAR.3E.1	Selectable Audit Review	X	X	X	
FAU_STG.1E.1	Protected Audit Trail Storage			X	
FAU_STG.1E.2	Protected Audit Trail Storage		X	X	

Security Management

The TOE SFRs under class FMT in this Security Target relate to the general requirements for the TSF to manage the security attributes, TSF data and security management roles that are under its control. As the IT Environment manages the part of the audit trail that holds the audit records generated by OAM and OVD, this section is used to define the requirements for the IT Environment to manage the TSF data that are under its control.

FMT_MTD.1E.1.1 The *IT ENVIRONMENT* shall restrict the ability to *QUERY, CLEAR* the *OAM AUDIT TRAIL* to *SUITABLY AUTHORIZED ADMINISTRATORS.*

FMT_MTD.1E.1.2 The *IT ENVIRONMENT* shall restrict the ability to *QUERY, CLEAR* the *OVD AUDIT TRAIL* to *SUITABLY AUTHORIZED ADMINISTRATORS.*

Note that FMT_MTD.1.1, FMT_MTD.1E.1.1 and FMT_MTD.1E.1.2 together define the requirements for the management of TSF data.

FMT_SMF.1E.1 The *IT ENVIRONMENT* shall be capable of performing the following security management function:

a) *QUERY, CLEAR* the *OAM AUDIT TRAIL.*

b) *QUERY, CLEAR* the *OVD AUDIT TRAIL.*

Note that FMT_SMF.1.1, and FMT_SMF.1E.1 together define the requirements for the security management functions.

Protection of the TSF

The SFRs for the IT environment under class FPT cover requirements for the protection of the TSF and the provision of reliable time stamps for use in audit records.

FPT_SEP.1E.1 The *IT ENVIRONMENT* shall maintain a security domain *FOR THE TSC* that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1E.2 The *IT ENVIRONMENT* shall enforce separation between the security domains of subjects in the TSC *AND THE SECURITY DOMAINS OF UNTRUSTED APPLICATIONS.*

FPT_STM.1E.1 The *IT ENVIRONMENT* shall be able to provide reliable time stamps for *USE BY THE TSF.*

Note that FPT_STM.1.1 satisfies the dependency of the SFR FAU_GEN.1T for the provision of reliable time stamps.

Security Audit

The TOE SFRs under class FAU in this Security Target relate to the generation of audit data for security relevant TOE events,and the protection and review of audit data generated by OID. The SFRs for the IT environment in this section cover the capability to protect and review the audit data generated into the audit trail by OAM and OVD.

FAU_SAR.1E.1 The *IT ENVIRONMENT* shall provide *SUITABLY AUTHORIZED ADMINISTRATORS* with the capability to read *ALL AUDIT INFORMATION* from the audit records *GENERATED BY OAM AND OVD*.

FAU_SAR.1E.2 The *IT ENVIRONMENT* shall provide the audit records *GENERATED BY OAM AND OVD* in a manner suitable for the user to interpret the information.

Note that FAU_SAR.1T.1, FAU_SAR.1E.1, FAU_SAR.1T.2 and FAU_SAR.1E.2 together define the requirements for audit review.

FAU_SAR.3E.1 The *IT ENVIRONMENT* shall provide the ability to perform *SEARCHES* of audit data *GENERATED BY OAM AND OVD* based on *THE VALUES OF AUDIT DATA ATTRIBUTES*.

Note that FAU_SAR.3T.1 and FAU_SAR.3E.1 together define the requirements for selectable audit review.

FAU_STG.1E.1 The *IT ENVIRONMENT* shall protect the stored audit records *GENERATED BY OAM AND OVD* from unauthorized deletion.

FAU_STG.1E.2 The *IT ENVIRONMENT* shall be able to *PREVENT* unauthorized modifications to the stored audit records *GENERATED BY OAM AND OVD* in the audit trail.

Note that FAU_STG.1T.1, FAU_STG.1E.1, FAU_STG.1T.2 and FAU_STG.1E.2 together define the requirements for protecting audit trail storage.

Minimum Strength of Function

The minimum strength of function for the TOE is *SOF-High*.

This Page Intentionally Blank

CHAPTER

6 TOE Summary Specification

TOE Security Functionality

This section contains a high-level specification of each Security Function (SF) of the TOE that contributes to satisfaction of the Security Functional Requirements of chapter 5. The specifications cover four major areas: user identification and authentication, security attributes, resource access control and auditing.

For the TOE's evaluated configuration, the security attributes are held as follows:

- security attributes used for the identification and authentication of TOE users are held in data sources accessed via Oracle Virtual Directory (OVD);
- security attributes used for the authorization of TOE users to access resources protected by Oracle Access Manager are held using Oracle Internet Directory (OID).

Most of the SFs described in this section are implemented in Oracle Access Manager (OAM), although many of the Oracle Internet Directory SFs in [OIDST, 6] are also in the TOE and hence have been included in this section. Finally, the SFs in this section that concern access to security attributes used for the identification and authentication of TOE users are wholly or partly implemented in OVD.

User Identification and Authentication

UIA.AUTH If a user requests access to a resource protected by the TOE and

a) the resource is protected by a Policy configured to use the Form-based authentication scheme; and

b) the ObSSOCookie does not exist in the user's HTTP request
or the value of the ObSSOCookie indicates that the user is logged out

or the authentication scheme is at a level higher than the authentication level recorded in theObSSOCookie;

then if:

c) the user provides a valid user identifier; and

d) the user provides the password corresponding to the stored password for that user; and

e) if the password has expired as per SF UIA.PWDC a) then the user successfully supplies a new password conforming to SF SA.CHPWD; and

f) the user's account is not locked

the TOE will create a session with the TOE, for which the session will have recorded with it the IP address of the computer the user is using, and the TOE will create the ObSSOCookie and return it in the HTTP response.

Note that SF UIA.PWDC covers the conditions under which a user's account can be locked. In particular, if check d) fails, then IA.PWDC b) and c) specify the condition under which the user's account may consequently be locked. Note also that the TOE performs the checks to implement UIA.AUTH c) to f) by attempting to make a connection to OVD using the identifier and password provided.by the user.

UIA.ASESS If a user requests access to a resource protected by the TOE and

a) the resource is protected by a Policy configured to use the Anonymous authentication scheme; and

b) the ObSSOCookie does not exist in the user's HTTP request
or the value of the ObSSOCookie indicates that the user is logged out
or the authentication scheme is at a level higher than the authentication level recorded in theObSSOCookie

the TOE will create a session with the TOE in which only material authorized for access by the anonymous user is accessible, for which the session will have recorded with it the IP address of the computer the user is using, and the TOE will create the ObSSOCookie and return it in the HTTP response.

Note that the TOE provides authentication schemes in addition to the Anonymous authentication scheme and the Form-based scheme, but these additional schemes are not within the scope of the evaluation. [OAMAG, 5] describes how to configure authentication schemes via the use of the Access Manager Console outside of the TOE's operational state.

UIA.AUTHC If a user requests access to a resource protected by the TOE and

a) the ObSSOCookie exists in the user's HTTP request; and

b) its value does not indicate that the user is logged out; and

c) the authentication scheme configured for the Policy protecting the resource is at a level no higher than the authentication level recorded in theObSSOCookie; and

d) the user has a current session with the TOE that has not been terminated

the user is given access to the resource in this session provided that the user is not denied access by the Resource Access Control Policy defined in SF RAC.POL.

Note that the ObSSOCookie, which is generated by the Access Server, is used to determine whether the user has already been authenticated within the current session with the TOE. This feature can be used to provide single sign-on capability.

UIA.REAUTH If the TOE has created a session for a user to access a resource protected by the TOE and that resource is protected by a Policy configured to use the Form-based authentication scheme then, if:

a) the session has been in existance for longer than the maximum length configured by the administrator; or

b) the session has been inactive for longer than the maximum inactivity period configured by the administrator; or

c) the session has been logged out via a Logout URL

the TOE will terminate the current session and will require the user to authenticate again as per SF UIA.AUTH or SF UIA.ASESS before the user can start a new session with the TOE.

Note that configuring session timeout is described in [OAMAG, 7: Configuring the WebGates] and configuring a Logout URL is described in [OAMAG, 2: Configuring a Single Sign-On Logout URL].

UIA.PWDC Password policies can be configured to apply to users that request access to resources protected by the TOE. The following restrictions on the use of a password are held in a password policy and are acted on by the TOE as per SF UIA.AUTH:

a) the number of days for which the password is valid;

b) the number of consecutive failed attempts to enter a user password correctly before the user account becomes locked;

c) the lockout interval for which a user account remains locked after a user exceeds the maximum number of consecutive failed attempts to enter the user's password within the lockout interval.

Note that the TOE provides more configurable controls on user passwords than are listed in the above SF and in SF SA.CHPWD, but these additional controls are not within the scope of the evaluation. [OAMICAG, 7: Configuring Password Policies] defines the full set of such controls. These controls are configured by administrators via the use of the Access Manager Console outside of the TOE's operational state.

Resource Access Control

RAC.SUA The TOE enforces the Resource Access Control Policy defined in RAC.POL on a TOE user based on the following:

a) the user security attributes defined in SF SA.UATT;

b) the IP address of the computer the user is using to access the resource; and

c) the time at which access is requested.

