ORACLE APPLICATION SERVER 10g

Security Target for
Oracle Identity Manager Release 9.1.0.2

November 2011

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

Security Target for Oracle Identity Manager Release 9.1.0.2

November 2011

Authors: Julian Skinner and Peter Goatly.

Contributors: Adam O'Brien and Hugh Griffin.

Contents

1 Introduction....1

Identification and CC Conformance 1
TOE Overview 1
TOE Product Components 2
Document Overview 2

2 TOE Description 3

Oracle Identity Manager....3
OIM Architecture 4
OIM Features....5
TOE Definition....7
TOE Modes of Operation....8
Identification and Authentication....9
TOE Access Control....10
Provisioning Access Control....10
Security Attribute Maintenance 11
Reconciliation Dataflow....12
Audit and Accountability 12
Other Oracle Identity Manager Security Features....12

3 Security Environment 15

IT Assets....15
Operational Environment 15
Threats....16
Organisational Security Policies 17

Assumptions 17

4 Security Objectives 19

TOE Security Objectives 19
Operational Environment 20
Environmental Security Objectives 20

5 IT Security Requirements 25

TOE Security Functional Requirements 25
TOE Security Assurance Requirements 34
Security Requirements for the IT Environment 34
Minimum Strength of Function 37

6 TOE Summary Specification 39

TOE Security Functionality 39
Security Mechanisms and Techniques 44
Assurance Measures 44

7 Protection Profile Claims 47

PP Reference 47

8 Rationale 49

Security Objectives Rationale 49
Security Requirements Rationale 53
TOE Summary Specification Rationale 58
Assurance Measures Rationale 62
PP Claims Rationale 62

A References 63

B Glossary 65

Acronyms 65
Terms 66

CHAPTER

1 Introduction

This document is the security target for the Common Criteria evaluation of Oracle Identity Manager Release 9.1.0.2.

Identification and CC Conformance

Title: Security Target for Oracle Identity Manager Release 9.1.0.2

Target of Evaluation (TOE): Oracle Identity Manager (OIM)

Release: 9.1.0.2

Connectors: Database User Management Connector 9.0.4.5 and Oracle Internet Directory Connector 9.0.4.5

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

Database Platform: Oracle Database 10*g* (10.2.0.2.0).

Application Server Platform: Oracle Application Server 10*g* (10.1.3.3.0).

CC Conformance: This Security Target is extended with respect to [CC, Part 2] and is conformant with [CC, Part 3].

Assurance: EAL4 augmented with ALC_FLR.3.

Keywords: Oracle Identity Manager, OIM, EAL4

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

TOE Overview

Oracle Identity Manager is a highly flexible and scalable enterprise identity management system that centrally controls user accounts and access privileges to enterprise IT resources. It provides the functionalities of identity administration, approval and request management, policy-based entitlement management, and audit and compliance automation. OIM automates user identity provisioning and

deprovisioning and enables organizations to manage the entire life cycle of user identities across all resources in the organization.

The security functionality in the TOE includes:

- user identification and authentication with password management;
- TOE access control;
- provisioning access control;
- security attribute maintenance; and
- auditing.

TOE Product Components

For this evaluation the Oracle Identity Manager components included in the TOE are:

- the Oracle Identity Manager server application;
- the Oracle Internet Directory Connector (Release 9.0.4.5); and
- the Database User Management Connector (Release 9.0.4.5).

These components run on the Oracle Application Server 10*g* (10.1.3.3.0) products Oracle Containers for J2EE (OC4J) and Oracle HTTP Server (OHS).

Oracle Identity Manager relies on the Oracle Database 10*g* Server Enterprise Edition 10.2.0.2.0 to act as the repository for storing its data and uses Oracle Net Services 10.2.0.2.0 for its communication interfaces with Oracle Database.

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

Document Overview

For Issue 0.1, change bars indicate changes relative to the TOE Scope document. With the exception of Issue 0.1, change bars indicate changes relative to the previous issue of this document.

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.

CHAPTER

2 TOE Description

This chapter describes the product features that provide security functionality and contribute to the security of a system using the TOE.

The major elements of the Oracle Identity Manager (OIM) security architecture are described below, and the TOE is subsequently defined as a subset of this architecture. The TOE's mechanisms for identification and authentication, access control, and accountability and auditing are summarised. Additional OIM security features that are not addressed by the security functional requirements of Chapter 5 are also briefly discussed.

An overview of the features of Oracle Identity Manager is given in [OIMC, 3].

Oracle Identity Manager

Oracle Identity Manager is a highly flexible and scalable enterprise identity management system that centrally controls user accounts and access privileges to enterprise IT resources. It provides the functionalities of identity administration, approval and request management, policy-based entitlement management, and audit and compliance automation. OIM automates user identity provisioning and deprovisioning and enables organizations to manage the entire life cycle of user identities across all resources in the organization.

OIM can be used as the single point of management for the IT resources in an organization. OIM provides various configuration options for integration with different kinds of resources.

Provisioning Configuration

Oracle Identity Manager can be used to create, maintain, and delete users on target systems. In this configuration, Oracle Identity Manager acts as the front-end entry point for managing user data on the target systems. After accounts are provisioned, the users for whom the accounts have been provisioned can access the target systems without any interaction with Oracle Identity Manager.

Reconciliation Configuration

Oracle Identity Manager provides a centralized control mechanism to manage users and entitlements and to control user access to resources. However, Oracle Identity Manager can be configured not to act as the primary repository or the front-end entry point of the user accounts. Instead, Oracle Identity Manager can be configured to periodically poll target systems for maintaining an up-to-date profile of all accounts that exist on those systems.

The above 2 configurations can be combined to manage the entire life cycle of user identities across all resources in the organization. The “TOE Definition” section below indicates that both of these configurations are included in the evaluated configuration.

OIM Architecture

OIM is built on a J2EE-based N-tier deployment architecture that separates the platforms presentation, business logic and data tiers. The J2EE application server model of Oracle Identity Manager provides scalability, fail-over and load-balancing, and inherent Web deployment. It is based on an open, standards-based technology and has a three-tier architecture (the client applications, an Oracle Identity Manager supported J2EE-compliant Application Server and an ANSI SQL-compliant database). Oracle Identity Manager can provision LDAP-enabled and non-LDAP-enabled applications. OIM runs on leading J2EE complaint application server platforms.

Client Software

The OIM client software consists of the Design Console and the Administrative and User Console. Users login to Oracle Identity Manager through the Administrative and User Console, which provides the Oracle Identity Manager server application with the user's login credentials. With the Administrative and User Console, users search for, edit and delete information in the Oracle Identity Manager repository and raise requests for resource provisioning etc. The Design Console can only be accessed by System Administrators and is only used to configure OIM for operational use.

Application Server Software

The OIM software hosted by the application server implements the business logic in Java Business Objects. These objects are managed and supported by the J2EE application server (examples of which are JBoss Application Server, BEA WebLogic Server, IBM WebSphere Application Server and Oracle Containers for J2EE). The Java Business Objects implement the business logic of the Oracle Identity Manager server application, although they are not exposed to any methods from other applications. The business functionality of Oracle Identity Manager can be accessed using the application programming interface (API) layer in the J2EE infrastructure, which provides the lookup and communication mechanism.

HTTP Server

Oracle HTTP Server (OHS) is used to serve HTTPS requests from the Oracle Admin and User client to the OC4J container in which OIM operates. SSL is configured for defense in depth within components external to the TOE, and therefore, is out of the scope of the evaluation.

External Resources

OIM provisions users to external IT systems via connectors.

Data Access

Oracle Identity Manager implements business logic to manage the storage of data in its repository.

OIM’s architecture is illustrated in the figure on the next page. This figure illustrates a set of external IT systems that the TOE can provision to users as well as the repository used to store OIM’s data.

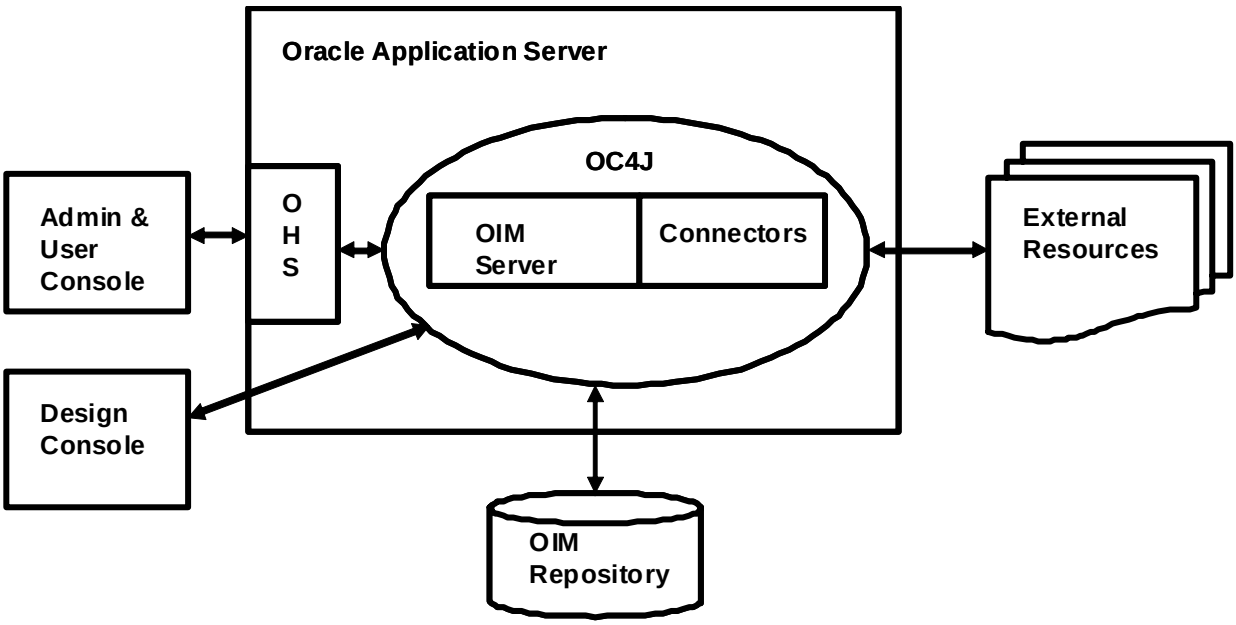

Figure 1: OIM Architecture

The "TOE Definition" section below indicates which of the architectural components are included in the evaluated configuration.

OIM is accessed by users via the Administrative and User Console and via the Design Console.

Administrative and User Console

The Administrative and User Console is a Web-based thin client that can be accessed from any Web browser. This console provides user self-service and delegated administration features that serve most of the provisioning requirements.

Design Console

The Design Console is used to configure the system settings for the use of the TOE. Once the initial configuration of the TOE has been completed, the Design Console is used by the system administrator when it is necessary to change items in the OIM re-repository (in the OIM Database) such as password policies, provisioning settings, reconciliation settings and the maximum number of permissible login retry attempts.

OIM Features

This section describes the features of Oracle Identity Manager.

Profile Management

Users can view and edit their own profiles by using the self-service interface of Oracle Identity Manager.

Provisioning

Provisioning is the granting of access to resources to users in conformance with Oracle Identity Manager policies.

Request Management

Users can create provisioning requests for resources with fine-grained entitlements.

Business approvers, such as team leaders, line managers, and department heads, can use the same Web-based interface to examine and approve incoming requests.

Policy Management

Oracle Identity Manager enables policy-based automated provisioning of resources with fine-grained entitlements. For any set of users, administrators can specify access levels for each resource to be provisioned, granting each user only the exact level of access required.

Workflow Management

Oracle Identity Manager supports the separation of approval and provisioning workflows. An approval workflow enables an organization to model its preferred approval processes for managing resource access requests. A provisioning workflow enables an organization to automate IT tasks for provisioning resources with the most complex of provisioning procedures.

