National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Oracle Access Manager Suite Version 11g Release 2

Report Number: CCEVS-VR-VID10812-2017
Version 1.0
August 31, 2017

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

Stelios Melachrinoudis, Lead Validator
MITRE

Daniel Faigin, Senior Validator
Aerospace Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
Josh Jones
Herb Markle
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Annapolis Junction, 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 Access Manager Suite Version 11g Release 2 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 Annapolis Junction, Maryland, United States of America, and was completed in July 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR), Assurance Activity Report (AAR), 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 Access Control, version 2.1 (ESM_ACPP) and Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1 (ESM_PMPP).

The Target of Evaluation (TOE) is the Oracle Access Manager Suite Version 11g Release 2 which contains the following components:

- Oracle Access Manager (OAM) 11g Release 2
- Oracle Entitlements Server (OES) 11g Release 2

The Oracle Access Manager Suite TOE is a software application that provides web-based access control to web applications that reside in its Operational Environment.

The 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_ACPP and ESM_PMPP documents. 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 and AAR for the ESM_ACPP and ESM_PMPP Evaluation Activities and CEM work units. 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 Access Manager Suite Version 11g Release 2 Security Target v1.0*, dated July 13, 2017 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 Profiles containing Assurance Activities, which are interpretations 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 Access Manager Suite Version 11g Release 2
Protection Profile	Standard Protection Profile for Enterprise Security Management Access Control, version 2.1 Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1
Security Target	Oracle Access Manager Suite Version 11g Release 2 Security Target v1.0, dated July 13, 2017
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Oracle Access Manager Suite Version 11g Release 2" Evaluation Technical Report v1.0 dated July 24, 2017
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, Annapolis Junction, Maryland
CCEVS Validators	Stelios Melachrinoudis, MITRE Daniel Faigin, Aerospace 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 competent and trusted administrator who will follow the guidance provided in order to install the TOE.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- The TOE will receive policy data from the Operational Environment.
- The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
- The TOE will receive reliable time data from the Operational Environment.
- The TOE will receive identity data from the Operational Environment.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.ADMIN_ERROR** – An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- **T.CONDTRADICT** – A careless administrator may create a policy that contains contradictory rules for access control enforcement.
- **T.DISABLE** – A malicious user or careless user may suspend or terminate the TOE’s operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.
- **T.EAVES** – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
- **T.FALSIFY** – A malicious user can falsify the TOE’s identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
- **T.FORGE** – A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
- **T.FORGE** – A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
- **T.MASK** – A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
- **T.NOROUTE** – A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
- **T.OFLOWS** – A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior.
- **T.UNAUTH** – A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.
- **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.
- **T.WEAKPOL** – A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

3.3 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 Standard Protection Profile for Enterprise Security Management Access Control, version 2.1 and Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the ESM_ACPP and ESM_PMPP are claimed by the TOE and documented in the ST.

- Consistent with the expectations of the Protection Profiles, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality 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 ST. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, a number of separate products installed in tandem with Oracle Identity and Access Management or contained within the Oracle Access Manager suite are not part of the TSF. These products are listed in Section 2.3.3 of the Security Target.

- The TOE includes all the code that enforces the functions identified (see Section 5).