RAC.OBA The TOE enforces the Resource Access Control Policy defined in RAC.POL on each resource based on its security attributes defined in SF SA.ATT.

RAC.POL When a TOE user attempts to access a resource protected by the TOE, the TOE grants such access according to the set of authorization rules defined in the policy or policy domain that applies to the resource.

Note that an authorization rule specifies information that identifies which users can access a resource it protects and which users are denied access to the resource. One or more authorization rules are included in an authorization expression for a policy domain or policy. Policy domains and policies are configured for resources by administrators via the use of Policy Manager outside of the TOE's operational state. [OAMAG, 4: Configuring Resource Types] and [OAMAG, 6: Authorization Rules] describe the configuring of policies, policy domains and authorization rules.

Security Attributes

SA.ATT The security attributes of a resource are:

a) its URL; and

b) the policy domain or policy that applies to the resource.

Note that a policy is the set of authentication, authorization and auditing rules that apply to one or more resource types within a policy domain. In the absence of a policy for a specific resource type, the default rules for all resource types in the policy domain apply.

SA.UATT Each user has a user entry that holds the user's security attributes. Each user entry is uniquely identified by its distinguished name (DN). The security attributes for a user requesting access to a resource are:

a) user identifier;

b) password;

c) roles held by the user; and

d) group memberships.

Note that the user identifier mentioned in the above SF is mapped to the DN for the user entry as described in [OAMAG, 5: Credential Mapping Plug-In].

UIA.OVDUID Each user whose security attributes are held via OVD can be uniquely identified via the distinguished name (DN) of the user's entry. There is a special user, called the super user, whose name and password are held in OVD's configuration files. The super user is the administrative user for OVD and is not subject to any access controls.

SA.ACC Access via OVD to user security attributes held by data sources is controlled according to the access control information stored in the relevant OVD configuration file.

Note that OVD access control is configured by administrators by editing the file acls.os_xml or by using the Oracle Virtual Directory Manager server editor outside of the TOE's operational state. Further details on the access control information that is held in this file are available in [OVDPM, 11: Oracle Virtual Directory Access Control] and [OVDPM, 11: Oracle Virtual Directory Access Control Configuration].

SA.CHPWD The TOE applies the following checks, which are held in the relevant password policy, when a user password is to be updated:

a) the minimum number of characters in the password;

b) the minimum number of upper-case characters in the password;

c) the minimum number of lower-case characters in the password;

d) the minimum number of non-alphanumeric characters in the password;

e) the minimum number of numeric characters in the password;

f) the minimum number of days the password must last before it can be changed;

g) if the password policy specifies password reuse constraints then the new password is compared against these constraints.

If any of these checks fail, then the TOE rejects the new password.

Note that Oracle Access Manager permits users to change their passwords, but SF SA.CHPWD only applies to the TOE in its operational state as per SF UIA.AUTH. Note also that the TOE provides more configurable controls on user passwords than are listed in the above SF and in SF UIA.PWDC, but these additional controls are not within the scope of the evaluation. [OAMICAG, 7: Configuring Password Policies] defines the full set of such controls. These controls are configured by administrators via the use of the Access Manager Console outside of the TOE's operational state.

SA.UEFF At the start of a user's session with the TOE, the values of the user security attributes defined in SF SA.UATT are associated with the session. Changing the value of a user attribute or deleting a user entry will not affect the values of the user security attributes associated with the user's session until the caches holding the attributes have been flushed. In the evaluated configuration for the TOE, such caches time out and are flushed automatically after time periods configured by the administrator.

Note that caching is described in [OAMDEP, 4: Caching Access System Information] and instructions for the administrator in setting cache timeouts are given in [ECD, 4.1].

SA.OEFF When a resource is accessed during a user's session with the TOE, the values of the object security attributes for the resource that are defined in SF SA.ATT are associated with the session. Changing the value of an object attribute or removing a resource from the protection of the TOE will not affect the values of the resource's security attributes associated with the user's session until the caches holding the attributes have been flushed.

Note that caching is described in [OAMDEP, 4: Caching Access System Information] and instructions for the administrator to ensure any necessary cache updates take place when object security attributes are updated are given in [ECD, 4.1].

OID SFs for Security Attributes

The Oracle Internet Directory SFs in this section (which are also described in chapter 6 of [OIDST]) are in the TOE to cover access to security attributes held in an OID directory. These SFs supply functionality for the creation, access and modification of directory entries holding TOE security attributes that relate to policy domains and policies.

IA.UID Each directory user is uniquely identified via the distinguished name (DN) of the user's directory entry. The exception to this is that there are three special users: the super user, the guest user and the proxy user, whose names are held in the root directory-specific entry. The super user is the administrative user for the directory.

IA.CRUG The TOE will allow only suitably authorized users to create user entries and group entries in the directory. The default values of attributes of such new directory entries are as described in Chapters 8, 11 and 13 of [OIDAG].

SAM.EATT The directory contains a set of security attributes for each directory entry. These define the Access Control Information related to the attributes for the entry and the entry itself. The default Access Control Information established when the TOE is installed is covered in the About the Default Configuration section of Chapter 21 of [OIDAG].

SAM.MODATT A user can create, read, modify or delete security attributes for directory users and directory entries only if authorised by the Directory Access Control Policy defined in DAC.POL.

DAC.POL When a directory user attempts to perform an operation on a directory object, access is either granted or denied according to a set of rules specified in [OIDAG, 18: How ACL Evaluation Works]. A user is always allowed to modify the `userpassword` attribute of that user's directory entry.

Audit and Accountability

AA.INF When the Master Audit Rule has been configured, for every occurrence of an auditable event described in Chapter 4 of [OAMAG], the TOE will write an audit record to the OAM audit log which holds at least the following information:

a) IP address of the machine requesting access;

b) date and time of the audit event;

c) the ID of the Access Server that is auditing the event;

d) the requested URL;

e) the HTTP operation (e.g. GET or POST);

f) a string corresponding to the event that occurred.
The event can be one of the following: Authentication Success, Authentication Failure, Authorization Success, or Authorization Failure;

g) the user's distinguished name, if the user was successfully authenticated;

h) information for authentication success, authentication failure, authorization success, and authorization failure events.

In addition, audit policies can be configured to record when a policy is modified.

Note that administrators can create, modify or delete the Master Audit Rule and can amend which types of event are auditable to the OAM audit log by using the Access Manager Console outside of the TOE's operational state. In addition, audit rules that affect the auditing of events can be used in policy domains and policies that are configured by administrators via the use of Policy Manager outside of the TOE's operational state.

AA.OVDINF When auditing to OVD's Access Log is enabled, for every occurrence of an auditable event in OVD associated with the SFs SA.ACC, UIA.AUTH and UIA.REAUTH, the TOE will write to the Access Log an audit record which holds at least the following information:

date and time of event; type of event; subject identity (which may be that of the anonymous user); and the outcome (success or failure) of the event.

OID SFs for Audit and Accountability

The Oracle Internet Directory SFs in this section (which are also described in chapter 6 of [OIDST]) are in the TOE to cover the auditing of OID's security events that are relevant to the management of TOE security attributes held in OID directories.

AUD.INF When the audit level is non-zero, for every occurrence of an auditable event described in Chapter 14 of [OIDAG], the TOE will write an audit record which holds the following information:

date and time of event; type of event; subject identity (which is null if the user is anonymous); and the outcome (success or failure) of the event.

In addition:

a) when the audit level is changed, the identity of the directory entry modified is recorded;

b) when a user attempts to access a directory object, the object identifier and the requested access operation is recorded (provided that the operation was unsuccessful or caused a change to the object); and

c) when a security attribute is modified, the attribute name is recorded.

AUD.ACC The TOE will allow only users authorized by the Directory Access Control Policy defined in DAC.POL to view all records in the audit log in a format suitable for the users to interpret the information. The TOE provides facilities to search for audit records based on a function of one or more attribute values in the records.

AUD.DEL The TOE will allow only authorized users to delete audit records from the audit log (such users are authorized by the system administrator, who will inform them of the OID password). No other modification to the audit records is permitted.

Note that the bulkdelete command line tool is used to delete audit records from the audit log. This tool requests the user to confirm that they are an authorized administrator by supplying the OID password (which is the password used when OID connects to the Oracle database that holds its directory data, see [OIMUR, 3: oidpasswd] and [OIMUR, 4: bulkdelete]).

Security Mechanisms and Techniques

A password is used for authentication of TOE users in the evaluated configuration (for which Form-based Authentication is mandatory). The TOE password management functions (together called the PWD mechanism), when combined with the instructions to administrators that will be included in [ECD] to choose strong passwords and to distribute them securely to users, provide a Strength of Function level of *SOF-high*.

Specific SFs supporting the claimed SOF are:

- UIA.AUTH (SOF-High); *and*
- UIA.PWDC, SA.UATT and SA.CHPWD, which support UIA.AUTH by providing password management facilities.

Assurance Measures

The target assurance level is EAL4 augmented with ALC_FLR.3. The following table indicates the documentation that will be supplied to support each security assurance requirement for EAL4 and also the assurance requirement for ALC_FLR.3. No other specific assurance measures are claimed.