Deprovisioning

When the access for a user is no longer required or valid in an organization, Oracle Identity Manager revokes access on demand or automatically, as dictated by attribute-based access policies.

Self-Service Password Management

Users can manage their own passwords across managed resources by using the self-service capabilities of Oracle Identity Manager. In case a user forgets the password, Oracle Identity Manager can present customizable challenge questions to enable self-service identity verification and password retrieval (although this feature is not used in the evaluated configuration).

Password Synchronization

Oracle Identity Manager can synchronize or map passwords across managed resources and enforce differences in password policies among these resources.

Identity Reconciliation

The process of reconciliation is performed by the reconciliation engine. If Oracle Identity Manager detects any changes to user accounts or user access privileges in target systems, then the reconciliation engine can immediately take corrective action, such as by undoing the change or notifying the administrator. Oracle Identity Manager also helps administrators to detect and map existing accounts in target resources.

Rogue/Orphan Account Management

A rogue account is an account created “out of process” or beyond the control of the provisioning system. An orphan account is an operational account without a valid user. These accounts represent serious security risks to an organization. Oracle Identity Manager can monitor rogue and orphan accounts continuously. By combining denial access policies, workflows, and reconciliation, an organization can perform the required corrective actions when such accounts are discovered, in accordance with security and governance policies.

Attestation

Oracle Identity Manager offers an attestation feature that can be deployed quickly to enable an organization-wide attestation process that provides automated report generation, delivery, and notification. Attestation reviewers can review fine-grained access reports within an interactive user interface that supports fine-grained certify, reject, decline, and delegate actions. All report data and reviewer actions are captured for future auditing needs.

Audit

Oracle Identity Manager reports on both the history and the current state of the provisioning environment. Some of the identity data captured by Oracle Identity Manager includes user identity profile history, user group membership history, user resource

access, and fine-grained entitlement history. Oracle Identity Manager also captures data generated by its workflow, policy, and reconciliation engines. By combining this data along with identity data, an organization has all the required data to address any identity and access-related audit inquiry.

In addition to features for use by an enterprise's auditors, Oracle Identity Manager also provides features for the logging of audit records that can be used by administrators to check for actual or potential violations of the TOE's security policy.

Connectors

A connector is an abstraction for a collection of components that are used to perform reconciliation and provisioning operations on a target system. Each component plays a specific role during reconciliation, provisioning, or both. In a predefined connector, the definitions of these components are included in the connector XML files. When the connector XML files are imported, these components are automatically created in Oracle Identity Manager. An overview of the features of the Oracle Identity Manager Connectors is given in [OIMCC, 1].

TOE Definition

For this evaluation the Oracle Identity Manager components included in the TOE are:

- the Oracle Identity Manager server application;
- the Oracle Internet Directory Connector (Release 9.0.4.5); and
- the Database User Management Connector (Release 9.0.4.5).

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

- the Red Hat Linux operating system;
- the Oracle Database system that acts as the repository for storing the data used by Oracle Identity Manager; and
- the Oracle Application Server, comprising Oracle Containers for J2EE (OC4J) and Oracle HTTP Server (OHS), on which OIM runs.

The versions of these platforms specified in Chapter 1 have been chosen so that the evaluated configuration of the TOE is supported by Oracle.

The TOE is based on the J2EE architecture and as such communicates solely with the J2EE-compliant server hosting it. Thus the external interfaces into the TOE are those supported by the J2EE specification such as:

- Java Server Pages
- Servlets
- Enterprise Java Beans (EJBs)
- Java Message Service
- Java Authentication and Authorization Service (JAAS)
- Java Naming and Directory Interface (JNDI)
- J2EE Connector Architecture

The figure on the next page illustrates the logical scope of the configuration of the TOE to be used for this evaluation. The configuration is a Provisioning and Reconciliation deployment. [ECG] defines a configuration that involves an instance of Oracle Internet Directory being used as the Trusted Source of HR data for automated user creation and a database representing a second resource to which the users may be provisioned. [ECG] also covers the physical scope of the TOE for this evaluation and includes a definition of the machines used, the configuration of firewalls, the types of connections etc.

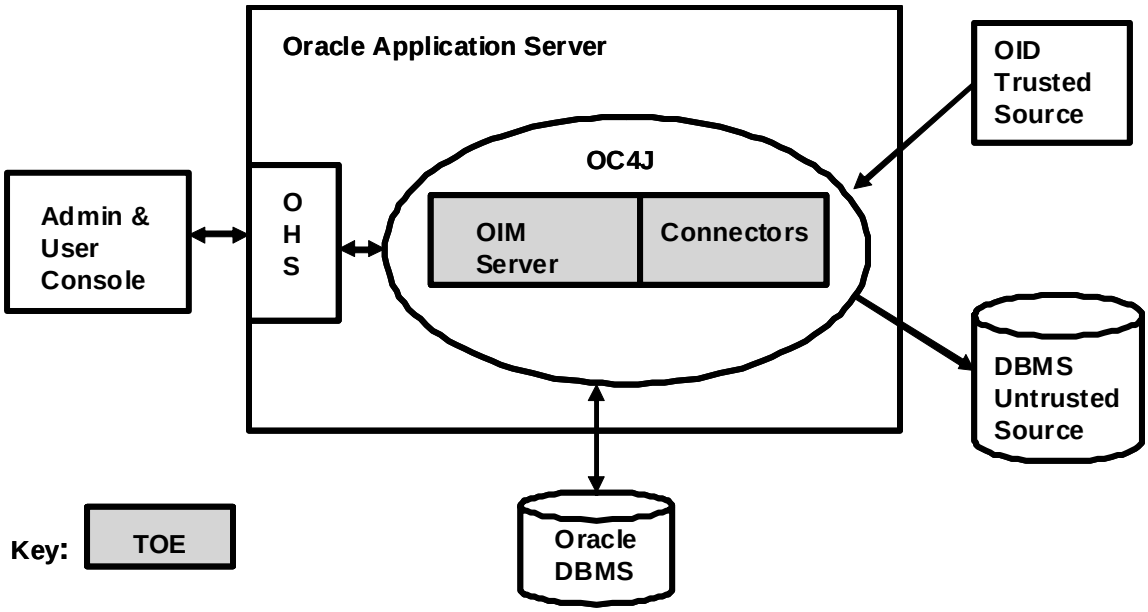

Figure 2: TOE configuration

Figure 2 indicates the specific subset of the OIM architecture shown in Figure 1 that forms the TOE for this evaluation. Figure 1 shows the full OIM architecture and the potential for multiple external resources to which users can be provisioned, while Figure 2 illustrates the actual deployment that will be used to cover the testing of both Provisioning and Reconciliation during the evaluation.

The Administrator and User Console is not included in the TOE because it is a thin client that does not include any functionality. It merely consists of Web pages for display via the user's browser. Users click on links in these pages to use the TOE features implemented in the OIM Server Application that is hosted by OC4J.

TOE Modes of Operation

Modes

The TOE has the following modes of operation (and no others):

- 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 provides provisioning and deprovisioning features for users and administrators who communicate with the TOE via the Administrative and User Console.

The actual resources that the users are provisioned with can be accessed independently of OIM and therefore are outside the scope of the TOE.

There is no TOE mode for debugging, although setting the log level to “Debug” results in detailed information being written to the log file.

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.

These operational assumptions are compatible with a secure environment, such as a Defence establishment, in which Oracle Identity Manager is used to provision sensitive resources to authorized users over a secure network.

Identification and Authentication

User Identification

An OIM account is granted to a user of OIM to give the user the ability to login to Oracle Identity Manager in order to access Oracle Identity Manager’s features. At the minimum, these features include creating and managing requests for provisioning resources. An OIM account can be created in the following ways:

- through reconciliation from one or more trusted identity sources, such as Oracle Human Resources Management System (HRMS) or an LDAP directory;
- manually through the Administrative and User Console;
- through the Java APIs and/or the SPML Web Service.

In addition, a user can also self-register in the Administrative and User Console to create an account. If the administrator has set OIM to require approvals for self-registration requests, the account is ready for use when the required approvals are obtained.

Password Policies

Oracle Identity Manager lets administrators define complex password policies. Supported password complexity requirements include:

- password length;
- alphanumeric and special characters usage;
- uppercase and lowercase usage;
- full or partial exclusion of user name;
- minimum password age; and
- historical passwords.

In addition, Oracle Identity Manager allows the application of multiple policies for each resource. For instance, users with fewer privileges can be subjected to a more relaxed password policy, whereas privileged administrators can be subjected to a more

stringent policy.

If a user forgets their password, then they can reset the password from a page which prompts the user to answer challenge questions (although this feature is not used in the evaluated configuration).

TOE Access Control

An OIM account is granted to a user of OIM in order to give the user the ability to login to Oracle Identity Manager to access Oracle Identity Manager features. At the minimum, these features include creating and managing requests for provisioning resources. An OIM user can be granted additional permissions, including delegated administration of various entities such as users and organizations and the ability to define workflows.

Access to other features of Oracle Identity Manager is only available to users who are members of a group that has been designated as an administrator of specific entities in OIM for another group in OIM. See [OIMAG, 10: Table 10.2] for details of the permissions and entities for Administrative Groups.

Provisioning Access Control

Oracle Identity Manager allows accounts on other resources to be requested and allocated (provisioned) to users. The resource can be an application, access to a database, rights to a directory structure on a network, or other entities to which access is vital. The manner in which access to the resource is granted and the permissions given to a user on that resource are governed by provisioning processes that OIM Administrators define.

Oracle Identity Manager controls the provisioning of resources by using processes and tasks. It also uses a specific kind of process, called an approval process, to govern the approvals that must be obtained before the provisioning of a resource may occur. Oracle Identity Manager has two different types of resource-related processes: *approval processes* and *provisioning processes*.

An approval process determines whether or not a resource is to be approved for provisioning to one or more users or organizations for whom it is requested. Approval processes consist of a series of tasks that require responses from the users responsible for approving the provisioning of the resource. Because these responses are manually provided, they are assigned to an approver or a group of approvers.

A provisioning process is the process used to allocate (provision) the resource to one or more users or organizations for whom it is requested. Provisioning processes consist of a series of automated tasks that perform the steps necessary to grant access to a given resource. The provisioning process cannot be initiated until the approval process is complete, except in cases where an approval process has not been defined for the resource.

Access Policies

An access policy is a list of user groups and the resources with which users in the group are to be provisioned or deprovisioned. While defining policies, administrators can specify whether the resources in a particular policy are to be provisioned with or without approval. If an access policy of type “with approval” is applied to a user and

if the access policy specifies that resources be provisioned, then Oracle Identity Manager generates a request. This request must be approved before the user gets the resources. If an access policy of type "without approval" is applied to a user, the resources are directly provisioned to the user without any request being generated.

Policies are only applied to direct-membership users (that is, users who are not in subgroups) in the groups that are defined on the access policies. Administrators can specify if a resource in a policy must be revoked when the policy no longer applies. If you do so, then these resources are automatically revoked from the users by Oracle Identity Manager when the policy no longer applies to the users.

While creating an access policy, administrators can select resources to be denied along with resources to be provisioned for groups. If a resource is first selected for provisioning and then the same resource is selected to be denied, then Oracle Identity Manager removes the resource from the list of resources to be provisioned. If two policies are defined for a group in which one is defined to provision a resource and the other is defined to deny the resource, then Oracle Identity Manager does not provision the resource irrespective of the priority of the policies. If policies are defined to deny resources to users belonging to a group, then the resources will not be made available for selection during request-based or direct provisioning to these users.

Attestation

Attestation enables reviewers to be notified of a report they must review that describes the provisioned resources that certain users have. The reviewer can attest to the accuracy of the entitlements by providing a response. This attestation action, along with the response the reviewer provided, any associated comments, and an audit view of the data that the reviewer viewed and attested to, is tracked and audited to provide a complete trail of accountability. Reviewer actions can optionally trigger corrective action by configuring the workflow engine of Oracle Identity Manager. In Oracle Identity Manager, this process is known as an attestation task.