4 Architectural Information

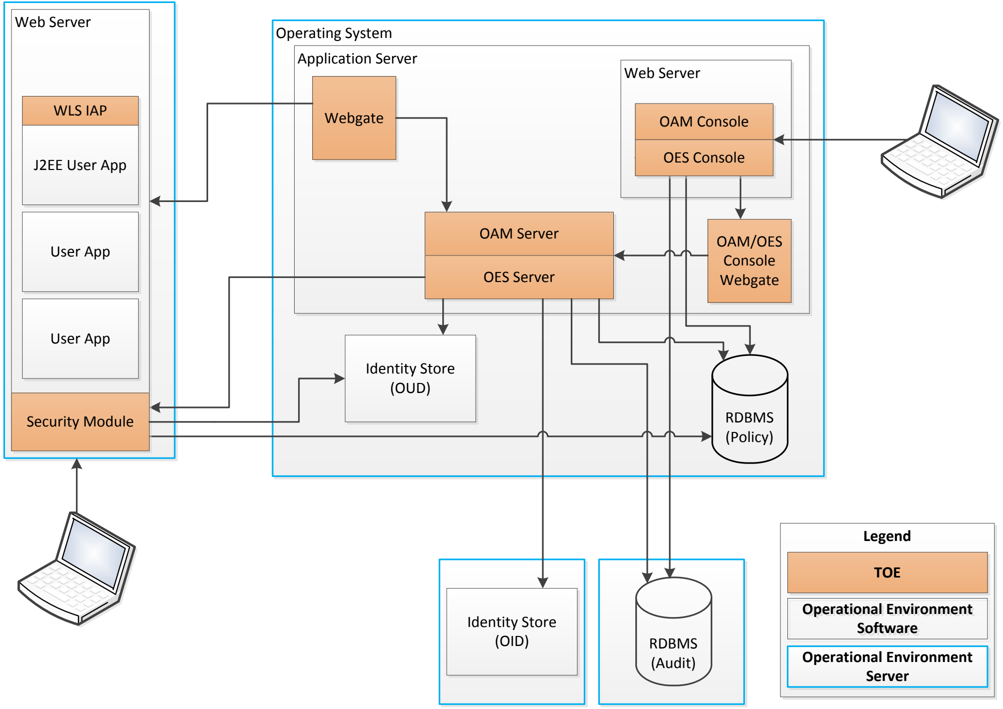
Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The TOE is the Oracle Access Manager Suite (OAM Suite) Version 11g Release 2 software consisting of Oracle Access Manager 11g Release 2 and Oracle Entitlements Server 11g Release 2. OAM Suite (the TOE) is an Enterprise Security Management product that provides web-based access control to web applications that reside in its Operational Environment. It enforces administrator-configurable rules that control access to web pages, files, scripts, and forms, ensuring that resources are protected from unauthorized access. The TOE includes a policy management function that is used to configure the access control policies that are applied to these web applications. This allows for organizations to deploy centralized web applications within an enterprise environment while ensuring that the organization's users are given appropriate and consistent access to these applications based on user attributes that are organizationally defined.

The following figure depicts the TOE boundary:

Figure 1: TOE Boundary



As illustrated in Figure 1, the OAM Suite has both Oracle Access Manager 11g Release 2 (OAM) and Oracle Entitlements Server 11g Release 2 (OES) components. At a high level, OAM is responsible for controlling whether or not a user can access a given resource (URL), while OES is responsible for controlling what the user can do with the resource once they have accessed it. User identity data is maintained as part of the LDAP Identity Store maintained by the organization. Either a local (OUD) or remote (OID) identity store can be used.

Since the TOE is technically comprised of two different components, each component has its own separate GUI. However, since administrators are defined by a shared Identity Store in the Operational Environment, the administrators and their roles and responsibilities can be standardized across the two interfaces. Additionally, each GUI can be deployed on the same underlying application server. Note that the underlying web application can be configured to display a warning banner prior to an administrator accessing either of the GUI interfaces. This is done by a trusted administrator modifying the landing page in the Operational Environment and is not provided by the TSF. Therefore, FTA_TAB.1 has been omitted from the evaluation boundary as per NIAP TD0055.

In the evaluated configuration, one or more Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) are connected to user space web applications in the Operational Environment. When users attempt to perform actions against these applications, the requests are either intercepted by a PEP or transmitted by the application to a PDP for further adjudication. The PDP compares the request to administratively-configured access control policies that are stored in the environmental RDBMS and determines whether or not the requests should be authorized. The application then acts based on these decisions. The TOE provides two kinds of PDPs/PEPs:

- **Webgate (or Access Client)** – provided by OAM, used to intercept HTTP requests
- **Security Module** – provided by OES, used to intercept Java, J2EE, or WebLogic requests made to a WebLogic server application

Architecturally speaking, a Webgate acts primarily as a PEP, although it does have limited caching capabilities for PDP responses. If OAM is used to control access to a WebLogic J2EE application, a component known as the WebLogic Server Identity Assertion Provider (WLS IAP) is installed on the application server to provide a secure conduit of data from the application container to the Webgate. For OES, a Security Module will always act as a PDP but the PEP capability may be implemented either by the Security Module itself or as an agent or plug-in as part of the calling application. This component would then interface directly with the Security Module via an SDK. Both Webgates and Security Modules receive policy data directly from the OAM and OES Server components, respectively.