Table 4: TOE Assurance Measures

Component	Name	Documents
ACM_AUT.1	Partial CM Automation	Document(s) describing the TOE's configuration management will be provided.
ACM_CAP.4	Generation Support and Acceptance Procs	Document(s) describing the TOE's configuration management will be provided.
ACM_SCP.2	Problem Tracking CM Coverage	Document(s) describing the TOE's configuration management will be provided.

Table 4: TOE Assurance Measures

Component	Name	Documents
ADO_DEL.2	Detection of Modification	Document(s) describing the TOE’s delivery procedures will be provided.
ADO_IGS.1	Installation, Generation, and Startup	Document(s) describing the TOE’s installation and configuration will be provided.
ADV_FSP.2	Fully Defined External Interfaces	Document(s) covering the TOE’s external interfaces will be provided.
ADV_HLD.2	Security Enforcing High-level Design	Document(s) describing the TOE’s high level design will be provided.
ADV_IMP.1	Subset of the TSF Implementation	All of the TOE’s source code will be provided.
ADV_LLD.1	Descriptive Low-level Design	Document(s) describing the TOE’s low level design will be provided.
ADV_RCR.1	Informal Correspondence Demonstration	A demonstration of correspondence will be provided within the design documentation.
ADV_SPM.1	Informal TOE Security Policy Model	A document describing the TOE’s Security Policy Model will be provided.
AGD_ADM.1	Administrator Guidance	Administrator guidance document(s) will be provided.
AGD_USR.1	User Guidance	User guidance document(s) will be provided.
ALC_DVS.1	Identification of Security Measures	Document(s) covering the security of the TOE’s development environment will be provided.
ALC_LCD.1	Developer Defined Life Cycle Model	Document(s) covering the TOE’s life cycle model will be provided.
ALC_TAT.1	Well Defined Development Tools	Document(s) covering the TOE’s development tools will be provided.
ATE_COV.2	Analysis of Coverage	Document(s) describing the TOE’s developer testing will be provided.
ATE_DPT.1	Testing - High-level Design	Document(s) describing the TOE’s developer testing will be provided.
ATE_FUN.1	Functional Testing	Document(s) describing the TOE’s developer testing will be provided.
AVA_MSU.2	Validation of Analysis	Document(s) providing guidance analysis for the TOE will be provided.
AVA_SOF.1	Strength of TOE Security Functions	Document(s) analysing the strength of the TOE security functions will be provided.
AVA_VLA.2	Independent Vulnerability Analysis	Document(s) providing vulnerability analysis for the TOE will be provided.
ALC_FLR.3	Systematic Flaw Remediation	Document(s) covering the flaw remediation procedures will be provided.

This Page Intentionally Blank

CHAPTER

7

Protection Profile Claims

PP Reference

The Security Target makes no claims about Protection Profile conformance.

This Page Intentionally Blank

CHAPTER

8 Rationale

Security Objectives Rationale

This section demonstrates how the identified security objectives are suitable to counter the identified threats and meet the stated security policies.

The threats for the TOE, the organisational security policies and the secure usage assumptions are stated in Chapter 3. The TOE security objectives and the environmental security objectives are stated in Chapter 4.

The table below covers those threats countered by the TOE and the security policies addressed by the TOE, showing that a threat is countered by at least one TOE security objective, and that each security policy is satisfied by at least one TOE security objective. This table does not cover threats addressed purely by the environment. A *YES* in the table indicates that the identified TOE security objective is relevant to the identified threat or security policy.

Table 5: Correlation of Threats and Policies to TOE Security Objectives

Threat/ Policy	O.I&A	O.ACCESS	O.AUDIT	O.ADMIN
T.DATA	YES	YES		YES
T.ACCESS	YES	YES		YES
T.ATTACK	YES	YES	YES	YES
T.ABUSE. USER	YES	YES	YES	YES
P.ACCOUNT	YES	YES	YES	YES

The following table illustrates how each of the environmental security objectives counters a threat, supports a policy or maps to a secure usage assumption.

Table 6: Mapping of Environmental Security Objectives to Threats, Policy, and Secure Usage Assumptions

Environmental Objective	Counters Threat	Supports Policy	Maps to Secure Usage Assumptions
OE.INSTALL	TE.OPERATE		A.TOE.CONFIG, A.SYS.CONFIG, A.MANAGE, A.ACCESS, A.PEER
OE.PHYSICAL			A.PEER, A.PHYSICAL
OE.AUDITLOG	T.ATTACK, T.ABUSE.USER	P.ACCOUNT	A.MANAGE
OE.RECOVERY	TE.CRASH		A.MANAGE
OE.TRUST	TE.ACCESS		A.MANAGE, A.ACCESS
OE.AUTHDATA	T.DATA, T.ACCESS		A.MANAGE, A.ACCESS
OE.MEDIA	TE.CRASH		A.MANAGE
OE.AUDIT.SYSTEM	T.ATTACK, T.ABUSE.USER	P.ACCOUNT	A.MANAGE
OE.ADMIN	T.DATA, T.ACCESS, T.ATTACK, T.ABUSE.USER,TE.ACCESS	P.ACCOUNT	A.MANAGE, A.ACCESS
OE.FILES	T.DATA, T.ACCESS, T.ATTACK, T.ABUSE.USER, TE.ACCESS	P.ACCOUNT	A.MANAGE
OE.SEP	T.DATA, T.ACCESS, T.ATTACK	P.ACCOUNT	A.MANAGE

T.DATA Rationale

T.DATA (*Unauthorized Access to Resources)* is directly countered by O.ACCESS, which ensures access to IT assets via the TOE is controlled. O.I&A gives support by providing the means of identifying the user attempting to access an IT asset so that access controls can be based on the user's identity (or the user's anonymity). O.ADMIN and OE.ADMIN provide support by ensuring that only authorized administrators can cause configuration files to be updated by TOE management functions and by the IT environment to affect the operation of access controls on resources. OE.FILES prevents unauthorized users gaining direct access to configuration files and files holding user security attributes to enable the circumvention of access controls on resources. OE.AUTHDATA ensures that user authentication data is held securely to stop it being used by users to masquerade as other users to gain unauthorized access to resources via the TOE. OE.SEP prevents TSF components being tampered with and ensures the isolation of user sessions that could otherwise result in unauthorized access to resources.

T.ACCESS Rationale

T.ACCESS (*Unauthorized Access to Security Attributes)* is directly countered by O.ACCESS, which ensures the TOE can protect the TOE security attributes from unauthorized access. O.I&A gives support by providing the means of identifying the user attempting to access an IT asset so that access controls can be based on the user's identity (or the user's anonymity). O.ADMIN and OE.ADMIN provide support by ensuring that only authorized administrators can cause configuration files to be updated by

TOE management functions and by the IT environment to affect the operation of access controls on security attributes. OE.FILES prevents unauthorized users gaining direct access to configuration files and files holding user security attributes to enable the circumvention of access controls on security attributes. OE.AUTHDATA ensures that user authentication data is held securely to stop it being used by users to masquerade as other users to gain unauthorized access to security attributes via the TOE. OE.SEP prevents TSF components being tampered with and ensures the isolation of user sessions that could otherwise result in unauthorized access to security attributes.

T.ATTACK Rationale

T.ATTACK (*Undetected Attack)* is countered directly by O.AUDIT.GEN, O.AUDIT.RECORD and OE.AUDIT.SYSTEM which ensure the TOE, with assistance from the IT environment, has the means of recording and investigating security relevant events which could be indicative of an attack aimed at defeating the TOE security features. O.I&A provides support by allowing audit records to include data identifying the user in a way which is appropriate to the resource being accessed. O.ACCESS and O.ADMIN provide support by controlling access to OID audit data and audit configuration data which only highly trusted individuals must be allowed to view and modify. OE.ADMIN ensures that the underlying operating system provides reliable timestamps for use in audit records. OE.FILES provides support by preventing users gaining direct access to files holding directory audit data to modify or remove evidence of an attack. OE.AUDITLOG ensures audit data is correctly managed by the administrator so that it can be used to detect attacks. OE.SEP prevents TSF components being tampered with and ensures the isolation of web user sessions that could otherwise result in attacks on TOE security features being undetected.

T.ABUSE.USER Rationale

T.ABUSE.USER (*Abuse of Privileges)* is countered directly by O.AUDIT.GEN, O.AUDIT.RECORD and OE.AUDIT.SYSTEM which ensure the TOE, with assistance from the IT environment, has the means of recording and investigating security relevant events which could be indicative of abuse of privilege by an authorized user of the directory. O.I&A provides support by reliably identifying the user responsible for particular events, thus ensuring that the user can be held accountable for actions for which he or she is responsible in a way which is appropriate to the resource being accessed. O.ACCESS and O.ADMIN provide support by controlling access to OID audit data and audit configuration data which only highly trusted individuals must be allowed to view and modify. OE.ADMIN ensures that the underlying operating system provides reliable timestamps for use in audit records. OE.FILES provides support by preventing users gaining direct access to files holding directory audit data to modify or remove evidence of an abuse of privilege.OE.AUDITLOG ensures audit data is correctly managed by the administrator so that it can be used to detect abuse of privilege.

TE.ACCESS Rationale

TE.ACCESS (*Unauthorized Access to IT Assets)* is directly countered by OE.FILES, which prevents unauthorized users gaining direct access to resource files, configuration files, files holding security attributes and audit trail files. OE.ADMIN provides support by ensuring that only authorized administrators can cause configuration files to be updated by the IT environment to affect the operation of access controls on IT assets. OE.TRUST ensures that file permissions and Access Control Lists on IT asset files are set appropriately to prevent system users gaining unauthorized access.

