National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Oracle Identity Manager Version 11g Release 2

Report Number: CCEVS-VR-VID10589-2015
Version 1.0
August 28, 2015

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin, Senior Validator
The Aerospace Corporation

Dr. Patrick Mallett, Lead Validator
The MITRE Corporation

Jean Petty, Lead Validator
The MITRE Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
Dave Cornwell
Chris Rakaczky

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Oracle Identity Manager, provided by Oracle Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Linthicum Heights, Maryland, United States of America, and was completed in August 2015. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 (ESM ICM PP).

The Target of Evaluation (TOE) is the Oracle Identity Manager Version 11g Release 2. The Oracle Identity Manager TOE is a software application that is used as a method to centralize the management of the roles and privileges of user accounts within an organization.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the ESM ICM PP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the ESM ICM PP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Oracle Identity Manager Version 11g Release 2 Security Target, Version 1.0, July 29, 2015 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Oracle Identity Manager Version 11g Release 2 *Refer to Table 2 for Specifications
Protection Profile	Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 (including the optional FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_HTTPS_EXT.1, FCS_RBG_EXT.1, FCS_TLS_EXT.1, and FMT_MTD.1 requirements)
Security Target	Oracle Identity Manager Version 11g Release 2 Security Target, Version 1.0, July 29, 2015
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Oracle Identity Manager Version 11g Release 2" Evaluation Technical Report v1.0 dated August 13, 2015
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Oracle Corporation
Developer	Oracle Corporation
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Linthicum, Maryland

CCEVS Validators	Daniel Faigin, The Aerospace Corporation Dr. Patrick Mallett, The MITRE Corporation Jean Petty, The MITRE Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- There will be a defined enrollment process that confirms user identity before the assignment of credentials.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- The TOE will receive reliable time data from the Operational Environment.

3.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- **T.ADMIN_ERROR** — An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- **T.EAVES** — A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
- **T.FALSIFY** — A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment.
- **T.FORGE** — A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.
- **T. INSUFFATR** — An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
- **T.MASK** — A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
- **T.RAWCRED** — A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.
- **T.UNAUTH** — A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.

- **T.WEAKIA** — A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- **O.ACCESSID** — The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.
- **O.AUDIT** — The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
- **O.AUTH** — The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
- **O.CRYPTO** — The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
- **O.EXPORT** — The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.
- **O.IDENT** — The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.
- **O.INTEGRITY** — The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.
- **O.MANAGE** — The TOE will provide Assignment Managers with the capability to manage the TSF.
- **O.PROTCOMMS** — The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
- **O.PROTCRED** — The TOE will be able to protect stored credentials.
- **O.ROBUST** — The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
- **O.SELFID** — The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.

3.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Security Requirements for Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 (including the optional

FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_HTTPS_EXT.1, FCS_RBG_EXT.1, FCS_TLS_EXT.1, and FMT_MTD.1 requirements) to which this evaluation claimed exact compliance.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.
- The TOE includes a number of connectors. Connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. The connectors allow the TOE to send and receive data to and from the IT entities within the operational environment, such as the Identity Stores. Oracle separates these connectors into 3 groups; Identity Connector Framework connectors, Legacy connectors, and Remote Manager Connectors. All connectors have two functional parts: (1) an API component, for endpoint specific APIs to read and write to the endpoint system (2) an encryption component, for secure communications between the connector and the endpoint/TOE depending on the connector group. The evaluation team tested the security functionality of the connectors by testing representative examples of each group.

The evaluated configuration of the TOE includes the Oracle Identity Manager Version 11g Release 2 product. The TOE includes all the code that enforces the policies identified (see Section 5).

The Non-FIPS 140-2 mode of operation is excluded from the evaluation. This mode will be disabled by configuration. The exclusion of this functionality does not affect compliance to the Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The Target of Evaluation (TOE) is the Oracle Identity Manager Version 11g Release 2. The Oracle Identity Manager TOE is a software application that is used as a method to centralize the management of the roles and privileges of user accounts within an organization. The TOE is capable of associating certain user attributes (or combinations of user attributes) with different sets of privilege on Operational Environment resources. The TSF can then configure these resources based this association. The TOE can consume data that already exists in organizational identity stores so the privilege model does not need to be one that is defined by the TOE. Environmental resources can be provisioned by job title, office location, national citizenship, or other attributes of the administrator's choosing. The TOE also provides a self-service component so that users are able to change their own passwords or initiate an approval process to update their permissions. The TOE is within a configuration as specified in Section 4.2 below .