Security Attribute Maintenance

Users are allocated a user ID and a password for use when logging in to Oracle Identity Manager. In the evaluated configuration, users can change their passwords once they have logged in. If their password has expired they will be requested to supply a new password. Any passwords that a user creates must conform to the relevant password policy.

The use of Oracle Identity Manager's Administrative Console to create and maintain user account data, access policy data and audit data depends on the privileges held by the user requesting access.

Groups

Administrators use user groups to create and manage the records of a collection of users to whom they want to permit access to common functionality, such as access rights or permissions.

User groups can be independent of an organization, span multiple organizations, or contain users from a single organization. Oracle Identity Manager provides three default user groups:

- System Administrators;
- Operators;

- All Users.

Members of the system administrators user group have full permission to create, edit, and delete records in Oracle Identity Manager, except for system records. These users can control the permissions of other users, change the status of process tasks even when the task is not assigned to them, and administer the system from the highest level.

Members of the Operators user group have access to the Organizations, Users, and Task List forms. These users can perform a subset of functions on these forms.

Members of the All Users user group have minimal permissions, including the ability to access the user's own user record. By default, each user belongs to the All Users user group.

The permissions associated with the default user groups can be modified.

Reconciliation Dataflow

In a trusted source reconciliation run, newly created users on the target system are reconciled into Oracle Identity Manager. In other words, the target system acts as the trusted source for information about new users. Trusted source reconciliation also involves the reconciliation of changes to user records that already exist in both the target system and Oracle Identity Manager.

Audit and Accountability

OIM sends audit records for events to a log file using log4j. Audit levels are set in the file `OIM_HOME\xellerate\config\log.properties`, which contains a general setting along with specific settings for the components and modules that comprise Oracle Identity Manager.

Other Oracle Identity Manager Security Features

In addition to the security features described above, Oracle Identity Manager provides features which are related to security but are not reflected in the functional requirements identified in Chapter 5 of this document. These features provide significant security capabilities to support robust and reliable identity management systems.

The features described below are **not** within the scope of this evaluation and the SFRs covered in Chapter 5 are not dependent on these features.

Design Console

The Design Console provides the full range of the Oracle Identity Manager system configuration and development capabilities, including Form Designer, Workflow Designer, and the Adapter Factory. The Design Console is accessed by using a desktop Java client. Only users with the role “end-user admin” can login to the Design Console. The use with the TOE of adapters that are not included as part of the TOE’s evaluated configuration, but which have been developed separately using the Adapter Factory, are not within the scope of this evaluation.

Remote Manager

The Remote Manager is an Oracle Identity Manager server component that runs on a target system computer. It provides the network and security layer required to inte-

grate with applications that do not have network-aware APIs or do not provide security.

SPML Interface

The SPML Web Service to OIM is an interface for inbound SPML-based provisioning requests. It supports the creation, modification, deletion, and lookup of Oracle Identity Manager users, user groups, and organizations. It also provides features for managing references (such as assignment and revocation of group memberships), resetting user passwords, and disabling and reenabling user accounts.

Predefined Generic Technology Connector Providers

The predefined providers described in [OIMAG, 20] are shipped with Oracle Identity Manager. These providers are the Shared Drive Reconciliation Transport Provider, the CSV Reconciliation Format Provider, the SPML Provisioning Format Provider, the Web Services Provisioning Transport Provider, the Transformation Providers and the Validation Providers.

This Page Intentionally Blank

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 provisioning actions by Oracle Identity Manager (OIM). The data items used by the TOE in managing the security of the resources are also to be protected.

The primary IT assets to be protected are:

- *Resources provisioned to users* via access policies set up and maintained by the TOE.

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

- *TOE data objects,* which are objects that are associated with operations that the TOE can perform.
- *Security attributes,* which are held in a relational database accessed by OIM.
- *Configuration files,* which are held in filestore to govern the way the TOE products operate.
- *Audit data* generated by the TOE during its operation.

Operational Environment

In the operational environment for the TOE, there is a need for the IT environment and suitable physical and procedural controls to be deployed in a way that assists the TOE in providing protection against attacks against the IT assets, the TOE, its underlying system and the network that it is connected to.

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 application servers and/or network services and/or custom software);
- *Users* who are capable of making requests to access resources provisioned to users through the TOE;
- *System Users* who are persons authorized to use 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.ACCESS *Unauthorized Access to the TOE.* An outsider, user or system user obtains unauthorized access to TOE data objects or security attributes via a TOE interface.

Note that this threat includes an outsider or system user accessing TOE data objects or security attributes for which they are not authorized by impersonating a user who is authorized for such access.

T.RESOURCES *Unauthorized Access to Resources.* A user obtains unauthorized access to resources via a TOE interface.

Note that this threat includes a user accessing resources for which they are not authorized by impersonating another user who is authorized for such access.

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 OIM.

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 occurring 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 occurring, or IT assets being placed at risk, as a result of actions taken by authorized users. For example, a user may grant administrator access to a group they are an administrator for to another user who is able to use this privilege to gain access to resources 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 than via a TOE interface.

Note that this threat includes the use of the IT Environment to directly modify the contents of files or the database used by the TOE in order to gain unauthorized access to IT assets.

TE.CRASH *Abrupt Interruptions.* Abrupt interruptions to the operation of the TOE may cause IT assets 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.PROVISION Users will be provisioned with appropriate resources for their duties and responsibilities within their organization.

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 operational documentation.

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 database systems and/or application servers and/or 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 TOE data objects and TOE security attributes.

Note that users access a TOE security attribute by gaining access to an appropriate TOE data object.

O.RESOURCES The TOE must prevent unauthorized access to resources via a provisioning request to the TOE and must ensure that users are only provisioned with appropriate resources for their duties and responsibilities within their organization.

O.RECON The TOE must ensure that TOE data updated during reconciliation is properly associated with the corresponding data already held by the TOE.

O.I&A The TOE must provide the means of identifying and authenticating users of the TOE. Users that do not identify themselves can be given sessions with the TOE allowing self-registration requests to be submitted and tracked.

O.AUDIT The TOE must provide the means of recording security relevant events in sufficient detail to help an administra-

tor 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 users accountable for any actions they perform that are relevant to the security of the TOE.

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.

Operational Environment

In the evaluated configuration defined in [ECG], 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, [ECG] will require 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 next section.

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 and the underlying application server's functions must include auditing of the startup and shutdown of the TOE's server application.

OE.AUDIT The underlying system must maintain a protected audit trail for the TOE so that administrators can use file editor software in the system to query it to detect and investigate security incidents. In addition, 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 and the underlying application server's functions must include auditing of the startup and shutdown of the TOE's server application.

OE.FILES The underlying system must provide access control mech-

anisms 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 TOE-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 [ECG], 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 [ECG] 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. Examples of such actions are the setting of restrictive permissions on operating system files and the setting of policies to ensure the use of strong passwords by users.

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 server 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 an administrator for the system underlying the TOE 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 administrators shall be distributed in a secure manner;

d) The network of computers that includes the TOE will be installed and maintained as specified in [ECG] 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 purpose unrelated to the TOE.

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.

This Page Intentionally Blank

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 characters used for these assignment, selection and refinement operations are 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 TOE 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_UID.1.1	Timing of Identification	X			
FIA_UID.1.2	Timing of Identification				
FIA_UAU.1.1	Timing of Authentication	X			
FIA_UAU.1.2	Timing of Authentication				

Element	Name	A	S	R	I
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			
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 "Access Control SFPs":				
FDP_ACC.1.1	Subset Access Control	X		X	X
FDP_ACF.1.1	Security Attribute Based Access Control	X			X
FDP_ACF.1.2	Security Attribute Based Access Control	X			X
FDP_ACF.1.3	Security Attribute Based Access Control	X			X
FDP_ACF.1.4	Security Attribute Based Access Control	X			X
FDP_ETC.2.1	Export of user data with security attributes	X		X	
FDP_ETC.2.2	Export of user data with security attributes				
FDP_ETC.2.3	Export of user data with security attributes				
FDP_ETC.2.4	Export of user data with security attributes	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		X
FMT_MSA.3.2	Static Attribute Initialisation	X			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				
FPT_TDC.1.1	Inter-TSF Basic TSF Data Consistency	X			
FPT_TDC.1.2	Inter-TSF Basic TSF Data Consistency	X			
	SFRs under the heading "Security Audit":				
FAU_GEN.1T.1	Audit Data Generation		X	X	
FAU_GEN.1T.2	Audit Data Generation	X		X	

Element	Name	A	S	R	I
FAU_GEN.2.1	User Identity Association				
FAU_SEL.1.1	Selective Audit	X	X		

Identification and Authentication

The TOE SFRs under class FIA in this Security Target relate to the identification and authentication of TOE users. 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_UID.1.1 The TSF shall allow:

a) REQUESTS FOR SELF-REGISTRATION; AND
b) TRACKING OF SELF-REGISTRATION REQUESTS.
on behalf of the user to be performed before the user is identified.

Note that tracking of self-registration requests covers the ability to see the stage reached by the approval process for the request, but the approval process itself cannot be performed by an unauthenticated user.

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_UAU.1.1 The TSF shall allow:

a) REQUESTS FOR SELF-REGISTRATION; AND
b) TRACKING OF SELF-REGISTRATION REQUESTS.
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_AFL.1.1 The TSF shall detect when *AN ADMINISTRATOR CONFIGURABLE POSITIVE INTEGER WITHIN THE RANGE 1 TO* 10^{80}*-1* unsuccessful authentication attempts occur related to *CONSECUTIVE INSTANCES OF A USER ATTEMPTING TO LOGIN.*

Note that an administrator can set the maximum number of unsuccessful login retry attempts to be any positive integer up to 10^{80}*-1, which is effectively no practical limit. [ECG], however, 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) *USER AUTHENTICATION DATA;*
c) *USER ACCOUNT DATA;*
d) *GROUP MEMBERSHIPS.*

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

Note that the metrics to be met by the secrets are defined in Security Function SA.CHPWD in Chapter 6 and in [ECG] to ensure that a minimum strength of function for the TOE of SOF-High is achieved. The TOE implements more controls on user passwords than are covered in this SF and [ECG], but these additional controls are not needed to achieve the required minimum strength of function. An administrator uses the OIM Design Console outside of the TOE's operational state to configure such controls

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

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

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 IN WHICH THE USER HAS AUTHENTICATED SUCCESSFULLY, THE USER IDENTIFIER WILL BE ASSOCIATED WITH EACH SUBJECT ACTING ON BEHALF OF THAT USER;*
b) *ANY GROUP MEMBERSHIPS HELD BY THE USER WILL BE ACCESSIBLE TO 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) *IF A USER'S IDENTIFIER OR GROUP MEMBERSHIP CHANGES, THEN THIS CHANGE IS IMMEDIATELY ASSOCIATED WITH ANY SUBJECT ACTING ON BEHALF OF THE USER;*
b) *ANY CHANGES TO THE VALUES OF THE OTHER USER SECURITY ATTRIBUTES DO NOT AFFECT THE USER'S CURRENT SESSION WITH THE TSF.*

Access Control SFPs

The TOE SFRs under class FDP in this Security Target relate to the TOE Access Control SFP and the Provisioning Access Control SFP. The TOE Access Control SFP controls the ability of users to access TOE features. The Provisioning Access Control SFP controls the provisioning of resources to users.

TOE Access Control

FDP_ACC.1.1A The TSF shall enforce the *TOE ACCESS CONTROL SFP BASED* on:

a) *USERS*;
b) *TOE DATA OBJECTS; AND*
c) *OPERATIONS BY USERS ON TOE DATA OBJECTS.*

Note that a refinement has been applied to replace "on" by "based on" as the SFP does not operate <u>on</u> users, objects and operations. The SFP's access control decisions are actually <u>based on</u> users, objects and operations.