TE.OPERATE Rationale

T.OPERATE (*Insecure Operation)* is countered directly by OE.INSTALL, which ensures that the TOE and its underlying platform are correctly installed, managed and operated.

TE.CRASH Rationale

T.CRASH (*Abrupt Interruptions)* is countered by OE.MEDIA and OE.RECOVERY. These ensure that suitable recovery mechanisms are in place to recover from a crash and that the media used during the crash recovery is able to maintain the confidentiality, integrity and availability of the TOE.

P.ACCOUNT Rationale

P.ACCOUNT is satisfied by O.AUDIT.GEN, O.AUDIT.RECORD and OE.AUDIT.SYSTEM which ensure the TOE, with assistance from the IT environment, has the means of recording and investigating security relevant events which could be indicative of an attack aimed at defeating the TOE security features. OE.ADMIN ensures that the underlying operating system provides reliable timestamps for use in audit records. O.I&A provides support by allowing audit records to include data identifying the user in a way which is appropriate to the resource being accessed. O.ACCESS and O.ADMIN provide support by controlling access to OID audit data and audit configuration data which only highly trusted individuals must be allowed to view and modify. OE.ADMIN ensures that the underlying operating system provides reliable timestamps for use in audit records. OE.FILES provides support by preventing users gaining direct access to files holding directory audit data to modify or remove evidence of an attack. OE.AUDITLOG ensures audit data is correctly managed by the administrator so that it can be used to detect attacks. OE.SEP prevents TSF components being tampered with and ensures the isolation of web user sessions that could otherwise result in attacks on TOE security features being undetected.

Assumptions Rationale

This section demonstrates how the security objectives map to the TOE secure usage assumptions.

A.TOE.CONFIG is directly provided by OE.INSTALL part a) because [ECD] defines the evaluated configuration of the TOE.

A.SYS.CONFIG is directly provided by OE.INSTALL part b).

A.PHYSICAL is directly provided by OE.PHYSICAL.

A.ACCESS is provided by OE.INSTALL, OE.TRUST, OE.AUTHDATA, and OE.ADMIN.

A.MANAGE is provided by OE.TRUST, supported by OE.INSTALL, OE.AUDITLOG, OE.AUTHDATA, OE.MEDIA, OE.ADMIN, OE.AUDIT.SYSTEM, OE.FILES, OE.RECOVERY and OE.SEP.

A.PEER is provided by OE.INSTALL and OE.PHYSICAL, which covers other IT components that communicate with the TOE over a physical connection.

Security Requirements Rationale

Suitability of TOE Security Requirements

The table below correlates the IT security objectives to the SFRs which satisfy them (as indicated by a *YES*), showing that each IT security objective is satisfied by at least one SFR, and that each SFR satisfies at least one IT security objective.

Table 7: Correlation of IT Security Objectives to Security Functional Requirements

Requirement	O.I&A	O.ACCESS	O.AUDIT	O.ADMIN
FIA_AFL.1	YES			
FIA_ATD.1	YES	YES	YES	YES
FIA_SOS.1	YES			
FIA_UAU.1	YES			
FIA_UAU.6	YES			
FIA_UID.1	YES	YES		
FIA_USB.1		YES		
FDP_ACC.1		YES		
FDP_ACF.1		YES		
FMT_MSA.1	YES	YES		YES
FMT_MSA.3	YES	YES		YES
FMT_MTD.1			YES	
FMT_REV.1	YES	YES		YES
FMT_SMF.1	YES	YES	YES	YES
FMT_SMR.1		YES		YES
FPT_RVM.1		YES		
FTA_TSE.1	YES			
FAU_GEN.1T			YES	
FAU_GEN.2			YES	
FAU_SAR.1T			YES	
FAU_SAR.3T			YES	
FAU_STG.1T			YES	

O.I&A Suitability

O.I&A is directly provided by FIA_UID.1, FIA_UAU.1 and FIA_USB.6, which provide the means of identifying, authenticating and re-authenticating users of the TOE. FIA_AFL.1 performs certain actions if a specified number of consecutive unsuccessful authentication attempts is made. FIA_ATD.1 provides a set of user attributes for each user while FMT_MSA.1, FMT_MSA.3, FMT_REV.1and FMT_SMF.1 specify controls over the modification of these attributes. FIA_SOS.1 provides for quality metrics to be applied when new passwords are chosen. FTA_TSE.1 controls the ability to create a TOE session by a user.

O.ACCESS Suitability

O.ACCESS is directly provided by FDP_ACC.1 which defines the access control policy and FDP_ACF.1 which specifies the access control rules. FMT_REV.1 enforces revocation of security attributes. FIA_ATD.1, FMT_SMR.1 and FIA_USB.1 ensure the TOE maintains the relevant security attributes and role of a user and that such attributes are associated with subjects created to act on his or her behalf. FIA_UID.1 ensures users are identified prior to any TSF-mediated access actions (where a possible identifier for the user can be that of the anonymous user). FPT_RVM.1 ensures that the access control functions are always invoked prior to access. FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1 provide support for the management of security attributes to control access to directory objects.

O.AUDIT Suitability

O.AUDIT is directly provided by FAU_GEN.1T which generates audit records for all security relevant events. FAU_GEN.2 supports the enforcement of individual accountability by ensuring the user responsible for each event can be identified appropriately. FIA_ATD.1 provides for the maintenance of user security attributes that can be included in audit records. FAU_STG.1T provides permanent storage for the OID audit trail, while FMT_MTD.1 and FMT_SMF.1 provide for the maintenance of that audit trail. FAU_SAR.1T and FAU_SAR.3T provide functions to review the contents of the OID audit trail.

O.ADMIN Suitability

O.ADMIN is directly provided by FMT_MSA.1, FMT_MSA.3, FMT_REV.1, FMT_SMF.1, and FMT_SMR.1, which specify the TOE's controls over the management of security attributes. FIA_ATD.1 provides for the maintenance of user security attributes.

The rationale above demonstrates the suitability of the TOE security requirements.

Suitability of Security Requirements for the IT Environment

The Security Requirements for the IT Environment section of Chapter 5 defines a set of SFRs for the IT environment to support the TOE SFRs. In addition, it provides general requirements for the IT environment to ensure the secure operation of the TOE that are described informally in order not to unduly limit the environments that can satisfy them. These general requirements are together sufficient to meet the following objectives for the IT environment defined in Chapter 4: OE.ADMIN, OE.I&A, OE.AUDIT.SYSTEM, OE.FILES and OE.SEP.

The table below shows how the SFRs for the IT environment are mapped to the security objectives for the IT environment (*YES* indicates where there is a mapping).

Table 8: Mapping of Security Objectives for the IT Environment to SFRs

Requirement	OE.ADMIN	OE.AUDIT. SYSTEM	OE.FILES	OE.SEP
FMT_MTD.1E	YES	YES		
FMT_SMF.1E	YES	YES		

Table 8: Mapping of Security Objectives for the IT Environment to SFRs

Requirement	OE.ADMIN	OE.AUDIT. SYSTEM	OE.FILES	OE.SEP
FPT_SEP.1E				YES
FPT_STM.1E	YES	YES		
FAU_SAR.1E		YES		
FAU_SAR.3E		YES		
FAU_STG.1E		YES	YES	

The rationale for these mappings is as follows:

- FMT_MTD.1E and FMT_SMF.1E, which specify the IT environment's controls over the management of the OAM and OVD audit trail, and FPT_STM.1E, which covers the requirement for the operating system to provide reliable timestamps, map to OE.ADMIN.
- FMT_MTD.1E and FMT_SMF.1E, which relate to management by the IT environment of the audit functions and the audit trail, and FAU_SAR.1E, FAU_SAR.3E, FAU_STG.1E , which provide audit record analysis and management functionality, are mapped to OE.AUDIT.SYSTEM. Also mapped to OE.AUDIT.SYSTEM is FPT_STM.1E, which covers the provision by the IT environment of reliable time stamps for inclusion in audit records.
- FMT_STG.1E, which requires that the IT environment protects OAM and OVD audit records stored in audit trail files against unauthorized deletion or modification, maps to OE.FILES.
- FPT_SEP.1E, which covers requirements for the IT environment to provide separation features to protect the TOE, is mapped to OE.SEP.

Dependency Analysis

The table below demonstrates that all dependencies of functional components are satisfied. This analysis covers all TOE SFRs and SFRs for the IT environment.