4.2 Physical Boundaries

The physical boundary of the TOE includes the OIM software that is installed on top of the environmental WebLogic application server and the connectors that are used to provision endpoint systems. The TOE does not include the hardware or operating systems of the systems on which it is installed. It also does not include the third-party software which is required for the TOE to run. The following table lists the minimum hardware and software components that are required to use the TOE:

Table 2 – Operational Environment System Requirements

Component	Linux	UNIX
Server OS	Oracle Linux 6 UL1+ or Red Hat Enterprise Linux 6	Solaris 11
OS Type	64-bit	
Minimum Physical Memory	4 GB	
Minimum Available Memory	2 GB	
Application Server	Oracle WebLogic Server 11g	
Database	Oracle 10g or 11g	
Identity Store	Microsoft Active Directory, Oracle Internet Directory (OID), or Oracle Unified Directory (OUD)	
Co-Requisite Software	Oracle Access Manager (OAM) 11g	

The TOE resides on a network and supports the following hardware, software, and firmware in its environment:

Table 3 – IT Environment Components

Component	Definition
Application Server	WebLogic application server software that is used as a framework to run the OIM application.
Database Server	Physical system on which the RDBMS is installed.
Endpoint Systems	Systems and their associated applications that end users access to perform their organizational duties.
LDAP	Organizational data store that defines end users and their organizational attributes
Local Filesystem	System storage on the Server that is used to store some configuration and log data for the Application Server.
OAM	Authentication/authorization application that governs access to the TOE's administrative interface.
OIM Design Console	A local server application that is used to set initial configuration parameters for OIM that are not pertinent to the security functionality of the TOE.
RDBMS	Database used to store a variety of configuration, operation, and audit data for the TOE. In the evaluated configuration, this is expected to be Oracle 10g or 11g.
Server	Physical system on which the OIM software is installed. Contains local file system, SMTP server, and application server.
SMTP Server	Email server used to send notifications and self-service data to administrators and end users.

5 Security Policy

5.1 Enterprise Security Management

The primary functionality of the TOE is to maintain the identity and credential lifecycle for organizational users. The TSF can define and maintain the organizational attributes of users, enroll and un-enroll users, and impose controls that ensure that their authentication credentials (passwords) are sufficiently secure. Additionally, the TSF can associate various user attributes with the notion of an "identity" such that environmental systems and applications are configured for different users based on this identity. For example, the TSF can associate a number of different office locations with a region and give users who are located in this region a certain set of permissions. As users enter the organization, leave the organization, or change their location, the change will be detected by the TSF so that the user permissions can be updated automatically. Administrators can also manually assign different attributes to organizational users. All updates to identity and credential data that require the TSF to connect to an external server are secured using TLS.

The TSF relies on an authentication server and data store in the Operational Environment to define its administrators and handle their authentication. This allows the TOE to rely on existing organizational user account and authentication information rather than introducing its own.

5.2 Security Audit

The TOE generates audit records of its behavior and administrator activities. Audit data includes date, time, event type, subject identity, and other data as required. Audit data is written to a remote database over a secure connection and to the local file system of the server on which the TOE resides.

5.3 Cryptographic Support

The TOE provides cryptographic capabilities in support of TLS and HTTPS secure communications. Cryptographic capabilities are provided by the FIPS 140-2 validated RSA BSAFE Crypto-J version 5.0 software cryptographic module, certificate #1503. This module is provided with OIM and is therefore considered to be within the scope of the TOE. The module was validated at Overall Level 1, with Level 2 Roles, Services, and Authentication and Level 3 Design Assurance.

5.4 Identification and Authentication

The TOE checks administrative privileges with each submitted request so that an active administrative session cannot be used to violate the principle of least privileges should that administrator's privileges be changed after the session has been established.