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

a) *THE USER IDENTIFIER AND GROUP MEMBERSHIPS ASSOCIATED WITH THE USER; AND*

b) *ACCESS PERMISSIONS FOR THE REQUESTED TYPE OF OPERATION ON THAT DATA OBJECT THAT ARE ASSOCIATED WITH THE GROUPS THAT THE USER IS A MEMBER OF.*

Note that the "group" concept used in this SFR relates to a collection of one or more OIM users and does not relate to the "group" concept in any operating system.

FDP_ACF.1.2A The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) *THE USER IS GRANTED ACCESS TO THE DATA OBJECT UNDER THE TOE ACCESS CONTROL SFP ONLY IF THERE IS AN ACCESS PERMISSION FOR THE REQUESTED TYPE OF OPERATION ON THAT DATA OBJECT ASSOCIATED WITH THE GROUPS OF WHICH THE USER IS A MEMBER,*
OR IF THE USER IS A MEMBER OF AN ADMINISTRATIVE GROUP THAT HAS THE RIGHT TO PERFORM THE OPERATION ON THE DATA OBJECT
OR IF THE DATA OBJECT DOES NOT REQUIRE EXPLICIT PERMISSION FOR ITS ACCESS.

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

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

Provisioning Access Control

FDP_ACC.1.1B The TSF shall enforce the *PROVISIONING ACCESS CONTROL SFP BASED* on:

a) *USERS*;
b) *RESOURCES; AND*
c) *THE PROVISIONING OF RESOURCES TO USERS.*

Note that a refinement has been applied to replace "on" by "based on" as the SFP does not operate <u>on</u> users, objects and operations. The SFP's access control decisions are actually <u>based on</u> users, objects and operations.

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

a) *THE USER IDENTIFIER AND GROUP MEMBERSHIPS ASSOCIATED WITH THE USER; AND*
b) *ACCESS POLICIES THAT APPLY TO THE RESOURCE.*

Note that the "group" concept used in this SFR relates to a collection of one or more OIM users and does not relate to the "group" concept in any operating system.

Note also that FDP_ACC.1.1B and FDP_ACF.1.1B provide lists of items operated on by the rules covering the provisioning processes that are in FDP_ACF.1.2B.

FDP_ACF.1.2B The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) *A USER IS ALLOWED TO BE PROVISIONED TO A RESOURCE IF AN ACCESS POLICY OF TYPE "WITHOUT APPROVAL" THAT APPLIES TO THE RESOURCE EXISTS, FOR WHICH THE USER IS A MEMBER OF A GROUP LISTED*

IN THE POLICY AND THE RESOURCE IS SPECIFIED FOR PROVISIONING TO USERS IN THIS GROUP;

b) *A USER IS ALLOWED TO BE PROVISIONED TO A RESOURCE IF AN ACCESS POLICY OF TYPE "WITH APPROVAL" THAT APPLIES TO THE RESOURCE EXISTS, FOR WHICH THE USER IS A MEMBER OF A GROUP LISTED IN THE POLICY AND THE RESOURCE IS SPECIFIED FOR PROVISIONING TO USERS IN THIS GROUP AND THE REQUEST FOR PROVISIONING HAS BEEN APPROVED;*

c) *A USER IS ALLOWED TO BE PROVISIONED TO A RESOURCE ONLY IF SUCH PROVISIONING IS GRANTED VIA a) OR b) ABOVE;*

d) *WHEN A USER IS ADDED TO OR REMOVED FROM MEMBERSHIP OF A GROUP, THE ACCESS POLICIES THAT APPLY TO THAT GROUP ARE CHECKED TO SEE IF USERS SHOULD BE PROVISIONED OR DEPROVISIONED TO RESOURCES;*

e) *WHEN THE DEFINITION OF AN ACCESS POLICY IS CHANGED OR ACCESS POLICY DATA IS CHANGED, THE ACCESS POLICY IS CHECKED TO SEE IF USERS SHOULD BE PROVISIONED OR DEPROVISIONED TO RESOURCES;*

f) *WHEN A PROVISIONING PROCESS CAUSES AN ATTESTATION PROCESS TO TAKE PLACE, A REPORT IS PRODUCED SO THAT THE REVIEWER CAN ENSURE THE USERS MENTIONED IN THE REPORT ONLY HAVE RESOURCES PROVISIONED FOR THEM THAT ARE NECESSARY FOR THEIR DUTIES AND RESPONSIBILITIES.*

FDP_ACF.1.3B The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

a) *A USER IS ALLOWED TO BE PROVISIONED TO A RESOURCE IF A REQUEST FOR SUCH PROVISIONING HAS BEEN MADE AND HAS BEEN APPROVED;*

b) *A SUITABLY AUTHORIZED ADMINISTRATOR CAN CAUSE A USER TO BE PROVISIONED TO A RESOURCE WITHOUT HAVING TO OBTAIN ANY APPROVALS.*

Note that FDP_ACF.1.3B covers the ability for users to be provisioned to resources without the need for an applicable access policy.

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

FDP_ETC.2.1 The TSF shall enforce the *PROVISIONING ACCESS CONTROL SFP* when exporting user data, controlled under the SFP, outside of the TSC.

Note that a refinement has been applied to the above SFR to change "SFP(s)" to "SFP" for the sake of clarity, because only one of the two SFPs is covered by it.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC:

a) *A CONNECTOR THAT IS PART OF THE TSF MUST BE USED TO EXPORT THE DATA FOR USE IN PROVISIONING A USER TO A RESOURCE.*

Note that the export of user data during provisioning would typically be associated with the setting up of an account on a remote service for a user to use an IT resource.

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.

FMT_MSA.1.1 The TSF shall enforce the *TOE ACCESS CONTROL SFP* to restrict the ability to QUERY, *MODIFY, DELETE, CREATE* the security attributes
USER IDENTIFIER, USER AUTHENTICATION DATA, USER ACCOUNT DATA AND GROUP MEMBERSHIPS FOR USERS, AND
ACCESS PERMISSIONS ASSOCIATED WITH GROUPS, AND
ACCESS POLICIES APPLYING TO RESOURCES
to *SUITABLY AUTHORIZED USERS.*

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

FMT_MSA.3.1B The TSF shall enforce the *PROVISIONING 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.

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

Note that the above SFR relates to the TOE ACCESS CONTROL SFP.

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

Note that the above SFR relates to the PROVISIONING ACCESS CONTROL SFP.

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

a) *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 users are authorized to perform TOE operations via the permissions associated with groups that they are members of. Thus an authorized administrator is

a user that is a member of groups with the necessary permissions to perform administrative duties. Some groups are classified as administrative groups and hence users that are members of such groups are automatically administrators.

Note also that "security management role" is a Common Criteria term and that SFR FMT_SMR.1 is used to state requirements for the security management roles that are to be used for the TSF. The roles listed in the SFR include those identified in the FMT SFRs that depend on FMT_SMR.1.

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

Protection of the TSF

The TOE SFRs in this section relate to the integrity and management of the mechanisms that provide the TSF and to the integrity of TSF data.

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.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *USER SECURITY ATTRIBUTE VALUES* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *THE FOLLOWING INTERPRETATION RULES*:

a) *IN A TRUSTED SOURCE RECONCILIATION RUN, THE TARGET SYSTEM ACTS AS THE TRUSTED SOURCE FOR INFORMATION ABOUT USERS THAT ARE NEW TO OIM AND THESE USERS ARE AUTOMATICALLY CREATED AS USERS FOR OIM.*

b) *IF RECORDS ALREADY EXIST IN BOTH THE TARGET SYSTEM AND OIM FOR A PARTICULAR USER, TRUSTED SOURCE RECONCILIATION IS TO CAUSE CHANGES TO THE OIM USER'S SECURITY ATTRIBUTE VALUES IF IT IS NECESSARY TO MAKE OIM'S AND THE TARGET SYSTEM'S INFORMATION ABOUT THIS USER CONSISTENT.*

when interpreting the TSF data from another trusted IT product.

Security Audit

The TOE SFRs under class FAU in this Security Target relate to the generation of audit data for security relevant TOE events. Note that such audit data results from the TOE's features for the logging of audit records that can be used by administrators to check for actual or potential violations of the TOE's security policy. Oracle Identity Manager also provides features for use by an enterprise's auditors, but these features are outside the scope of this evaluation.

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 selection operation for the FAU_GEN.1T.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
FIA_UID.1	Unsuccessful use of the user identification mechanism	None
FIA_UAU.1	Unsuccessful use of the authentication mechanism	None
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
FDP_ACF.1	Unsuccessful requests to perform an operation on an object covered by the SFP	Object identifier, requested access
FDP_ETC.2	Unsuccessful export of information	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_SMF.1	Use of the Management Functions	None
FMT_SMR.1	Modifications to the group of users that are part of a role	None
FPT_TDC.1	Use of the TSF data consistency mechanisms	None

Note that the FAU_GEN.1.1 element defined in Section 3.2 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. However, auditing takes place according to the value of the logging level throughout the time when the OIM server application is running. To cater for this, FAU_GEN.1 has been extended as a requirement for this TOE. This extended component has been designated as FAU_GEN.IT. The Security Requirements for the IT Environment defined later in this Chapter include the requirement FAU_GEN.1E.2 for the IT Environment to be able to generate an audit record for the start-up and shutdown of the OIM server application (during which any audit records generated by the TOE are stored in logging files). This requirement therefore satisfies the need for the TOE administrator to know the periods of time during which audit records could have been written to the TOE's audit trail.

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) *OTHER AUDIT RELEVANT INFORMATION AS IDENTIFIED IN TABLE 2 ABOVE*.

Note that a refinement has been applied to the above SFR to omit the words "For each audit event type, based on the auditable event definitions of the functional components included in the SECURITY TARGET AND" for the sake of clarity. Apart from this refinement, FAU_GEN.1T.2 is identical to FAU_GEN.1.2.

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_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type.

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 provisioning control system that uses an Oracle database to hold its security attributes. 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 a TOE interface.
- 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 high-

lighted 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_GEN.1E.1	Audit Data Generation		X	X	
FAU_GEN.1E.2	Audit Data Generation	X		X	
FAU_SAR.1E.1	Audit Review	X		X	
FAU_SAR.1E.2	Audit Review			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 logging properties file holding the definition of the audit level and the audit trail files that hold the audit records generated by the TSF, 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.1A The *IT ENVIRONMENT* shall restrict the ability to *MODIFY* the *AUDIT LEVEL FOR AUDITABLE EVENTS* to *SUITABLY AUTHORIZED ADMINISTRATORS.*

Note that the logging properties file that is used to set the audit level is to be protected by operating system DAC permissions to ensure that only administrators can access it.

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

Note that the audit trail files that hold the audit records generated by the TSF are to be protected by operating system DAC permissions to ensure that only administrators can access them.

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

a) *MODIFY THE AUDIT LEVEL FOR AUDITABLE EVENTS;*

b) *QUERY, CLEAR THE AUDIT TRAIL.*

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

Note also that the features in the IT Environment providing the security management functions listed above are file editors (which can edit items in the logging properties file holding the definition of the audit level and can view and edit the audit trail files).

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 TSF* 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.1E.1 satisfies the dependency of the SFR FAU_GEN.1T.2 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. The SFRs for the IT environment in this section cover the capability to generate audit records for the start-up and shutdown of the OIM server application and to review and protect the audit data generated into the audit trail by the TSF.

FAU_GEN.1E.1 The *IT ENVIRONMENT* shall be able to generate an audit record of the following auditable event:

a) start-up and shutdown of the *TSF'S SERVER APPLICATION*.

FAU_GEN.1E.2 The *IT ENVIRONMENT* 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) *NO OTHER AUDIT RELEVANT INFORMATION*.