The TOE can be thought of as a combination of a Policy Management product and a distributed Access Control product, as shown in the following figure:

Figure 2: ESM PP context for the TOE

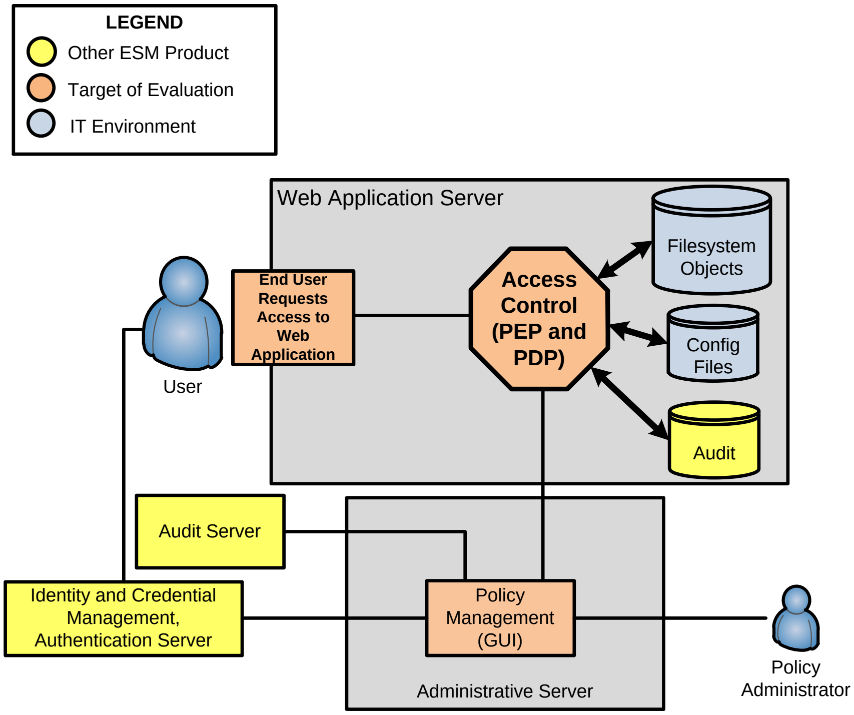


Figure 2 illustrates the TOE in the context of the Enterprise Security Management Protection Profile suite. The ability of the PDP and PEP to intercept activities on a web application can be seen as an Access Control product. The OAM and OES administrative interfaces can be seen as a Policy Management capability. The Identity Store serves as Identity and Credential Management for administrators and users, and audit data can be logged to an external source.

4.2 Physical Boundaries

The TOE is limited to the OAM Suite (which contains OAM and OES), which at a general level provides both the means to enforce access controls against web-based resources and the interface to define the access control rules. The following table describes the TOE components in the evaluated configuration:

Table 2 – Evaluated Components of the TOE

Component	Definition
Access Clients	See Webgates.
OAM Console	A web-based administrative GUI used to configure the behavior of Webgates.
OAM Server	A server-side application, installed on an environmental WebLogic Managed Server, which is responsible for handling the back-end of the OAM Console. Note that the OAM Server and OES Server may reside on the same underlying application server.
OES Administration Console	The web-based administrative GUI used to configure the behavior of Security Modules. Also referred to as OES Console in this ST.
OES Server	A server-side application, installed on an environmental WebLogic Managed Server, which is responsible for handling the back-end of the OES Console. Note that the OAM Server and OES Server may reside on the same underlying application server.
Security Modules	Agents provided as part of OES that are installed onto web servers (WebLogic) and can enforce access control on specific actions or functions provided by the web server.
Webgates	Agents provided as part of OAM that are used to control access to web servers by acting as filters for HTTP requests.

Component	Definition
WLS IAP	An agent deployed on a J2EE WebLogic server as a mechanism that allows the server to communicate with a Webgate.