5.5 Security Management

The TOE is managed by authorized administrators using a web GUI. Administrative privileges are defined by the TSF using identity data that is defined in the Operational Environment. The TOE can also define workflow steps such that administrative activities can be subjected to an approval process. The TOE provides a set of out-of-the-box administrative roles with fixed privileges to manage different aspects of the TSF. In

addition to direct administration, an organizational user can perform self-service by updating their organizational password or updating some of their personal attributes. These users can also initiate requests to be assigned privileges that can be subjected to a workflow approvals process to ensure that users can quickly be given appropriate privileges to perform their organizational responsibilities.

5.6 Protection of the TSF

The TOE ensures that administrator credentials are hashed before being sent to the Operational Environment and does not store cleartext password data in memory. If a user forgets their password and uses the recovery feature to access their account, the password will be reset. Similarly, the answers to user security questions (used for password recovery) are stored in a hashed format. The TOE also protects secret and private key data such that there is no mechanism to disclose this information and compromise the security of trusted communications.

5.7 Trusted Path/Channels

The TOE allows trusted channels to be established between itself and the remote data stores (LDAP, RDBMS) that it interfaces with. These trusted channels are secured using TLS. In addition, the TOE establishes a trusted path between authorized administrators and the TSF using HTTPS for the web GUI.

6 Documentation

The following documentation located on NIAP's website was used as evidence for the evaluation of the Oracle Identity Manager:

- *Oracle Identity Manager 11g Release 2 Supplemental Administrative Guidance for Common Criteria, Version 1.0, August 2015*
- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)*
- *Oracle Fusion Middleware Administering Oracle Identity Manager 11g Release 2 (11.1.2.3.0)*
- *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager 11g Release 2 (11.1.2.3.0)*
- *Enterprise Deployment Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite 11g Release 2 (11.1.2.3.0)*
- *Fusion Middleware Developer's Guide for Oracle Identity Manager 11g Release 2 (11.1.2)*
- *Oracle Fusion Middleware Administrator's Guide 11g Release 2 (11.1.2.3)*

There are many documents available on Oracle's support website, but the above mentioned documents are the only documents that are to be trusted as having been part of the evaluation.

This guidance documentation contains the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance document is applicable for all configurations of the Oracle Identity Manager product claimed by this evaluation. Additionally, the guidance documentation contains references and pointers to other TOE guidance documentation for additional detail regarding the security-related functionality. These references were also examined during the evaluation.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Oracle Identity Manager Version 11g Release 2.

To use the product in the evaluated configuration, the product must be configured as specified in the *Oracle Identity Manager 11g Release 2 Supplemental Administrative Guidance for Common Criteria, Version 1.0, August 2015* document. Refer to Section 6 for information on where to retrieve this document from NIAP's website and how to use this document to configure the TOE into the evaluated configuration.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Evaluation Technical Report for a Target of Evaluation "Oracle Identity Manager Version 11g Release 2" Evaluation Technical Report v1.0 dated August 13, 2015*, which is not publically available.

8.1 Test Configuration

The evaluation team configured two environments for testing the TOE which were configured according the *Oracle Identity Manager 11g Release 2 Supplemental Administrative Guidance for Common Criteria, Version 1.0, August 2015* document.

Linux Environment
The following is the evaluated configuration of the OIM software installed on the Oracle Linux 6 Operating System:

Operating Systems:	Oracle Enterprise Linux 6 (UL1+)
Java Application Server:	WebLogic
RDBMS:	Oracle Database 11g
Identity Stores:	Oracle Internet Directory (OID), Oracle Unified Directory (OUD), and Active Directory
Authentication:	Provided by Oracle Access Manager (OAM)
User Enrollment:	External Identity Store and manual administration
Connectors:	OID 11.1.1.6.0 Microsoft Active Directory User Management 9.1.1.7 Microsoft Exchange Connector 11.1.1.6

Solaris Environment
The following is the evaluated configuration of the OIM software installed on the Solaris 11 Operating System:

Operating Systems:	Solaris 11
Java Application Server:	WebLogic
RDBMS:	Oracle Database 11g
Identity Stores:	Oracle Internet Directory (OID), Oracle Unified Directory (OUD), and Active Directory
Authentication:	Provided by Oracle Access Manager (OAM)
User Enrollment:	External Identity Store and manual administration
Connectors:	OID 11.1.1.6.0 Microsoft Active Directory User Management 9.1.1.7 OUD 11.1.1.6.0

The following environment components and test tools* were utilized during the testing:

- WireShark: version 1.8.10

*Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the Oracle Identity Manager by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the ESM ICM PP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.
- Port Scanning

Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

- Web Interface Vulnerability Identification (Burp Suite)
  Burp Suite is a web application vulnerability assessment tool suite. Burp looks for major vulnerabilities including cross-site scripting, SQL injection, directory traversal, unchecked file uploads, etc. as well as less critical vulnerabilities such as unnecessary information disclosure.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Assurance Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Oracle Identity Manager TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Assurance Activities specified in the ESM ICM PP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Oracle Identity Manager product that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 (ESM ICM PP).

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification as well as a separately developed Functional Specification document. Additionally the evaluator performed the Assurance Activities specified in the ESM ICM PP related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the ESM ICM PP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the ESM ICM PP and recorded the results in a Test Report, summarized in the Evaluation Technical Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the ESM ICM PP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the ESM ICM PP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the ESM ICM PP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). In order to remain CC compliant, the device(s) must first be configured in FIPS mode as defined in the *Oracle Identity Manager 11g Release 2 Supplemental Administrative Guidance for Common Criteria, Version 1.0, August 2015* document.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Please note further that certain functionality is excluded from the approved configuration and that some functions relative to the devices were not tested, nor are any claims made relative to their security. The product contains more functionality than was covered by the evaluation. Only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Oracle Identity Manager Version 11g Release 2 Security Target, Version 1.0, July 29, 2015*.

13 List of Acronyms

Acronym	Definition
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ICF	Identity Connector Framework
ICM	Identity and Credential Management
LDAP	Lightweight Directory Access Protocol
OAM	Oracle Access Manager
OID	Oracle Internet Directory
OIM	Oracle Identity Management
OS	Operating System
OUD	Oracle Unified Directory
PP	Protection Profile
RDBMS	Relational Database Management System
SMTP	Simple Mail Transfer Protocol
SPML	Service Provisioning Markup Language
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

14 Terminology

Terminology	Definition
Administrator	The subset of organizational users who have authorizations to manage the TSF.
Entitlement	A privilege assigned to an account on a target system that is configured through provisioning.
Identity Store	The repository in the Operational Environment where organizational users are defined along with their credential data and identity attributes.
Organizational User	A user defined in the identity store that has the ability to interact with assets in the Operational Environment.
Provisioning	The process of configuring the settings and/or account information of environmental assets based on the privileges that different types of organizational users need on them to carry out their organizational responsibilities.
Self-Service	The process by which an end user can initiate a password reset or a request for elevated privileges.
User	In an OIM context, is synonymous with organizational user.

Table 4: Customer Specific Terminology

Terminology	Definition
Authorized Administrator	The claimed Protection Profile defines an Authorized Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be any user with the ‘admin’ role.
Security Administrator	Synonymous with Authorized Administrator.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.

Table 5: CC Specific Terminology

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Oracle Identity Manager Version 11g Release 2 Security Target, Version 1.0, July 29, 2015.
6. Evaluation Technical Report for a Target of Evaluation "Oracle Identity Manager Version 11g Release 2" Evaluation Technical Report v1.0 dated August 13, 2015.
7. Oracle Identity Manager 11g Release 2 Supplemental Administrative Guidance for Common Criteria, Version 1.0, August 2015.
8. Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).
9. Oracle Fusion Middleware Administering Oracle Identity Manager 11g Release 2 (11.1.2.3.0).
10. Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager 11g Release 2 (11.1.2.3.0).
11. Enterprise Deployment Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).
12. Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite 11g Release 2 (11.1.2.3.0).
13. Fusion Middleware Developer's Guide for Oracle Identity Manager 11g Release 2 (11.1.2).
14. Oracle Fusion Middleware Administrator's Guide 11g Release 2 (11.1.2.3).