Note that FAU_GEN.1T.1, FAU_GEN.1T.2, FAU_GEN.1E.1 and FAU_GEN.1E.2 together meet the requirements of the FAU_GEN.1 component defined in Section 3.2 of [CC] Part 2.

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

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

FAU_STG.1E.1 The *IT ENVIRONMENT* shall protect the stored audit records from unauthorized deletion.

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

Note that file editors and the operating system provide the software in the IT Environment to read and protect the files holding the audit records.

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, access control, security attributes and auditing.

In the TOE's evaluated configuration, the TOE security attributes are held using an Oracle Database.

User Identification and Authentication

IA.PRELOGIN The Oracle Identity Manager Welcome page allows users to submit and track self-registration requests without having to login, provided that such features have been configured for use.

Note that an end-user administrator uses the OIM Design Console outside of the TOE's operational state to configure the features for use via the Oracle Identity Manager Welcome page.

Note also that, in the evaluated configuration, users cannot change their passwords by using the self-service capabilities of the Oracle Identity Manager Welcome page.

IA.LOGIN When requesting to login to the TOE, OIM users supply their user ID and password to the Administrative and User Console.

Provided the user ID and password are valid and the user's account has not been locked, the user is granted access to the Administrative and User features of OIM.
If the supplied password is incorrect, the OIM user's account becomes locked if the user has exceeded the maximum number of login retry attempts.
If the correct password is supplied, but it is invalid because the Expires After Days value in the relevant password policy has

been exceeded, then the user will only be granted access after successfully supplying a new password conforming to the rules of the relevant password policy.

Note that authorisation and session management are handled by the Application Server. The authentication (checking of offered password against the known good password, stored in the database) is performed by the Login module supplied by OIM.

Note also that an administrator uses the OIM Design Console outside of the TOE's operational state to set the maximum number of login retry attempts. [ECG] defines a specific value to be used in the TOE's evaluated configuration.

IA.CHANGEPWD When an OIM user's password for use with SF IA.LOGIN is to be created or changed, the password policies configured for the Xellerate Users resource are applied.

Note that the Xellerate Users resource represents the set of accounts by which users gain access to OIM. There is an Xellerate User object to hold each OIM user's account data. Users can only make changes to passwords once they have logged in to the TOE or if the login process has found that their password has expired. This is because, in the evaluated configuration, the TOE is configured to prevent users changing their passwords by using the self-service capabilities of Oracle Identity Manager.

Note also that an end-user administrator uses the OIM Design Console outside of the TOE's operational state to configure password policies.

TOE Access Control

TAC.POL When an OIM user attempts to perform an operation on a TOE data object, the TOE grants access according to:

a) the user ID and group memberships associated with the OIM user and

b) the access permissions for the requested type of operation on that data object that are associated with the groups for which the user is a member.

Note that the members of administrative groups have access rights in addition to those resulting from permissions associated with the groups for which they are members (see [OIMAG, 10: Data Object Permissions]).

Provisioning Access Control

PAC.POL The TOE provisions or deprovisions resources for an OIM user according to the groups for which the user is a member and the access policies that apply to these groups (where an access policy is a list of user groups and the resources with which users in the group are to be provisioned or deprovisioned). If an access policy of type "with approval" is applicable to a user and if the access policy specifies that resources are to be provisioned, then OIM generates a request. This request must be approved before the resources are provisioned to the user. If an access policy of type "without approval" is applied to a user, then, whenever an access policy is applied, the resources are directly provisioned to the user without any request being generated.

Note that the approval process for requests is covered in [OIMAG, 1: Approval Processes].

PAC.EVALPOL The TOE evaluates access policies when a user is made a part of a group or is removed from a group, in which case the access

policy for the user is evaluated as part of the add or remove operation.

In addition, OIM evaluates access policies during a run of the Set User Provisioned Date schedule task if one or more of the following events have occurred since the last run of the Set User Provisioned Date schedule task:

a) The access policy definition is updated so that the retrofit flag is set to ON, in which case the access policy is evaluated for all applicable users.

b) A group is added or removed from an access policy definition, for which the retrofit flag is set to ON, in which case the access policy is evaluated only for users that are members of the group that is added or removed.

c) A resource is added, removed, or the Revoke If No Longer Applies flag value is changed for a resource, in which case the access policies for which the retrofit flag is set to ON are evaluated for all applicable users.

d) Access policy data is updated or deleted (including both parent and child form data) for an access policy for which the retrofit flag is set to ON, in which case the access policy is evaluated for all applicable users.

PAC.PROVISION When a resource is to be provisioned to a user as a result of the processes specified in SF PAC.POL and PAC.REQPRV, or as a result of users created via a reconciliation run as per SA.RECONCILE, a provisioning process is used to undertake a series of automated tasks that perform the steps necessary to grant access to the resource. During the provisioning process, depending on the configuration, some of the user's security attribute values may be exported from the TOE by a connector that is part of the TOE along with other user data held by the TOE to enable the user to access the resource. Such user security attributes are to be linked to the associated user data.

An example of such an export would be if the user ID and password were used when setting up an account for the user to access an IT resource such as an operating system. In such a case, OIM would need to use an an account on that system that has privileges to create, amend and delete other accounts.

PAC.REQPRV A request can be made for a resource to be provisioned to a user without the need for an applicable access policy. Such requests can be created by an administrator with the necessary permissions or, if the resource is so configured, by users themselves. Approval workflows for the request are started after the request is submitted and provisioning of the approved account profile is started after the approval is completed.

PAC.DIRECTPRV An administrator with the necessary permissions can directly authorize the provisioning of a resource for a particular user on a target system without having to obtain any approvals.

PAC.ATTEST The TOE provides automated attestation report generation, delivery, and notification so that the nominated attestation

reviewers can check the report to make sure that the OIM users mentioned only have resources provisioned for them that are necessary for their duties and responsibilities. Reviewer actions can optionally trigger corrective action by configuring Oracle Identity Manager's workflow engine. Attestation activity can be initiated on a periodic basis or when required.

Security Attributes

SA.UATT The OIM user security attributes maintained by the TOE are:

a) user ID;

b) password;

c) OIM account status data;

d) group memberships.

SA.CHPWD The TOE applies the following checks, which are held in the relevant password policies, when an OIM user's password is to be updated:

a) the minimum number of characters that the password must contain;

b) the minimum number of alphabetic characters that the password must contain;

c) the minimum number of upper-case characters that the password must contain;

d) the minimum number of lower-case characters that the password must contain;

e) the minimum number of non-alphanumeric characters that the password must contain;

f) the minimum number of numeric characters that the password must contain;

g) if the password policy specifies a password reuse constraint and the user attempts to reuse a password, the TOE rejects the change if the reuse constraint is not met.

Note also that the TOE implements more controls on user passwords than are listed in the above SF. An administrator uses the OIM Design Console outside of the TOE's operational state to configure such controls.

SA.UEFF At the start of an OIM user's session with the TOE, the values of the user's security attributes defined in SF SA.UATT are associated with the session. Any changes to the user ID and to group memberships will immediately be applied to the session. Any changes to the other security attributes will be effective the next time that the OIM user logs in to the TOE.

SA.RECONCILE In a trusted source reconciliation run, if OIM detects new target system accounts, then it automatically creates these users as new OIM users (if this is defined in the action rules). If OIM detects changes to target system accounts for existing OIM users, then these changes are also made for the corresponding OIM Users.

SA.CRUSER Accounts for users to access the TOE can be created by administrators or via self-registration by OIM users with suitable access permissions (if this feature has been configured) or via data supplied by a trusted source reconciliation run (as per SF SA.RECONCILE). Users are created with a unique user ID. There is no default password for a newly created user, except if the user is created through reconciliation, when the password is initially set to the value of the user's name in the source system. Each password must be manually configured to a secure value by an administrator on completion of reconciliation.

Note that OIM users are classified as end-users or end-user administrators. Only end-user administrators can use the OIM Design Console outside of the TOE's operational state to configure the TOE's operation. OIM users are authorized to perform TOE operations via the permissions associated with groups of which they are members. Thus an OIM administrator is a user that is a member of groups with the necessary permissions to perform administrative duties. Some groups are classified as administrative groups and hence users that are members of such groups are automatically administrators.

Note also that, when an OIM user account is created, a password must be supplied for the user that satisfies the relevant password policies. The exception to this is if the user is created through reconciliation. In this case, even in the evaluated configuration, the password is initially set to the value of the user's cn attribute in the source OID system. Each password must be manually configured to a secure value by an administrator on completion of reconciliation as specified in [ECG, J.3.5].

SA.DEFTACATT When a new group is created, it has no access permissions associated with it unless these permissions were granted during the process of creating the group.

SA.DEFPACATT When a new access policy is created, it has no resources associated with it unless the resources were associated during the process of creating the access policy.

Audit and Accountability

AA.INF Depending on the settings in the logging properties file, for every occurrence of an auditable event the TOE will write an audit record to the audit log which holds at least the following information:

a) date and time of the audit event;

b) the category name for the event;

c) the user ID (if a specific user caused the event);

d) whether the event represented a success or failure;

e) the object ID (if a specific object was being acted on).

Note that this SF relates to the generation of audit data for security relevant TOE events via the TOE's features for the logging of audit records that can be used by administrators to check for actual or potential violations of the TOE's security policy. The auditable events referred to in this SF are those listed in Table 2 of Chapter 5. Oracle Identity Manager also provides features for use by an enterprise's auditors,which are summarised in the "Audit" section of Chapter 2, but these features are outside the scope of this evaluation

Note also that, in the evaluated configuration, the logging properties file and the audit log files are to be protected by operating system DAC permissions to ensure that only administrators can access them. The logging properties file is described in [OIMIC, 7: Setting Log Levels].

Security Mechanisms and Techniques

A password is used for authentication of TOE users. The TOE password management functions (together called the PWD mechanism), when combined with the instructions to administrators that will be included in [ECG] to choose strong password policies, provide a Strength of Function level of *SOF-high.*

Specific SFs supporting the claimed SOF are:

- IA.LOGIN (SOF-High); *and*
- IA.CHANGEPWD, SA.UATT and SA.CHPWD, which support IA.LOGIN 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.
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.

Table 4: TOE Assurance Measures

Component	Name	Documents
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

This 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.RESOURCES	O.RECON	O.AUDIT	O.ADMIN
T.ACCESS	YES	YES		YES		YES
T.RESOURCES	YES		YES	YES		YES
T.ATTACK	YES				YES	
T.ABUSE.USER	YES				YES	
P.PROVISION	YES		YES	YES		YES
P.ACCOUNT	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			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.ACCESS, T.RESOURCES	P.PROVISION	A.MANAGE, A.ACCESS
OE.MEDIA	TE.CRASH		A.MANAGE
OE.AUDIT	T.ATTACK, T.ABUSE.USER	P.ACCOUNT	A.MANAGE
OE.ADMIN	T.ATTACK	P.ACCOUNT	A.MANAGE, A.ACCESS
OE.FILES	T.ACCESS, T.RESOURCES, T.ATTACK, T.ABUSE.USER, TE.ACCESS	P.ACCOUNT, P.PROVISION	A.MANAGE
OE.SEP	T.ACCESS, T.RESOURCES, T.ATTACK	P.ACCOUNT, P.PROVISION	A.MANAGE

T.ACCESS Rationale

T.ACCESS (*Unauthorized Access to the TOE)* is directly countered by O.ACCESS, which ensures the TOE can protect the TOE's features and security attributes from unauthorized access. O.I&A gives support by providing the means of identifying the user attempting to access the TOE so that access controls can be based on the user's identity. O.ADMIN provides support by ensuring that only authorized administrators can use TOE management functions to affect the operation of access controls on the TOE. O.RECON ensures that TOE data updated during reconciliation is properly associated with the corresponding data already existent in the TOE repository in case such a reconciliation led to a person erroneously being given an account by which they could gain unauthorized access to the TOE. OE.FILES prevents unauthorized people gaining direct access to configuration files and files holding security attributes and TOE-related database tables to enable the circumvention of access controls on the TOE. OE.AUTHDATA ensures that user authentication data is held securely to stop it being used by people to masquerade as authorized users to gain unauthorized access to 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 the TOE.