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 software components that are required to use the TOE:

Table 3 – Operational Environment System Requirements

Component	Requirement
Operating System	• Oracle Enterprise Linux 6
Processor Type	• Intel Core i7, x64
Memory	• 8 GB
Application Server	• Oracle WebLogic Server 10g
JDK	• Oracle JDK 1.6.0_121
RDBMS	• Oracle 11.2.0.1 or higher
Identity Store	• Oracle Internet Directory 11g • Oracle Unified Directory 11g
Web Browser (for administrative UI access)	• Internet Explorer 11 or higher • Firefox 31 or higher

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its operational environment:

Table 4 – Operational Environment Components

Component	Definition
Application Server	Provides the back-end functionality to support the hosting and execution of the applications used by administrators to manage the TSF.
Identity Store	An LDAP repository that defines identity and attribute data for organizational users as well as administrators of the TOE.
Keystore	A Java-based repository that is used to store certificate data for use with public-key cryptography.
Operating System	The underlying platform on which each component of the TOE is installed. Includes the local filesystem component for storage of audit data for TOE activity.
RDBMS	A relational database that stores access control policy data that is defined by the TOE and audit data for TOE activity.
User Application(s)	Web applications that are deployed internally to an organization and used to perform various internal functions. Example include applications related to finances, personnel management, and help desk.

5 Security Policy

5.1 Enterprise Security Management

The TOE provides enterprise security management through its ability to define and enforce access control policies which are transmitted from a centralized server to distributed components responsible for their enforcement. The TSF provides the ability to define these policies through its management interfaces. Policies can be defined to control access to web resources (files and URLs) as well as content (scripts and forms) within a particular web resource.

When a policy is created or modified, the TSF applies this policy to the RDBMS and notifies the appropriate Webgate or Security Module that the policy has been updated. Security Modules will have updated policy information pushed to them by the server while Webgates will poll the OAM Server for relevant policy data when a user attempts to access a protected resource. All remote communications of this type are secured using TLS.

The TOE relies on the environmental Identity Store to identify subjects for access control policy enforcement. Subject data can be augmented by attributes that are defined by the TOE and stored within the user database. Administrators of the TOE are also defined using the Identity Store. Administrators of the TOE are authenticated by the Identity Store using LDAP with username/password.

5.2 Security Audit

The TOE generates records of auditable events which are logged to the environmental RDBMS and also stored on the local filesystem of the component that generated the event. The TSF does not store audit data within the TOE. Any audit data that is transmitted remotely from the TOE to the Operational Environment is secured using TLS.

An administrator can configure the types of events for which logs are generated for both administrator and end user activities for OAM Server and Webgate activities. All OES Server and Security Module activities are always audited. Once generated, audit data is stored in a manner that prevents unauthorized modification or deletion.

5.3 Communications

The TOE provides feedback to administrators when changes to policy rules are applied. Each individual PDP, whether it is a Webgate or Security Module, is identified by a unique name. Policies are uniquely identified by name as well. Policy changes implemented by an Administrator are recorded in the RDBMS and are retrieved from the server and applied by the PDPs for which they are intended. In addition to providing a notification when the policy data is retrieved, an administrator is capable of querying a PDP to determine the specific policy that it has implemented.

5.4 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-C Micro Edition version 4.1.2 software cryptographic module, CMVP certificate #2300. This means that the individual cryptographic algorithms used by the TOE are also FIPS-validated and that the cryptographic module takes appropriate action to zeroize cryptographic keys when no longer needed. This module is provided with OAM Suite and is therefore considered to be within the scope of the TOE. However, Oracle simply provides this component;

it is not modified in any way. The module was validated at Overall Level 1, with Level 3 Cryptographic Module Specification.

5.5 User Data Protection

The TOE performs web-based access control against web servers and web applications that run on them. Access control policies can enforce whether or not a user is able to access a URL or file as well as what they can do on a given web page by controlling the executable scripts and forms that they can interact with. The environmental identity store is used to identify end users. Since the TOE connects to the same identity store in order to define policies, the subjects defined by the access control policies use the same identifying data as they present when attempting to access resources in the Operational Environment.

When a subject attempts to access a protected resource, the TSF examines the HTTP request and determines if any access control policy rules apply to them. Based on the result of the rule evaluation, the TSF will either allow the request, deny the request, or require authentication before allowing the request. The TOE defines a rule processing hierarchy for URL and file access that allows either a best match or a strictly enforced rule ordering, depending on administrative preference.