Table 9: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
1	**FIA_AFL.1**	FIA_UAU.1	4
2	**FIA_ATD.1**	-	-
3	**FIA_SOS.1**	-	-
4	**FIA_UAU.1**	FIA_UID.1	6
5	**FIA_UAU.6**	-	-
6	**FIA_UID.1**	-	-

Table 9: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
7	**FIA_USB.1**	FIA_ATD.1	2
8	**FDP_ACC.1**	FDP_ACF.1	9
9	**FDP_ACF.1**	FDP_ACC.1 FMT_MSA.3	8 11
10	**FMT_MSA.1**	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	8 14 15 See Note 1 below
11	**FMT_MSA.3**	FMT_MSA.1 FMT_SMR.1	10 15
12	**FMT_MTD.1**	FMT_SMF.1 FMT_SMR.1	14 15 See Notes 1 and 2 below
13	**FMT_REV.1**	FMT_SMR.1	15
14	**FMT_SMF.1**	-	-
15	**FMT_SMR.1**	FIA_UID.1	6
16	**FPT_RVM.1**	-	-
17	**FTA_TSE.1**	-	-
18	**FAU_GEN.1T**	FPT_STM.1E	26 See Notes 3 and 4 below
19	**FAU_GEN.2**	FAU_GEN.1T FIA_UID.1	18 6
20	**FAU_SAR.1T**	FAU_GEN.1T	18 See Note 2 below
21	**FAU_SAR.3T**	FAU_SAR.1T	20 See Note 2 below
22	**FAU_STG.1T**	FAU_GEN.1T	18 See Note 2 below

Table 9: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
23	**FMT_MTD.1E**	FMT_SMF.1E FMT_SMR.1	24 15 See Note 5 below
24	**FMT_SMF.1E**	-	-
25	**FPT_SEP.1E**	-	-
26	**FPT_STM.1E**	-	-
27	**FAU_SAR.1E**	FAU_GEN.1T	18
28	**FAU_SAR.3E**	FAU_SAR.1E	27
29	**FAU_STG.1E**	FAU_GEN.1T	18

Note 1: FMT_SMF.1 b) covers the dependency of FMT_MSA.1 for the management of security attributes and FMT_SMF.1 a) covers the dependency of FMT_MTD.1 for the management of the OID audit trail.

Note 2: The nature of the extensions to SFRs FMT_MTD.1, FAU_SAR.1, FAU_SAR.3, and FAU_STG.1 does not impact on the dependencies as defined for the CC Part 2 components from which they are derived. The extensions relate to the fact that the TSF only provides the ability to manage the OID audit trail. The security requirements for the IT environment FMT_MTD.1E, FAU_SAR.1E, FAU_SAR.3E, and FAU_STG.1E cover the IT environment's ability to manage the OAM and the OVD audit trail.

Note 3: The security requirement for the IT environment FPT_STM.1E.1 satisfies the dependency of the SFR FAU_GEN.1T for the provision of reliable timestamps.

Note 4: The modification of FAU_GEN.1 does not impact its ability to satisfy the dependencies of FAU_GEN.2, FAU_SAR.1, and FAU_STG.1.

Note 5: FMT_MTD.1E has 2 iterations. Its entry in the table above indicates that all of FMT_MTD.1E's dependencies are satisfied by FMT_SMF.1E and FMT_SMR.1.

Dependency analysis of the security assurance requirements

EAL4 is a self-contained assurance package and ALC_FLR.3 has no dependencies on any other component.

Demonstration of Mutual Support

The dependency analysis provided in the table above demonstrates mutual support between functional components, showing that all dependencies required by Part 2 of the CC are satisfied.

The following supportive dependencies exist for the TOE and the IT environment to prevent bypassing of and tampering with the TOE SFRs:

FIA_UID.1, FIA_UAU.1 and FIA_UAU.6 together with FIA_ATD.1 and FMT_MSA.1 provide support to all TOE SFRs which rely on the identification of individual users and their security attributes, namely: FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_SMR.1, FAU_GEN.1T, FMT_MTD.1, FMT_SMF.1 and FAU_SAR.1T.

FMT_MSA.3 provides support to FDP_ACC.1 and FDP_ACF.1 by ensuring objects are protected by default when newly created.

FMT_MSA.1 provides support to FDP_ACC.1, FDP_ACF.1 and FMT_SMF.1 by controlling the modification of security attributes.

FMT_REV.1 provides support to FMT_MSA.1, FDP_ACC.1 and FDP_ACF.1 by enforcing revocation of object security attributes.

FAU_STG.1T and FAU_STG.1E support FAU_GEN.1T by providing permanent storage for the generated audit records.

FMT_MTD.1 supports FAU_STG.1T and FMT_SMF.1 by protecting the integrity of the OID audit trail.

FPT_RVM.1 and FPT_SEP.1E support FDP_ACC.1 and FDP_ACF.1 by ensuring the Resource Access Control SFP is always invoked before access is granted to resources and by providing separate domains that protect the TSC from interference and tampering by untrusted subjects.

Strength of Function Validity

The PWD mechanism is the only TOE mechanism that is probabilistic or permutational. It has a strength of SOF-*high*, which is an appropriate claim for environments that demand EAL4 assurance. This strength of function is intended to provide enough protection against straight forward or intentional attack from threat agents having a high attack potential.

Assurance Requirements Appropriate

The target assurance level is EAL4, augmented with ALC_FLR.3. EAL4 is appropriate because the TOE is designed for use within environments where asset owners require up to EAL4 assurance to reduce the risk to those assets to an acceptable level.

ALC_FLR.3 has been included in addition to EAL4 to cause the evaluation of the TOE's flaw remediation procedures which TOE users need to be in place following its release. These procedures are required to offer continuing assurance to users that the TOE provides secure access to the resources that are crucial to their enterprise's success.

To meet this requirement, the flaw remediation procedures must offer:

- the ability for TOE users to report potential security flaws to Oracle,
- the resolution and correction of any flaws with assurance that the corrections introduce no new security flaws, and
- the timely distribution of corrective actions to users.

ALC_FLR.3 is the ALC_FLR component which is at an appropriate level of rigour to cover these requirements.

TOE Summary Specification Rationale

This section demonstrates that the TOE Security Functions and Assurance Measures are suitable to meet the TOE security requirements.

TOE Security Functions Satisfy Requirements

The table below demonstrates that for each TOE SFR the TOE security functions are suitable to meet the SFR, and the combination of TOE security functions work together so as to satisfy the SFR:

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FIA_AFL.1.1	UIA.PWDC UIA.AUTH UIA.REAUTH	UIA.PWDC provides the configurable control governing the number of failed attempts to enter a user password correctly before a user account is locked. UIA.AUTH and UIA.REAUTH detect if this number is reached or exceeded.
FIA_AFL.1.2	UIA.PWDC UIA.AUTH UIA.REAUTH	UIA.PWDC provides the configurable control governing the number of failed userpassword check attempts before a user account is locked. UIA.AUTH and UIA.REAUTH lock the user's account if this number has been reached or exceeded.
FIA_ATD.1.1	SA.UATT	The TOE holds the required security attributes for each user.
FIA_SOS.1.1	SA.CHPWD	SA.CHPWD specifies the configurable metrics held in the password profile that the TOE checks user passwords against before they can be updated.
FIA_UAU.1.1	UIA.ASESS	If a user requests access to a resource hosted by the TOE and that resource is protected by a Policy configured to use the Anonymous authentication scheme, then the TOE will create a session in which only material authorized for access by the anonymous user is accessible.
FIA_UAU.1.2	UIA.AUTH UIA.AUTHC UIA.PWDC	If a user requests access to a resource hosted by the TOE and that resource is protected by a Policy configured to use the Form-based authentication scheme, then UIA.AUTHC and UIA.AUTH cover the conditions for the establishment of a session with the TOE to access that resource once the user has authenticated successfully. UIA.PWDC covers the case if the password has expired. UIA.AUTHC covers the situation if the user has already authenticated successfully during the user's current browser session and UIA.AUTH states the conditions to be met for the user to be authenticated succesfully for the first time during the user's current browser session.
FIA_UAU.6.1	UIA.REAUTH	If a user has established a session with the TOE to access a resource hosted by the TOE and that resource is protected by a Policy configured to use the Form-based authentication scheme, then UIA.REAUTH covers the conditions under which the user has to re-authenticate before the session with the TOE can continue.
FIA_UID.1.1	UIA.ASESS	If a user requests access to a resource hosted by the TOE and that resource is protected by a Policy configured to use the Anonymous authentication scheme, then the TOE will create a session in which only material authorized for access by the anonymous user is accessible. Under these circumstances, the user does not supply a user identifier before accessing a resource via the TOE.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FIA_UID.1.2	UIA.AUTH UIA.AUTHC	If a user requests access to a resource hosted by the TOE and that resource is protected by a Policy configured to use the Form-based authentication scheme, then UIA.AUTHC and UIA.AUTH cover the conditions for the establishment of a session with the TOE. UIA.AUTHC covers the situation if the user has already identified and authenticated successfully during the user's current browser session and UIA.AUTH requires the user to identify themselves before they can be authenticated succesfully for the first time during the user's current browser session.
FIA_USB.1.1	UIA.AUTH UIA.AUTHC UIA.ASESS SA.UATT	UIA.AUTH and UIA.AUTHC and UIA.ASESS state that the IP address of the computer originating the user's request to access the resource is associated with the user's session.SA.UATT lists the security attributes that are associated with a user requesting access to a resource.
FIA_USB.1.2	UIA.AUTH UIA.AUTHC UIA.ASESS SA.UATT SA.UEFF	UIA.AUTH and UIA.AUTHC and UIA.ASESS state that the IP address of the computer originating the user's request to access the resource is associated with the user's session.SA.UATT lists the security attributes that are associated with a user requesting access to a resource. SA.UEFF states that the value of a user attribute defined in SF SA.UATT will be effective in the user's session with the TOE only if the user had that attribute value at the start of the session. UIA.ASESS states that the identifier for the anonymous user is associated with the user's session with the TOE if the resource is protected by a policy configured to use the Anonymous authentication scheme.
FIA_USB.1.3	SA.UEFF	SA.UEFF states that the value of a user attribute defined in SF SA.UATT will be effective in the user's session with the TOE only if the user had that attribute value at the start of the session.
FDP_ACC.1.1	RAC.SUA RAC.OBA RAC.POL	RAC.SUA and RAC.OBA state that the Resource Access Control policy applies to users and resources. RAC.POL specifies the operations that the policy applies to by referring to [OAMAG, 4: Configuring Resource Types].
FDP_ACF.1.1	RAC.SUA RAC.OBA RAC.POL UIA.AUTH UIA.AUTHC UIA.ASESS SA.ATT SA.UATT SA.UEFF SA.OEFF	RAC.SUA and RAC.OBA state that the Resource Access Control policy applies to users and resources. RAC.POL defines the policy, which covers the use of time of access in policy rules. UIA.AUTH, UIA.AUTHC and UIA.ASESS state that the IP address of the computer originating the user's request to access the resource is associated with the user's session.SA.ATT and SA.UATT lists the security attributes that are associated with a resource and with a user requesting access to the resource. SAM.UEFF and SAM.OEFF state the conditions under which the user and resource security attributes are effective for a session with the TOE.
FDP_ACF.1.2	RAC.POL	RAC.POL fully covers the access control rules defined in FDP_ACF.1.2.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FDP_ACF.1.3	N/A	This SFR does not mandate any functionality. It is included for compliance with the CC.
FDP_ACF.1.4	N/A	This SFR does not mandate any functionality. It is included for compliance with the CC.
FMT_MSA.1.1	SA.ACC IA.CRUG SAM.MODATT SA.CHPWD	SA.ACC covers the policy for access control of the TOE security attributes held via OVD. IA.CRUG allows only authorized users to create user entries and group memberships when such TOE security attributes are held via OID. SAM.MODATT ensures an authorized user can create, read, modify or delete security attributes in OID directory entries that hold TOE security attributes. SA.CHPWD allows authorized users to change user password attributes.
FMT_MSA.3.1	SA.ACC SAM.EATT IA.CRUG	SA.ACC covers the policy for access control of the TOE security attributes held via OVD. SAM.EATT states that default security attributes when TOE security attributes are held via OID are as per the Default Access Policies defined for OID. IA.CRUG states that the default values of attributes of newly created user entries and group entries when such TOE security attributes are held via OID are as described in Chapters 8, 11 and 13 of [OIDAG].
FMT_MSA.3.2	SA.ACC RAC.SUA RAC.OBA RAC.POL SAM.EATT	SA.ACC covers the policy for access control of the TOE security attributes held via OVD. Unless access to TOE security attribute default values held by OID have been explicitly granted, as described in DAC.SUA, DAC.OBA and DAC.POL, no access will be allowed. SAM.EATT states that default security attributes when TOE security attributes are held via OID are as per the Default Access Policies defined for OID, which cover how authorized users can reset the default security configuration.
FMT_MTD.1.1	AUD.ACC AUD.DEL	AUD.DEL states that only an authorized administrator can clear the OID audit trail. AUD.ACC will allow only authorized users to view records in the OID audit log.
FMT_REV.1.1	SA.ACC SAM.MODATT	SA.ACC and SAM.MODATT ensure that only a suitably authorized user can delete security attribute entries for users and resources held via OVD and OID and hence to effectively revoke such attributes.
FMT_REV.1.2	SA.OEFF SA.UEFF	SA.OEFF and SA.UEFF state the conditions under which the user and object security attributes are effective for a session with the TOE and hence when a change to revoke such attributes becomes effective.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FMT_SMF.1.1	AUD.ACC AUD.DEL SA.ACC DAC.POL IA.CRUG SA.CHPWD SAM.EATT SAM.MODATT	AUD.DEL states that only an authorized administrator can clear the OID audit trail. AUD.ACC will allow only authorized users to view records in the OID audit log. SA.ACC covers the method by which security attribute entries for users and resources held via OVD can be modified, deleted and created. IA.CRUG allows only authorized users to create user entries and group memberships in the OID directory. SAM.MODATT and DAC.POL ensure an authorized user can create, read, modify or delete security attributes for OID directory users and OID directory entries, where the relevant attributes for entries are defined in SAM.EATT. SA.CHPWD allows authorized users to change user password attributes.
FMT_SMR.1.1	IA.UID UIA.OVDUID	IA.UID ensures that the TSF maintains the roles of normal user and super user for access to security attributes held in an OID directory and audit data held in the OID audit trail and states that the super user is the administrator for the directory. UIA.OVDUID ensures that the TSF maintains the roles of normal user and super user for access to security attributes held via OVD and states that the super user has administrator access for such attributes.
FMT_SMR.1.2	IA.UID UIA.OVDUID	IA.UID states how entries for normal users and the super user are identified for access to security attributes held in an OID directory and audit data held in the OID audit trail. UIA.OVDUID states how entries for normal users and the super user are identified for access to security attributes held via OVD.
FPT_RVM.1.1	RAC.POL SA.ACC IA.CRUG SAM.MODATT SA.CHPWD	RAC.POL ensures that the resource access control policy enforcement functions are always invoked before an access operation for a user can proceed. SA.ACC, IA.CRUG, SAM.MODATT and SA.CHPWD ensure that the relevant directory access control policy enforcement functions are always invoked before an access operation on a security attribute for a user can proceed.SA.ACC covers the policy for access control of the TOE security attributes held via OVD. IA.CRUG only allows authorized users to create user entries and group memberships when such TOE security attributes are held via OID. SAM.MODATT allows only an authorized user to create, read, modify or delete security attributes for directory users and directory entries when such TOE security attributes are held via OID. SA.CHPWD allows authorized users to change user password attributes.
FTA_TSE.1.1	RAC.POL	RAC.POL defines the resource access policy, which covers the use of time of access in the policy rules that may deny a user a session with the TOE (see [OAMAG, 6: Settimg Timing Conditions]).
FAU_GEN.1T.1	AA.INF AA.OVDINF AUD.INF	Audit records are generated to contain information as defined by AA.INF, AA.OVDINF and AUD.INF.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FAU_GEN.1T .2	AA.INF AA.OVDINF AUD.INF	Audit records are generated to contain information as defined by AA.INF, AA.OVDINF and AUD.INF.
FAU_GEN.2.1	AA.INF AA.OVDINF AUD.INF	Audit records are generated to contain the required user identity information as defined by AA.INF, AA.OVDINF and AUD.INF.
FAU_SAR.1T. 1	AUD.ACC	AUD.ACC states that the TOE will allow only authorized users to view all records in the OID audit log.
FAU_SAR.1T. 2	AUD.ACC	AUD.ACC states that the TOE will allow authorized users to view records in the OID audit log in a format suitable for the users to interpret the information.
FAU_SAR.3T. 2	AUD.ACC	AUD.ACC provides facilities for searching for audit records in the OID audit log according to their attribute values.
FAU_STG.1T. 1	AUD.DEL	AUD.DEL states that the TOE will allow only authorized users to delete audit records from the OID audit log.
FAU_STG.1T. 2	AUD.DEL	AUD.DEL states that the TOE will allow no modification to the audit records in the OID audit log.

The table below shows that all the SFRs are satisfied by at least one SF and that every SF is used to satisfy at least one SFR (but note that SFRs FDP_ACF.1.3 and FDP_ACF.1.4 are not explicitly satisfied by any particular SF because these SFRs specify null functionality).

Table 11: Mapping of SFs to SFRs

	FIA												FDP					FMT									FPT	FTA	FAU							
	AFL.1.1	AFL.1.2	ATD.1.1	SOS.1.1	UAU.1.1	UAU.1.2	UAU.6.1	UID.1.1	UID.1.2	USB.1.1	USB.1.2	USB.1.3	ACC.1.1	ACF.1.1	ACF.1.2	ACF.1.3	ACF.1.4	MSA.1.1	MSA.3.1	MSA.3.2	MTD.1.1	REV.1.1	REV.1.2	SMF.1.1	SMR.1.1	SMR.1.2	RVM.1.1	TSE.1.1	GEN.1T.1	GEN.1T.2	GEN.2.1	SAR.1T.1	SAR.1T.2	SAR.3T.1	STG.1T.1	STG.1T.2
UIA.AUTH	Y	Y				Y			Y	Y	Y			Y																						
UIA.ASESS					Y			Y		Y	Y			Y																						
UIA.AUTHC						Y			Y	Y	Y			Y																						
UIA.REAUTH	Y	Y					Y																													
UIA.PWDC	Y	Y				Y																														
RAC.SUA													Y	Y						Y																
RAC.OBA													Y	Y						Y																
RAC.POL													Y	Y	Y					Y							Y	Y								
SA.ATT														Y																						
SA.UATT			Y							Y	Y			Y																						
UIA.OVDUID																									Y	Y										
SA.ACC																		Y	Y	Y		Y		Y			Y									
SA.CHPWD				Y														Y						Y			Y									
SA.UEFF											Y	Y		Y									Y													
SA.OEFF														Y									Y													

Table 11: Mapping of SFs to SFRs

	FIA												FDP					FMT									FPT	FTA	FAU							
	AFL.1.1	AFL.1.2	ATD.1.1	SOS.1.1	UAU.1.1	UAU.1.2	UAU.6.1	UID.1.1	UID.1.2	USB.1.1	USB.1.2	USB.1.3	ACC.1.1	ACF.1.1	ACF.1.2	ACF.1.3	ACF.1.4	MSA.1.1	MSA.3.1	MSA.3.2	MTD.1.1	REV.1.1	REV.1.2	SMF.1.1	SMR.1.1	SMR.1.2	RVM.1.1	TSE.1.1	GEN.1T.1	GEN.1T.2	GEN.2.1	SAR.1T.1	SAR.1T.2	SAR.3T.1	STG.1T.1	STG.1T.2
IA.UID																									Y	Y										
IA.CRUG																		Y	Y					Y			Y									
SAM.EATT																			Y	Y				Y												
SAM.MODATT																		Y				Y		Y			Y									
DAC.POL																								Y												
AA.INF																													Y	Y	Y					
AA.OVDINF																													Y	Y	Y					
AUD.INF																													Y	Y	Y					
AUD.ACC																					Y			Y								Y	Y	Y		
AUD.DEL																					Y			Y											Y	Y

Assurance Measures Rationale

Table 4 in chapter 6 shows that, for each Security Assurance Requirement, there is an appropriate assurance measure.