T.RESOURCES Rationale

T.RESOURCES (*Unauthorized Access to Resources)* is directly countered by O.RESOURCES, which ensures the TOE can prevent unauthorized access to resources via a provisioning request to the TOE. O.I&A gives support by providing the means of identifying the user attempting to be provisioned with the resource so that access controls can be based on the user's identity. O.ADMIN provides support by ensuring that

only authorized administrators can use TOE management functions to affect the operation of the TOE's provisioning access controls. O.RECON ensures that TOE data updated during reconciliation is properly associated with the corresponding data already existent in the TOE repository in case such a reconciliation led to a user erroneously being given unauthorized access to resources. OE.FILES prevents unauthorized users gaining direct access to configuration files and files holding security attributes and TOE-related database tables to enable the circumvention of the TOE's provisioning access controls. 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 a provisioning request to 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 via a provisioning request to the TOE.

T.ATTACK Rationale

T.ATTACK (*Undetected Attack)* is countered directly by O.AUDIT and OE.AUDIT 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 that is appropriate to the audit event. 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 the logging properties file and files holding audit data to disable auditing or 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 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 and OE.AUDIT 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. 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 audit event. OE.FILES provides support by preventing users gaining direct access to the logging properties file and files holding audit data to disable auditing or 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 configuration files, files holding security attributes and TOE-related database tables, and audit trail files. 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.CRASH Rationale

TE.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.PROVISION Rationale

P.PROVISION is satisfied by O.RESOURCES, which ensures that users are only provisioned with appropriate resources for their duties and responsibilities within their organization. O.I&A gives support by providing the means of identifying the user attempting to be provisioned with the resource. O.ADMIN provides support by ensuring that only authorized administrators can use TOE management functions to affect the operation of the TOE's provisioning access controls and to affect the generation of attestation reports. O.RECON ensures that TOE data updated during reconciliation is properly associated with the corresponding data already existent in the TOE repository in case such a reconciliation led to a user erroneously being given inappropriate access to resources. OE.FILES prevents unauthorized users gaining direct access to configuration files and files holding security attributes and TOE-related database tables to enable the circumvention of the TOE's provisioning access controls and to prevent the generation of attestation reports. 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 a provisioning request to 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 via a provisioning request to the TOE.

P.ACCOUNT Rationale

P.ACCOUNT is satisfied by O.AUDIT and OE.AUDIT 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 that is appropriate to the audit event. 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 the logging properties file and files holding audit data to disable auditing or 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 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 [ECG] 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.RECOVERY, OE.AUTHDATA, OE.MEDIA, OE.ADMIN, OE.AUDIT, OE.FILES 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.RESOURCES	O.RECON	O.AUDIT	O.ADMIN
FIA_UID.1	YES	YES	YES			
FIA_UAU.1	YES					
FIA_AFL.1	YES					
FIA_ATD.1	YES	YES	YES		YES	YES
FIA_SOS.1	YES					
FIA_USB.1	YES	YES	YES			
FDP_ACC.1		YES	YES			
FDP_ACF.1		YES	YES			
FDP_ETC.2			YES			
FMT_MSA.1	YES	YES	YES			YES
FMT_MSA.3	YES	YES	YES			YES
FMT_SMF.1	YES	YES	YES			YES
FMT_SMR.1		YES	YES			YES
FPT_RVM.1		YES	YES			
FPT_TDC.1				YES		
FAU_GEN.1T					YES	
FAU_GEN.2					YES	
FAU_SEL.1					YES	

O.I&A Suitability

O.I&A is directly provided by FIA_UID.1 and FIA_UAU.1, which provide the means of identifying and authenticating users of the TOE. FIA_UID.1 and FIA_UAU.1 ensure that users that do not identify and authenticate themselves can only be given sessions with the TOE allowing self-registration requests to be submitted and tracked. 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 and FMT_SMF.1 specify controls over the modification of these attributes and FIA_USB.1 specifies how the user security at-

tributes are associated with subjects acting on behalf of that user. FIA_SOS.1 provides for quality metrics to be applied when new passwords are chosen for use when a user authenticates.

O.ACCESS Suitability

O.ACCESS is directly provided by FDP_ACC.1.1A which defines the TOE access control policy and FDP_ACF.1.1A, FDP_ACF.1.2A, FDP_ACF.1.3A and FDP_ACF.1.4A which specify the TOE access control rules. 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. FPT_RVM.1 ensures that the TOE 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 TOE access.

O.RESOURCES Suitability

O.ACCESS is directly provided by FDP_ACC.1.1B which defines the provisioning access control policy and FDP_ACF.1.1B, FDP_ACF.1.2B, FDP_ACF.1.3B and FDP_ACF.1.4B which specify the provisioning access control rules. FDP_ACF.1 includes a rule ensuring that the appropriateness of the resources to which they are provisioned is checked by people in authority in their organizations. 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. FPT_RVM.1 ensures that the provisioning 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 provisioning access. FDP_ETC.2 ensures that data is correctly exported from the TSF when provisioning a user to a resource.

O.RECON Suitability

O.RECON is directly provided by FPT_TDC.1, which ensures that TOE data updated during reconciliation will be properly associated with the corresponding data already held by the TOE.

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_SEL.1 provides the ability to select which auditable events are to be audited to ensure that administrators only have to search through appropriate material when investigating actual or potential security violations.

O.ADMIN Suitability

O.ADMIN is directly provided by FMT_MSA.1, FMT_MSA.3, 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.AUDIT, 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	OE.FILES	OE.SEP
FMT_MTD.1E	YES	YES		
FMT_SMF.1E	YES	YES		
FPT_SEP.1E				YES
FPT_STM.1E	YES	YES		
FAU_GEN.1E	YES	YES		
FAU_SAR.1E		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 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 and FAU_STG.1E, which provide audit record analysis and management functionality, are mapped to OE.AUDIT. Also mapped to OE.AUDIT are FPT_STM.1E and FAU_GEN.1E, which cover the provision by the IT environment of reliable time stamps for inclusion in audit records and the requirement that the underlying operating system's functions must include the provision of reliable timestamps for use in audit records and that the underlying application server's functions must include auditing of the startup and shutdown of the TOE's server application.
- FAU_GEN.1E and FPT_STM.1E map to OE.ADMIN, which includes requirements on the underlying application server and operating system for the support of auditing functions. OE.ADMIN's requirements for auditing correspond to the requirements defined in FAU_GEN.1E and FPT_STM.1E.
- FMT_STG.1E, which requires that the IT environment protects 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 on the next page 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_UID.1**	-	-
2	**FIA_UAU.1**	FIA_UID.1	1
3	**FIA_AFL.1**	FIA_UAU.1	2
4	**FIA_ATD.1**	-	-
5	**FIA_SOS.1**	-	-
6	**FIA_USB.1**	FIA_ATD.1	4
7	**FDP_ACC.1**	FDP_ACF.1	8
8	**FDP_ACF.1**	FDP_ACC.1 FMT_MSA.3	7 11
9	**FDP_ETC.2**	FDP_ACC.1	7
10	**FMT_MSA.1**	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	7 12 13
11	**FMT_MSA.3**	FMT_MSA.1 FMT_SMR.1	10 13
12	**FMT_SMF.1**	-	-
13	**FMT_SMR.1**	FIA_UID.1	1
14	**FPT_RVM.1**	-	-
15	**FPT_TDC.1**	-	-
16	**FAU_GEN.1T**	FPT_STM.1E	22 See Notes 1, 4 below
17	**FAU_GEN.2**	FAU_GEN.1T FIA_UID.1	16 1
18	**FAU_SEL.1**	FAU_GEN.1T FMT_MTD.1E	16 19

Table 9: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
19	**FMT_MTD.1E**	FMT_SMF.1E FMT_SMR.1	20 13 See Notes 2 and 3 below
20	**FMT_SMF.1E**	-	-
21	**FPT_SEP.1E**	-	-
22	**FPT_STM.1E**	-	-
23	**FAU_GEN.1E**	FPT_STM.1E	22 See Notes 1, 4 below
24	**FAU_SAR.1E**	FAU_GEN.1T	16
25	**FAU_STG.1E**	FAU_GEN.1T	16

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

Note 2: The security requirements for the IT environment FMT_MTD.1E, FMT_SMF.1E, FAU_SAR.1E and FAU_STG.1E cover the IT environment's ability to manage the audit trail.

Note 3: 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.

Note 4: The modification of FAU_GEN.1 does not impact its ability to satisfy the dependencies of FAU_GEN.2, FAU_SAR.1, FAU_SEL.1 and FAU_STG.1 - especially given that collectively the TOE and IT environment meet FAU_GEN.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 and FIA_UAU.1 together with FIA_ATD.1 and FIA_USB.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, FDP_ETC.2, FMT_MSA.1, FMT_SMF.1, FMT_SMR.1, FPT_TDC.1, FAU_GEN.1T, and FAU_GEN.2.

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.

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

FAU_SAR.1E and FAU_STG.1E support FAU_GEN.1T by providing permanent storage for the generated audit records that can be analysed by administrators to detect potential or actual attempts to bypass or tamper with the SFRs.

FMT_MTD.1E and FMT_SMF.1E support FAU_GEN.1T by protecting the integrity of the audit trail that holds the generated audit records.