When a subject attempts to perform a function on a protected resource, the TSF examines the Java, J2EE, or Weblogic request and similarly applies a set of rules to determine whether or not the request is authorized. For this type of request, a strict rule processing order is applied.

5.6 Identification and Authentication

User identity data is defined in the environmental Identity Store. The TOE is able to assign administrative privileges to these users. When administrators log in to the web interfaces of the TOE to manage the TSF, they are associated with their administrative privileges through the assignment of a session cookie. Each subsequent HTTP request submitted to the web interfaces are checked for appropriate authorizations by the web application, so any change to administrative privileges are considered to take immediate effect.

5.7 Security Management

Administrative privileges on the TOE are based on applications and domains. An administrator can be assigned specific domains and applications and have the authority to manage the access control policies for those applications and domains. The TSF also provides system administrator roles with global authority over all applications and all domains. OAM and OES each define their own administrative roles but since they rely on the same environmental identity store, administrative authorities can be synchronized across both interfaces.

By default, the TSF enforces a restrictive deny-by-default policy on any resources that are defined to be protected. The TSF defines a hierarchical engine for how policy rules should be applied to a given request. An administrator may override this engine for rules applying to URLs and files and instruct the TSF to process rules in an administratively-defined order. For rules applying to scripts and forms, the TOE provides a policy evaluation tool that allows the administrator to walk through scenarios in order to see how a given request will be evaluated by a policy prior to committing it to the database.

5.8 Protection of the TSF

The TOE does not store administrator credential data locally; this is stored in the environmental identity store. The TOE also does not provide an interface to access protected cryptographic data. Both Webgates and Security Modules have the ability to continue enforcing policy to some extent if connectivity is lost between them and the server. Webgates do not store policy data locally but do cache policy decisions so that the last decision will continue to enforce that decision in the absence of new information. If connectivity with the server cannot be established for a request that there is no cached decision for, the Webgate will deny the request. Security Modules store copies of policy data locally so a persistent connection with the server is not required for them to continue enforcing access control. Both PDPs will periodically poll the server for new policy information, so in the event of communications being restored, the latest policy data will be retrieved without administrator intervention. Since policy data is transmitted over a trusted channel, there is no mechanism to perform a replay attack in an attempt to get the TSF to enforce an incorrect policy.

5.9 Resource Utilization

If the connection between a PDP and the server is lost, that PDP will be able to continue enforcing the last policy received or act on cached enforcement decisions, depending on the PDP type. The PDPs will periodically poll the server for new policy information, so in the event of communications being restored, the latest policy data will be retrieved without administrator intervention.

5.10 TOE Access

The TOE is able to return an access control decision that requires a subject to provide authentication credentials prior to them being able to access a given web page or file. Policy rules can be written to deny the subject access to these objects based on day and/or time. If access is attempted outside the allowed days and/or times in these cases, the attempt is rejected even if proper credentials are provided by the subject.

5.11 Trusted Path/Channels

The TOE relies on the FIPS-validated cryptographic module that is provided with the product in order to establish secure communications channels. All administrative communications with the management interfaces are secured using HTTPS. All interactions between the management servers and the PDPs, as well as between the TOE and the identity store and database, are secured using TLS.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria v1.0, dated March 2017
- Fusion Middleware Administering Oracle Entitlements Server
  http://docs.oracle.com/cd/E52734_01/oes/ESADR/toc.htm
- Oracle Fusion Middleware Administrator's Guide for Oracle Access Management
  https://docs.oracle.com/cd/E52734_01/oam/AIAAG/toc.htm
- SSL With Oracle JDBC Thin Driver
  http://www.oracle.com/technetwork/topics/wp-oracle-jdbc-thin-ssl-130128.pdf
- Oracle® Fusion Middleware Installation Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)
  https://docs.oracle.com/cd/E52734_01/core/INOAM/toc.htm
- Oracle Database JDBC Developer's Guide
  https://docs.oracle.com/cd/E11882_01/java.112/e16548/toc.htm
- Oracle Database Advanced Security Administrator's Guide
  https://docs.oracle.com/cd/E11882_01/network.112/e40393/toc.htm
- WebLogic JDBC Use of Oracle Wallet for SSL
  https://blogs.oracle.com/WebLogicServer/entry/weblogic_jdbc_use_of_oracle
- Oracle Fusion Middleware Installing WebGates for Oracle Access Manager
  https://docs.oracle.com/cd/E52734_01/core/WGINS/toc.htm
- Oracle Fusion Middleware Securing Oracle WebLogic Server
  https://docs.oracle.com/cd/E15523_01/web.1111/e13707/atn.htm#SECMG175

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 Access Manager Suite 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 Access Manager Suite Version 11g Release 2.