PP Claims Rationale

This security target makes no claims about Protection Profile conformance.

ANNEX

A References

[CC] *Common Criteria for Information Technology Security Evaluation,* Version 2.3, August 2005.

[CAPP] *Controlled Access Protection Profile,* Version 1.d, NSA, October 1999.

[ECD] *Evaluated Configuration for Oracle Identity and Access Management 10g (10.1.4.0.1),* Oracle Corporation.

[LDAP3] *Lightweight Directory Access Protocol Version 3,* Request For Comments (RFC) 2251 of the Internet Engineering Task Force, December 1997, available on the World Wide Web at http://www.ietf.org/rfc.htm

[OAMAG] *Oracle Access Manager Access Administration Guide 10g (10.1.4.0.1),* Part No. B25990-01, Oracle Corporation.

[OAMDEP] *Oracle Access Manager Deployment Guide 10g (10.1.4.0.1),* Part Number B25344-01*,* Oracle Corporation, July 2006.

[OAMICAG] *Oracle Access Manager Identity and Common Administration Guide 10g (10.1.4.0.1),* Part No. B25343-01, Oracle Corporation.

[OIAMI] *Oracle Identity and Access Management Introduction 10g (10.1.4.0.1),* Part No. B25342-01, Oracle Corporation.

[OIDAG] *Oracle Internet Directory Administrator's Guide 10g (10.1.4.0.1),* Part No. B15991-01, Oracle Corporation.

[OIDST] *Security Target for Oracle Internet Directory 10g (10.1.4.0.1),* Issue 0.7, Oracle Corporation, October 2007.

[OIMUR] *Oracle Identity Management User Reference 10g (10.1.4.0.1),*
Part No. B15998-01, Oracle Corporation.

[OVDPM] *Oracle Virtual Directory Product Manual 10g (10.1.4.0.1),*
Part No. B28833-01, Oracle Corporation.

[RFC2616] *Hypertext Transfer Protocol -- HTTP/1.1,*
Request For Comments (RFC) 2616 of the Internet Engineering Task Force,
June 1999,
available on the World Wide Web at http://www.ietf.org/rfc.htm

[RFC2965] *HTTP State Management Mechanism,*
Request For Comments (RFC) 2965 of the Internet Engineering Task Force,
October 2000,
available on the World Wide Web at http://www.ietf.org/rfc.htm

ANNEX

B Glossary

Acronyms

ACI	Access Control Item
ACL	Access Control List
ACP	Access Control Policy Point
API	Application Program Interface
ASN.1	Abstract Syntax Notation One
AVL	Adelson, Velskii and Landis (a type of binary tree)
BER	Basic Encoding Rules (for ASN.1)
DAC	Directory Access Control
DAD	Database Access Descriptor
DIB	Directory Information Base
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name System
DSE	Directory-Specific Entry

DSML	Directory Service Markup Language
DTD	Document Type Definition
DUA	Directory User Agent
EJB	Enterprise Java bean
GUID	Global Unique Identifier
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
OAM	Oracle Access Manager
OAP	Oracle Access Protocol
OID	Oracle Internet Directory
OIP	Oracle Identity Protocol
OVD	Oracle Virtual Directory
RDBMS	Relational Database Management System
RDN	Relative Distinguished Name
SAML	Security Assertions Markup Language
SASL	Simple Authentication and Security Layer
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SID	System Identifier
SOAP	Simple Object Access Protocol
SOF	Strength of Function
SSO	Single Sign-on

TLS	Transport Layer Security
TOE	Target Of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WSDL	Web Services Description Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations

Terms

If a term described below has [CC] written after it, then this term is defined in the IT Security evaluation scheme. All other terms relate to Oracle Access Manager (OAM), Oracle Virtual Directory (OVD) and Oracle Internet Directory (OID). [OAMI, Glossary] and [OIDAG, Glossary] cover the full set of terms for OAM and OID. The terms that are relevant to this document are described below.

Access Client

An Oracle Access Manager component that monitors attempts to access a Web site and uses the Access Server to provide authorization and authentication services prior to completing the access requests. In the evaluated configuration for the TOE, this is an Oracle Access Manager-provided client called WebGate.

Access Control Group

A group entry in OID contains a list of names. A user is a member of the group if the user's DN is held in the group entry's multi-valued attribute `member` or `uniqueMember`. There are two types of access control groups: ACP groups and privilege groups.

Access Control Item (ACI)

The OID directory holds access control information to define the administrative policies relating to access control. This information is stored as user-modifiable operational attributes called access control items (ACIs).

Access Control List (ACL)

A list of Access Control Items is called an Access Control List (ACL).

Access Control Policy Point (ACP)

An Access Control Policy Point (ACP) is an entry for which the `orclACI` attribute has been given a value. The `orclACI` attribute contains ACL directives that are prescriptive. That is, these directives apply to all entries in the subtree below the ACP where this attribute is defined.

Access Server

This standalone server (of which there can be several instances) provides dynamic policy evaluation services for both Web-based and non-Web resources and applications. Different applications and web servers can make use of the authentication, authorization, and auditing services it provides.

ACP Group

If an individual is a member of an ACP group, then the directory server grants to that individual the privileges associated with that ACP group.

Adaptor

Provides proxied access to a range of data sources via OVD, including LDAPv2/ LDAPv3 directory servers and relational databases.

Administrator

A person who has some or all of the responsibilities of installing, configuring and maintaining a system, establishing and managing user accounts, allocating administrative privileges and permissions to trusted system users and auditing the usage of the system. Such users would be allocated the privileges and permissions necessary to discharge their responsibilities. [OIDAG, Part II] describes the basic administrative duties for managing an OID directory server. The super user for a directory has privileges that enable this user to perform such administrative duties.

Attribute

Each entry in a directory contains information stored in attributes.

Audit Log

The OID audit log is made up of directory entries, where each entry records the audit data for one event.

Audit Level

To enable OID auditing, the attribute `orclauditlevel` in the DSE must be modified to the appropriate level. The value held in this attribute is called the directory's audit level.

Audit Rule

A named filter that determines the tracking level of the authentication and authorization activities performed by Oracle Access Manager.

Authentication

Authentication is the process by which the claimed identity of a user requesting access to an IT asset is validated. OID implements four different levels of directory user authentication: Anonymous, Password-based (Simple Authentication), Certificate-based through Secure Socket Layer (SSL), and Indirect Authentication.

Authentication Services

Such services provide the means to authenticate users and systems when they try to access resources protected by Oracle Access Manager. In the TOE's evaluated configuration, these services support only the basic username and password authentication method.

Authorization

The process that determines the access permitted to users after they have been authenticated.

Authorization Rule

A named logic flow that describes the process to be followed to get an authorization result, generally over a set of resources within an Oracle Access Manager policy domain. An authorization rule usually contains an authorization scheme.

Authorization Scheme

A named link to a shared library holding the software for a method to be used to authorize a user.

Authorized Administrator

An administrator who has been granted the necessary privileges to perform his or her administrative duties.

AVL Tree

A binary tree representation that can be used for the entries in a directory.

Binding

The process of authenticating a user to a directory.

Data Anywhere

The data management layer that aggregates and consolidates data from RDBMS databases and LDAP directories into a virtual LDAP tree that can be used to support authentication and authorization using Oracle Access Manager.

Default Rules

Blanket rules that apply to all resources within an Oracle Access Manager policy domain, created to ensure that access is always controlled. The default rules apply for authentication, authorization and auditing, unless overridden by more specific rules.

Directory

A directory stores and retrieves information about organisations, individuals and other resources.

Directory Information Base (DIB)

The complete set of all information held in a directory. The DIB consists of entries that are related to each other hierarchically in a directory information tree.

Directory Information Tree (DIT)

A hierarchical tree-like structure consisting of the DNs of the entries.

Directory Server Instance

Each Oracle Directory Server instance services directory requests through a single OID dispatcher process listening at a specific TCP/IP port number. There can be more than one directory server instance on a node, each listening on a different port.

Directory Access Control (DAC)

Access control on directory objects based on access control information established by directory users.