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_UID.1.1	IA.PRELOGIN	The Oracle Identity Manager Welcome page allows users to submit and track self-registration requests without having to login, provided that such features have been configured for use.
FIA_UID.1.2	IA.LOGIN	IA.LOGIN covers the conditions for the establishment of a session with the TOE. This includes the need for the user to be identitified.
FIA_UAU.1.1	IA.PRELOGIN	The Oracle Identity Manager Welcome page allows users to submit and track self-registration requests without having to login, provided that such features have been configured for use.
FIA_UAU.1.2	IA.LOGIN IA.CHANGEPWD	IA.LOGIN covers the conditions for the establishment of a session with the TOE. This includes the need for the user to be authenticated. The authentication process involves a new password being supplied (as per SF IA.CHANGEPWD) if the current password has expired.
FIA_AFL.1.1	IA.LOGIN	If the supplied password is incorrect, OIM checks if the user has exceeded the maximum number of login retry attempts.
FIA_AFL.1.2	IA.LOGIN	If the supplied password is incorrect, the OIM user's account becomes locked if the user has exceeded the maximum number of login retry attempts.
FIA_ATD.1.1	SA.UATT	The TOE holds the required security attributes for each user.
FIA_SOS.1.1	IA.CHANGEPWD SA.CHPWD	SA.CHPWD specifies the configurable metrics held in the password policy that the TOE checks a password against before it can be allocated to a user (as per IA.CHANGEPWD).
FIA_USB.1.1	SA.UATT SA.UEFF	SA.UEFF states that, at the start of an OIM user's session with the TOE, the values of a user security attribute defined in SF SA.UATT are associated with the session.
FIA_USB.1.2	SA.UATT SA.UEFF	SA.UEFF states that, at the start of an OIM user's session with the TOE, the values of a user security attribute defined in SF SA.UATT are associated with the session.
FIA_USB.1.3	SA.UEFF	SA.UEFF states that any changes to group memberships will immediately be applied to the session. Any changes to the other security attributes will be effective the next time that the OIM user logs in to the TOE.
FDP_ACC.1.1	TAC.POL PAC.POL	FDP_ACC.1.1A: TAC.POL covers the types of user, object and operation information that TOE Access Control is based on. FDP_ACC.1.1B: PAC.POL covers the types of user, object and operation information that Provisioning Access Control is based on.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FDP_ACF.1.1	TAC.POL PAC.POL SA.UATT SA.UEFF	FDP_ACF.1.1A: TAC.POL covers the details of the user, object and operation information that TOE Access Control is based on. SA.UATT covers the user security attributes that are available for TAC.POL to use and SAM.UEFF states the conditions under which these security attributes are effective for a session with the TOE. FDP_ACF.1.1B: PAC.POL covers the details of the user, object and operation information that Provisioning Access Control is based on. SA.UATT covers the user security attributes that are available for PAC.POL to use and SAM.UEFF states the conditions under which these security attributes are effective for a session with the TOE.
FDP_ACF.1.2	TAC.POL PAC.POL PAC.EVALPOL PAC.ATTEST	FDP_ACF.1.2A: TAC.POL covers the rules for TOE Access Control. FDP_ACF.1.2B: PAC.POL covers rules a)-c); PAC.EVALPOL covers rules d)-e); and PAC.ATTEST cover covers rule f) to meet the requirements for Provisioning Access Control.
FDP_ACF.1.3	PAC.REQPRV PAC.DIRECTPRV	FDP_ACF.1.3A does not mandate any functionality. It is included for compliance with the CC. FDP_ACF.1.3B: PAC.REQPRV covers rule a) and PAC.DIRECTPRV covers rule b) to meet the requirements for provisioning without the need for an applicable access policy.
FDP_ACF.1.4	N/A	This SFR does not mandate any functionality. It is included for compliance with the CC.
FDP_ETC.2.1	PAC.PROVISION	When a resource is to be provisioned to a user as a result of the approval process specified in SF PAC.POL, some user data held by the TOE may be exported to enable the user to access the resource.
FDP_ETC.2.2	PAC.PROVISION	When a resource is to be provisioned to a user as a result of the approval process specified in SF PAC.POL, some of the user's security attribute values may be exported from the TOE along with any user data that is exported.
FDP_ETC.2.3	PAC.PROVISION	When a resource is to be provisioned to a user as a result of the approval process specified in SF PAC.POL, some of the user's security attribute values may be exported from the TOE along with any user data that is exported. Such user security attributes are to be linked to the associated user data.
FDP_ETC.2.4	PAC.PROVISION	When a resource is to be provisioned to a user as a result of the approval process specified in SF PAC.POL, some user data held by the TOE may be exported to enable the user to access the resource. Such data must be exported by a connector that is part of the TOE.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FMT_MSA.1.1	TAC.POL SA.CRUSER SA.CHPWD	TAC.POL and SA.CRUSER cover the policy for access to the TOE data objects and for creating OIM user accounts. SA.CHPWD covers the mechanism for updating user passwords.
FMT_MSA.3.1	SA.DEFTACATT SA.DEFPACATT	SA.DEFTACATT and SA.DEFPACATT cover the rules for default security attribute values for use with the TOE Access Control and Provisioning Access Control policies.
FMT_MSA.3.2	SA.DEFTACATT SA.DEFPACATT	SA.DEFTACATT and SA.DEFPACATT cover the rules for initial security attribute values for use with the TOE Access Control and Provisioning Access Control policies.
FMT_SMF.1.1	TAC.POL SA.CRUSER SA.CHPWD	TAC.POL and SA.CRUSER cover the policy for access to the TOE data objects and for creating OIM user accounts. SA.CHPWD covers the mechanism for updating user passwords.
FMT_SMR.1.1	TAC.POL	TAC.POL covers the policy by which users are authorized to perform TOE operations via the permissions associated with groups that they are members of. Thus an authorized administrator is a user that is a member of groups with the necessary permissions to perform administrative duties. Some groups are classified as administrative groups and hence users that are members of such groups are automatically administrators.
FMT_SMR.1.2	TAC.POL	TAC.POL covers the policy by which users are authorized to perform TOE operations via the permissions associated with groups that they are members of. Thus an authorized administrator is a user that is a member of groups with the necessary permissions to perform administrative duties. Some groups are classified as administrative groups and hence users that are members of such groups are automatically administrators.
FPT_RVM.1.1	TAC.POL PAC.POL	TAC.POL ensures that the TOE Access Control SFP is always invoked before access is granted to the TOE features. PAC.POL ensures that the Provisioning Access Control SFP is always invoked before resources are provisioned to users.
FPT_TDC.1.1	SA.RECONCILE	In a trusted source reconciliation run, if OIM detects new target system accounts, then it automatically creates these users as new OIM users. If OIM detects changes to target system accounts for existing OIM users, then these changes are also made for the corresponding OIM Users.
FPT_TDC.1.2	SA.RECONCILE	In a trusted source reconciliation run, if OIM detects new target system accounts, then it automatically creates these users as new OIM users. If OIM detects changes to target system accounts for existing OIM users, then these changes are also made for the corresponding OIM Users.
FAU_GEN.1T.1	AA.INF	Audit records are generated to contain information as defined by AA.INF.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FAU_GEN.1T.2	AA.INF	Audit records are generated to contain information as defined by AA.INF.
FAU_GEN.2.1	AA.INF	Audit records are generated to contain the required user identity information as defined by AA.INF.
FAU_SEL.1.1	AA.INF	AA.INF covers the use of the logging properties file to include or exclude auditable events from the set of audited events.

The table below shows that all the SFRs listed in Chapter 5 are mapped to at least one SF defined in Chapter 6 and that every SF is mapped to at least one SFR (but note that SFRs FDP_ACF.1.3A 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			FAU			
	UID.1.1	UID.1.2	UAU.1.1	UAU.1.2	AFL.1.1	AFL.1.2	ATD.1.1	SOS.1.1	USB.1.1	USB.1.2	USB.1.3	ACC.1.1	ACF.1.1	ACF.1.2	ACF.1.3	ACF.1.4	ETC.2.1	ETC.2.2	ETC.2.3	ETC.2.4	MSA.1.1	MSA.3.1	MSA.3.2	SME.1.1	SMR.1.1	SMR.1.2	RVM.1.1	TDC.1.1	TDC.1.2	GEN.T1.1	GEN.IT.2	GEN.2.1	SEL.1.1
IA.PRELOGIN	Y		Y																													
IA.LOGIN		Y		Y	Y	Y																										
IA.CHANGEPWD				Y				Y																								
TAC.POL												Y	Y	Y							Y			Y	Y	Y	Y						
PAC.POL												Y	Y	Y													Y						
PAC.EVALPOL														Y																			
PAC.PROVISION																	Y	Y	Y	Y													
PAC.REQPRV															Y																		
PAC.DIRECTPRV															Y																		
PAC.ATTEST														Y																			
SA.UATT							Y		Y	Y			Y																				
SA.CHPWD								Y													Y			Y									
SA.UEFF									Y	Y	Y		Y																				
SA.RECONCILE																												Y	Y				
SA.CRUSER																					Y			Y									
SA.DEFTACATT																						Y	Y										
SA.DEFPACATT																						Y	Y										
AA.INF																														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.

[ECG] *Evaluated Configuration Guide for Oracle Identity Manager Release 9.1.0.2,* Oracle Corporation, March 2011.

[OIMAG] *Oracle Identity Manager Administrative and User Console Guide, Release 9.1.0.2,* Part No. E14765-02, Oracle Corporation.

[OIMC] *Oracle Identity Manager Concepts, Release 9.1.0.1,* Part No. E14065-01, Oracle Corporation.

[OIMCC] *Oracle Identity Manager Connector Concepts, Release 9.1.0,* Part No. E11217-02, Oracle Corporation.

[OIMCG] *Oracle Identity Manager Administrative and User Console Customization Guide, Release 9.1.0.1,* Part No. E14044-02, Oracle Corporation.

[OIMDC] *Oracle Identity Manager Design Console Guide, Release 9.1.0.2,* Part No. E14762-01, Oracle Corporation.

[OIMIC] *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server, Release 9.1.0.1,* Part No. E14062-01, Oracle Corporation.

[OIMR] *Oracle Identity Manager Reference, Release 9.1.0.1,* Part No. E14066-01, Oracle Corporation.

This Page Intentionally Blank

ANNEX

B Glossary

Acronyms

API	Application Program Interface
DAC	Discretionary Access Control
EJB	Enterprise Java Bean
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
OIM	Oracle Identity Manager
OID	Oracle Internet Directory
JAR	Java Archive
RDBMS	Relational Database Management System
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement

SOF	Strength of Function
TOE	Target Of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
XML	Extensible Markup Language

Terms

If a term described below has [CC] written after it, then this term is defined in Chapter 3 or Chapter 4 of [CC] Part 1, or is defined within the text of [CC] Part 2. All other terms relate to Oracle Identity Manager (OIM), for which [OIMR, Glossary] covers the full set of its terms. The terms that are relevant to this document are described below.

Access — Access is the granting of enterprise resources to Oracle Identity Manager users and/or organizations. Access to these resources depends upon the specific policies adopted by the enterprise. The customer defines (and Oracle Identity Manager implements) policies that determine whether, how, and under what circumstances users gain access to various corporate resources.

Access Policy — A list of user groups and the resources with which users in the group are to be provisioned or deprovisioned. Access policies are defined by using the Access Policies menu item in the Oracle Identity Manager Administrative and User Console.

Access Rights Management — The process by which access to enterprise resources is granted or revoked. This includes decisions regarding which users can access specific resources and when they are allowed to access them.

Adapter — A Java class, generated by the Adapter Factory, that enables Oracle Identity Manager to interact with an external JAR file, a target IT resource, or a user-defined form. An adapter extends the internal logic and functionality of Oracle Identity Manager. It automates process tasks and defines the rules for the auto generation and validation of data in fields within Oracle Identity Manager. There are five types of adapters: task assignment adapters, task adapters, rule generator adapters, prepopulate adapters, and entity adapters.

Adapter Factory — A code generation tool provided by Oracle Identity Manager, which enables a User Administrator to create adapters.

Administrator — A person who has some or all of the responsibilities of installing, configuring and maintaining a system, establishing and managing user accounts, allocating adminis-

trative 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. OIM users are authorized to perform TOE operations via permissions associated with the groups of which they are members. Thus an OIM administrator is a user that is a member of groups with the necessary permissions to perform administrative duties. Some groups are classified as administrative groups and hence users that are members of such groups are automatically administrators.

Application Program Interface

This is the interface by which an application program accesses an operating system and other services. An API is defined at the source code level and provides a level of abstraction between the application and the kernel (or other privileged utilities) to ensure portability of the code. An API can also provide an interface between a high-level language and lower-level utilities and services that were written without consideration for the calling conventions supported by compiled languages. In this case, the API's main task might be the translation of parameter lists from one format to another and the interpretation of call-by-value and call-by-reference arguments in one or both directions.

Approval Process

This is one of two Oracle Identity Manager process types. This type of process is generally used to approve the provisioning of Oracle Identity Manager resources to users or organizations. Unlike provisioning processes, approval processes are usually comprised of tasks that must be manually completed.

Attestation

Attestation enables reviewers to be notified of a report they must review that describes the provisioned resources that certain users have. The reviewer can attest to the accuracy of the entitlements by providing a response. This attestation action, along with the response the reviewer provided, any associated comments, and an audit view of the data that the reviewer viewed and attested to, is tracked and audited to provide a complete trail of accountability. In Oracle Identity Manager, this process is known as an attestation task.

Audit

Oracle Identity Manager reports on both the history and the current state of the provisioning environment. Some of the identity data captured by Oracle Identity Manager includes user identity profile history, group membership history, user resource access, and fine-grained entitlement history. Oracle Identity Manager also captures data generated by its workflow, policy, and reconciliation engines. By combining this data along with identity data, an organization has all the required data to address any identity and access-related audit inquiry.

In addition to features for use by an enterprise’s auditors, Oracle Identity Manager also provides features for the logging of audit records that can be used by administrators to check for actual or potential violations of the TOE’s security policy. These audit records are generated using the log4j system and are written to the TOE’s audit log.

Audit Engine

The audit engine is the main component for creating the audit history for different areas of the Oracle Identity Manager system. This engine is in charge of receiving changes to data objects and passing them along to the relevant software that handles the auditing of those data object changes.

Audit Log

The TOE’s audit log holds audit records that can be used by administrators to check for actual or potential violations of the TOE’s security policy. The level of detail logged via the log4j system is dependent on the settings in the logging properties file.

Audit Manager	The OIM software, which manages the software components that audit data object changes.
Audit Record	A collection of information of interest for one transaction or event.
Automated Task	This is any task within a process that does not require user interaction for completion. Automated tasks always require a process task adapter. Provisioning processes are generally comprised of automated tasks.
Authentication	Authentication is the process by which the claimed identity of a user requesting access to an IT asset is validated.
Authorization	The process that determines the access permitted to users after they have been authenticated.
Authorized Administrator	An administrator who has been granted the necessary privileges to perform his or her administrative duties.
Client	This is the GUI software that runs as part of the Presentation Tier of Oracle Identity Manager (see Figure 1 in Chapter 2).
Connector	Used to integrate Oracle Identity Manager with a specific third-party application, such as Microsoft Active Directory or Novell eDirectory.
Data Field	Areas of a form into which information can be entered (for example, Organization Name). Data fields are used to contain, display, and potentially edit the data entered into them.
Data Object	A Data Object is an internal object representation of a table in the Oracle Identity Manager data model in which business logic is applied. It is also responsible for inserting, updating, and deleting data from the data store.
Database	The storage facility for data within Oracle Identity Manager. Oracle Identity Manager controls this data by using a Database Management System.
Delegated Administrator	An Oracle Identity Manager user that has been assigned administrative responsibilities. Administrative rights are assigned by using membership within administrative groups. Administrators have access only to those organizations, forms, data, and users for whom they are responsible.
Deprovisioning	The rescinding of a user's, group's, and/or organization's access to a resource.
Direct Provisioning	This is one of the methods by which a resource can be provisioned. Only users with specific administrative privileges can direct provision resources. When a resource is direct provisioned (to a user or organization), Oracle Identity Manager does not invoke the standard approval process (because this is only associated with requests) or the resource's approval process. Instead, Oracle Identity Manager proceeds directly to begin the applicable provisioning process for the resource.
Design Console	The Design Console is used to configure the system settings for the use of Oracle Identity Manager. Such setting are for areas such as user management, resource management, process management and business rule definition.

End-user	This type of user can only access the Oracle Identity Manager Administrative and User Console. End-users are generally only able to perform basic functions within Oracle Identity Manager.
End-user Administrator	This type of user can use both the Administrative and User Console and the Design Console of Oracle Identity Manager. End-user administrators are responsible for configuring Oracle Identity Manager for their company's end-users.
Group	A group is a collection of one or more users. Group definitions can be used to assign permissions to all members of the group. An administrative group can be created for a user group and users can be assigned to the administrative group to perform administrative operations for the user group.
Hypertext Transfer Protocol (HTTP)	Hypertext Transfer Protocol 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.
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.
Manual Task	This is any task within a process that requires user action in order to be completed. Approval processes generally comprise manual tasks.
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]
OIM Account	An OIM Account is granted to an OIM User to give the OIM User the ability to login to Oracle Identity Manager and to access Oracle Identity Manager's features. At the minimum, these features involve self-service and request. An OIM Account can be granted additional privileges, including the ability to define workflows and the delegated administration of various entities such as users and organizations. An OIM account can be created in the following ways: • through reconciliation from one or more trusted identity sources, such as Oracle Human Resources Management System (HRMS) or an LDAP directory; • manually through the Administrative and User Console; • through the Java APIs and/or the SPML Web Service. In addition, a user can also self-register in the Administrative and User Console to create an account. If the administrator has set OIM to require approvals for self-registration requests, the account is ready for use when the required approvals are obtained
Oracle Identity Manager	A software platform that automates access rights management and the provisioning of resources. Oracle Identity Manager instantly connects users to the resources that can be productive, and revokes and or prevents unauthorized access to protect proprietary information and enhance security.
Organization	A record used to represent an organizational unit within a company's hierarchy (for example, a department, division, or cost centre). Oracle Identity Manager does not limit

	the number of suborganizations that can be created within an organization.
Password Policy	A collection of criteria used to validate password creation and modification within Oracle Identity Manager or on an external resource. The criteria within a policy are applied based on the rule associated with it on the resource object to which it has been attached. Password policies can be defined for Oracle Identity Manager and/or third-party system passwords.
Password Policy Rule	A rule used to determine which password policy is to be applied to password creation and modification on a particular resource or within Oracle Identity Manager. Password policy rules are always of type General.
Reset Password	This occurs when a user changes their password or unlocks their account if it has become locked.
Platform	The combination of software and hardware underlying the TOE. [CC]
Process	This is a collection of one or more process tasks in addition to a requested instance of a process definition.
Process Definition	This is a record containing a detailed definition of all properties of a process as well as its workflow and the tasks that comprise it.
Process Status	This is the current state of execution for a process. The status of a process is determined by the status of its tasks.
Process Task	This is a step or component of a process (as specified within the Process Definition form). Process tasks can be independent or dependent on one another.
Provisioning	The granting of resource access to users in conformance with Oracle Identity Manager policies.
Provisioning Policy	An access policy that is applied to a group during resource provisioning. A provisioning policy is one of several factors that determine whether a resource object can ultimately be provisioned to the user. A provisioning policy definition specifies the resource objects that can be allowed or disallowed for one or more groups.
Provisioning Process	This is one of two Oracle Identity Manager process types. This type of process is used to provision Oracle Identity Manager resources to users or organizations.
Provisioning Status	The status of the resource object as it is being provisioned to a user or an organization. A resource object can have pre-defined statuses: Provisioning, Provisioned, Enabled, Disabled, Revoked, Provide Information or None.
Record	A collection of related items of information organized as a single unit of data (for example, a single record comprising a name, telephone number, and address). The record is the entity stored in the database that contains this related information (whereas forms are the mechanism employed by the user to view or edit that information).
Reconciliation	The process by which any action to create, modify, or delete a target system identity started in the target system (by using traditional means) is communicated back to the provisioning system and recorded.

Reconciliation Rule

A rule configured to identify a matching user in Oracle Identity Manager based on reconciliation fields.

Recovery Task

A process task that starts when a preceding process task achieves a status of Rejected. The relationship between the primary task and its recovery task must be pre-defined for this to occur. This relationship is set within the Undo/Recovery tab of the process task's Editing Task window.

Remote Manager

A server that enables Oracle Identity Manager to communicate with a remote application that is either non-network-aware, or is network-aware, but is not located on the Oracle Identity Manager Server. Remote managers are employed when Oracle Identity Manager has to perform some function with this third-party application (for example, call a method that resides within the external API).

Request

An entity that represents the beginning of the approval and provisioning of one or more resources to one or more users or organizations. When a request for the provisioning of resources is submitted, Oracle Identity Manager will:

- Select and evaluate a standard approval process.
- Select and evaluate a resource-specific approval process for each resource in the request.
- Select and run a resource-specific provisioning process for each resource in the request.

The request record maintains information about the standard approval process and the resource-specific approval process instances. Administrators or end-users generally place requests, although requests can also originate in external systems.

Request-based provisioning differs from direct provisioning. Direct provisioning bypasses both the standard approval process and the resource-specific approval process.

Request Status

This is the current state of the request. A request can have statuses: Request Initialized, Request Received, Approved, Not Approved, Object Approval Complete or Request Complete.

Resource

Also referred to as a Resource Object. This is any unit of hardware, software, or data over which a company wishes to enforce provisioning control. For example, hardware resources can be servers and printers in the network. Software resources can be programs, utilities, or even smaller elements within a program. Data resources could be any accessible files or databases.

The Oracle Identity Manager resource object definition is the virtual representation of the resources to be provisioned. For example, a resource object can have one or more approval processes, provisioning processes, rules, and password policies. The Oracle Identity Manager resource object definition is used to control the various processes and policies associated with the resource, as well as set systemwide options that will determine how the resource is provisioned.

Rule

User-defined criteria employed by Oracle Identity Manager to match conditions and take action based on them. There are five types of rules: General, Process Determination, Task Assignment, Prepopulate and Reconciliation.

Scheduled Task

A task configured in Oracle Identity Manager to run at a scheduled time.

Self-registration	A feature for the user to register with Oracle Identity Manager by using the OIM Administrative and User Console.
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)	Security functional components that are described in [CC] Part 2 are the basis for the security functional requirements expressed in a Security Target. These requirements describe the desired security behaviour expected of a Target of Evaluation or the IT environment of the TOE and are intended to meet the security objectives stated in the Security Target. [CC]
Server	The software architecture tier used to implement the business logic and manage the interaction between the Oracle Identity Manager Client and the database (see Figure 1 in Chapter 2).
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]
Standard Approval Process	This type of approval process is used to approve a request as a whole, which can include multiple resource objects and users or organizations. It is not resource-specific but rather request-specific.
Status	The current state of execution for a given process or process task. The statuses of each task within a process determine the overall status of the parent process (certain tasks statuses have a greater effect on the process's overall status). There are six main statuses within Oracle Identity Manager: Canceled, Suspended, Rejected, Pending, Completed and Waiting.
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]
Suborganization	An organization that is a member of and derived from a higher-level (or parent) organization (for example, a department within a division).
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 an object, a suitably authorized user is one who is permitted by the TOE Access Control SFP to perform the operation on the object.

System	A specific IT installation, with a particular purpose and operational environment [CC]
System Administrator	The OIM system administrator uses the Design Console to configure the TOE in readiness for its operational use and has both read and write access to all forms and records within Oracle Identity Manager.
Target Of Evaluation (TOE)	The product or system being evaluated. [CC]
Target Resource	The external resource or application to which a user or organization is to be provisioned with access by using Oracle Identity Manager. Within the context of Oracle Identity Manager's reconciliation functions, this term has a more specific meaning. It is then used to refer to a resource with which Oracle Identity Manager has been set to conduct reconciliation. Target resources differ from trusted sources in that Oracle Identity Manager only accepts changes to the primary user record from a trusted source. All other external applications with which Oracle Identity Manager is conducting reconciliation are referred to as target resources.
Target Resource Reconciliation	This refers to reconciliation that result in creation/update/revocation of resources provisioned to a user in Oracle Identity Manager.
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]
Trusted Source	This is the Resource object in which a unique key for reconciliation with data in Oracle Identity Manager has been defined. The trusted source is the resource object from which Oracle Identity Manager accepts changes to the user record definition. There can be more than one trusted source and more than one key for each trusted source.
Trusted Source Reconciliation	This is also known as Authoritative Identity Reconciliation, which can be used to create, update, and delete users in Oracle Identity Manager.
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]
User	Any entity (human or machine) outside the TOE that interacts with the TOE. [CC] An OIM user is an individual who possesses an account and login credentials within Oracle Identity Manager. There are two distinct types of users in Oracle Identity Manager: End-user Administrators and End-users.
User Target	This is the user for whom a resource has been requested or direct provisioned.

XML - Extensible Markup Language

This is an open standard for describing data from the World Wide Web Consortium (W3C). It is used for defining data elements on a Web page and business-to-business documents. It uses a tag structure similar to HTML; however, whereas HTML defines how elements are displayed, XML defines what those elements contain. HTML uses pre-defined tags, but XML helps tags to be defined by the developer of the page. As a result, virtually any data items, such as product, sales rep and amount due, can be identified, allowing Web pages to function similarly to database records. By providing a common method for identifying data, XML supports business-to-business transactions and is expected to become the dominant format for electronic data interchange.