Distinguished Name (DN)

Each entry in a directory is uniquely identified by a distinguished name, which defines exactly where in the directory's hierarchy the entry resides. It comprises all of the individual names of the parent entries back to the root.

Directory Server Instance

Each Oracle Directory Server instance services directory requests through a single OID dispatcher process listening at a specific TCP/IP port number. There can be more than one directory server instance on a node, each listening on a different port.

Dynamic Group

A group whose list of members is dynamically generated. Group membership can vary as users meet or do not meet the membership criteria.

Entry Level Access Control

The `orclEntryLevelACI` attribute is used for entry level access control, for which the policy pertains only to a specific entity.

HTTP Method

An HTTP method is an action to be performed on a resource, specified on the request line of the HTTP message by the client.

Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) is the underlying format used by the web to format and transmit messages and to determine what actions web servers and browsers should take in response to HTTP commands. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred. HTTP is defined in [RFC2616].

Identity Server

This standalone server (of which there can be several instances) processes all the requests related to user identity, group, organization, and credentials management requests.

Idle Session

A session that has generated no requests from the browser for a specified time period known as the idle session timeout. Oracle Access Manager considers such sessions to be inactive or idle. Oracle Access Manager terminates idle sessions automatically after the idle session timeout elapses.

Knowledge Reference

A knowledge reference (or referral) allows a directory server to return a reference to another server as a result of a directory query.

LDAP Client

LDAP Clients send LDAP requests to an OID listener/dispatcher process listening for LDAP commands at its port.

LDAP Data Interchange Format (LDIF)

The set of standards for formatting an input file for any of the LDAP command-line utilities.

LDAP Filter

A string of characters interpreted by an LDAP directory to generate custom search results. Also known as an LDAP rule.

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol is a standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate. LDAP Version 3 is defined in [LDAP3].

Listener

For each server component of the TOE products, this is a socket level monitor that listens for appropriate HTTP or LDAP protocol requests.

Mapping Script

This is a type of plug-in that allows administrators to perform manipulations allowing data to be mapped via a script as it passes through the server. For example, an Active Directory object can be made to look like an InetOrgPerson object.

Object

An entity within the TSC that contains or receives information and upon which subjects perform operations. Objects are visible through the TSFI and are composed of one or more TOE resources encapsulated with security attributes. [CC]

Object Class

An object class is a group of attributes that define the structure of a directory entry.

Oracle Access Manager (OAM)

Oracle Access Manager provides Web-based identity administration, as well as access control to Web applications and resources running in a heterogeneous environment. It provides the user and group management, delegated administration, password management and self-service functions necessary to manage large user populations in complex, directory-centric environments.

Oracle Access Protocol (OAP)

The protocol governing communications between the Access System components of Oracle Access Manager (Policy Manager, Access Server and WebGate) and a Web server.

Oracle Identity Protocol (OIP)

The protocol governing communications between the Identity System components of Oracle Access Manager (Identity Server, WebPass) and a Web server.

Oracle Internet Directory (OID)

Oracle Internet Directory is a general purpose directory service that enables fast retrieval and centralised management of information about dispersed users and network resources. LDAP V3 is used to communicate with it and OID is an Oracle Database 10*g* application.

Oracle Virtual Directory (OVD)

Oracle Virtual Directory is an LDAPv3-enabled service that provides virtualised abstraction of one or more enterprise data sources into a single directory view. Oracle Virtual Directory provides the ability to integrate LDAP-aware applications into diverse directory environments while minimizing or eliminating the need to change either the infrastructure or the applications.

Password Management Services

These services provided by Oracle Access Manager allow administrators to specify multiple password policies, constraints on password composition, configurable password validity period and notification, forced password change, lost password management setup, and password creation/change rules.

Password Policy

A password policy is a set of rules about how passwords can be created, changed and used within Oracle Access Manager. Oracle Internet Directory also has password policies that relate to the passwords stored for use when a user binds to a directory.

Platform

The combination of software and hardware underlying the TOE. [CC]

Plug-in

A method by which administrators can add software to OAM or OVD or can substitute custom-built software for OAM or OVD software to implement features such as authentication and authorization.

Policy

For Oracle Access Manager a policy is the set of authentication, authorization and auditing rules that apply to one or more resource types within a policy domain. In the absence of a policy for a specific resource type, the default rules for all resource types in the policy domain apply.

Policy Domain

For Oracle Access Manager a policy domain encompasses the resources to be protected, the rules for protection, the policies for protection and the administrative rights. Policy domains can be defined using Policy Manager.

Policy Manager

The Oracle Access Manager application through which users can perform policy management, designation of resources (both Web and non-Web), and policy testing through simulated user access.

Privilege Group

A Privilege Group is a higher-level access control group. This is similar to an ACP group, but it also provides for additional checking beyond a single ACP. Thus, if the OID directory finds an ACP at a higher level in the DIT that grants the privilege group access to the requested object, then it overrides any denials by a subordinate ACP and grants the user access to the object.

Referral

A referral (or knowledge reference) allows an OID directory server to return a reference to another server as a result of a directory query.

Resource

Information or an activity that can be protected by Oracle Access Manager and can be identified by a URI.

Role

A predefined set of rules establishing the allowed interactions between a user and the

TOE. [CC]

For Oracle Access Manager, a role is a predefined list of users that are grouped according to their organisational roles (some examples of roles are: all users, all managers, all direct reports of a manager). Such roles can be defined for the use of administration features. The special role of Master Administrator is empowered to configure the deployment and assign administrative tasks. Two roles are also defined for use in authorization rules, which are called ‘Anyone’ and ‘No Role’. The use of Anyone means that rule applies to any users (including anonymous users) and the use of No Role prevents any action being taken based on roles.

Schema

A schema defines the type of information stored in a directory. It consists of object classes and attributes.

Searchbase

The location in the DIT where users can begin their searches.

Security Attribute

Information associated with subjects, users, and/or objects which is used for the enforcement of the TSP. [CC]

Security Domain

The set of objects that a subject has the ability to access. [CC]

Security Function (SF)

A part or parts of the TOE which have to be relied upon for enforcing a closely related subset of the rules from the TSP. [CC]

Security Function Policy (SFP)

The security policy enforced by a SF. [CC]

Security Functional Requirement (SFR)

A security functional requirement defined in a protection profile or security target. [CC]

Server

A program that accepts connections in order to service requests by sending back responses. Any given program may be capable of being both a client and a server. The use of these terms refers only to the role being performed by the program for a particular connection, rather than to the program’s capabilities in general.

SOF-high

A level of the TOE strength of function where analysis shows that the function provides adequate protection against a deliberately planned or organised breach of TOE security by attackers possessing a high attack potential. [CC]

Strength of Function (SOF)

A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms. [CC]

Subject

An entity within the TSC that causes operations to be performed. [CC]

Suitably Authorized Administrator

When a particular administrative operation is under consideration, a suitably authorized administrator is an administrator who has been granted the necessary privileges to perform this operation.

Suitably Authorized User

When a user is attempting to perform an operation on a directory object, a suitably authorized user is one who is permitted by the Directory Access Control SFP to perform the operation on the object. This policy is described in Chapter 18 of [OIDAG].

super user

The super user is the administrator for the directory (but note that it is subject to access control policies as from this release of the TOE, and hence no longer has full access to all directory information by default). The actual name and the password for the super user are held in the DSE (by default the super user's name is `orcladmin`)

System

A specific IT installation, with a particular purpose and operational environment [CC]

Target Of Evaluation (TOE)

The product or system being evaluated. [CC]

TOE resource

Anything usable or consumable in the TOE. [CC]

TOE Scope of Control (TSC)

The set of interactions which can occur with or within a TOE and are subject to the rules of the TSP. [CC]

TOE Security Functions (TSF)

A set consisting of all the software of the TOE that must be relied on for the correct enforcement of the TSP. [CC]

TOE Security Policy (TSP)

A set of rules that regulate how assets are managed, protected and distributed within a TOE. [CC]

TSF Interface (TSFI)

A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF. [CC]

Uniform Resource Identifier (URI)

A compact string of characters for identifying an abstract or physical resource. It is formally defined by RFC 2396.

Uniform Resource Locator (URL)

A Uniform Resource Identifier that identifies a resource via a representation of its primary access mechanism (e.g. its network location). URLs are usually made up of a scheme, like http or https, a hostname, and a path, for example: `http://httpd.apache.org/docs-2.1/glossary.html`.

User

Any entity (human or machine) outside the TOE that interacts with the TOE. [CC]

User Agent

The client which initiates an HTTP request. This is typically a browser.

Userpassword Check

This phrase refers to OID operations that check whether the `userpassword` attribute of a user entry has a particular value. These are `bind` operations for which a password has been supplied and `compare` operations which are acting on the `userpassword` attribute of a user entry.

Virtual Directory

A logical, aggregated directory that presents user data drawn from multiple sources, just as if all that data came from a standard LDAP directory to which a customised schema has been uniformly applied.

Virtual Directory Schema

This is a schema that can be developed for use by the top-level directory that the Oracle Virtual Directory Server makes visible to Oracle Access Manager. It must be extended with the Oracle Access Manager user schema. Optionally the virtual directory schema can be further extended with additional attributes drawn from the target data sources.

This Page Intentionally Blank