To use the product in the evaluated configuration, the product must be configured as specified in the *Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria v1.0*, March 2017 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 proprietary *Evaluation Technical Report for a Target of Evaluation "Oracle Access Manager Suite Version 11g Release 2" Evaluation Technical Report v1.0,* dated July 24, 2017, as summarized in the publicly available *Assurance Activity Report for a Target of Evaluation "Oracle Access Manager Suite Version 11g Release 2" Evaluation Technical Report v1.0,* dated July 24, 2017.

8.1 Test Configuration

The evaluation team conducted testing at Oracle's Redwood City, CA facility on an isolated network. The evaluation team configured the TOE according the *Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria v1.0* (AGD) document for testing. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces.

The TOE was configured to communicate with the following environment components:

- Operating Systems: Oracle Enterprise Linux 6 (UL1+)
- Application Server: WebLogic
- RDBMS: Oracle Database 11g
- Identity Stores: Oracle Internet Directory (OID) and Oracle Unified Directory (OUD)

The following test tools were installed on a separate workstation (management workstation)

- WireShark version 2.2.3

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

8.2 Developer Testing

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

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE 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_ACPP and ESM_PMPP 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 and initially discovering no known vulnerabilities, the team 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
- Web Interface Vulnerability Identification

The TOE successfully prevented any attempts of subverting its security.

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 Evaluation 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 TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Evaluation Activities specified in the ESM_ACPP and ESM_PMPP.

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 Access Manager Suite 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 Evaluation Activities specified in the ESM_ACPP and ESM_PMPP in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

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. Additionally, the evaluator performed the Evaluation Activities specified in the ESM_ACPP and ESM_PMPP 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 Evaluation Activities specified in the ESM_ACPP and ESM_PMPP 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 Evaluation Activities in the ESM_ACPP and ESM_PMPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity 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_ACPP and ESM_PMPP, 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 evaluation team also ensured that the specific vulnerabilities defined in the ESM_ACPP and ESM_PMPP were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities. Please refer to Section 3.4 of the AAR for more specific information about the vulnerabilities assessed.

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 requirements in the ESM_ACPP and ESM_PMPP, 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 Evaluation Activities in the ESM_ACPP and ESM_PMPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria v1.0,* dated March 2017.

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. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, a number of separate products installed in tandem with Oracle Identity and Access Management or contained within the Oracle Access Manager suite are not part of the TSF. These products are listed in Section 2.3.3 of the Security Target.

In testing FCO_NRR.2, evaluators found that the process starting from the TOE sending a policy from a given source and ending with the TOE transmitting an accurate receipt of policy update to the Policy Management product takes less than one second. Thus, evaluators concluded that the time interval could not be accurately assessed. The Validation Team accepted this explanation; however, this issue will need to be revisited in future evaluations since the Assurance Activity mandates that "an accurate receipt is transmitted back to the Policy Management product within the time interval specified in the ST."

10.1 TRRT Decisions

Two TRRT requests were made by the CCTL and vendor over the course of this evaluation.

The first TRRT request concerned a test in both FTP_ITC.1 and FTP_TRP.1 that states that "the evaluator shall ensure, for each communication channel with an authorized IT entity, modification of the channel data is detected by the TOE." The lab argued that a previous TD for the NDPP (TD0004) should apply to the ESM AC, PM, and ICM PPs, which mandates removing this test. A previous TRRT response for the same issue, which was raised in early 2016, stated that NDPP TD 0004 should apply to the ESM PPs; however, no new TD was issued. A new TRRT response was issued on August 29. 2017 confirming that "this test should be removed from the ESM PPs" and that "a new TD will be issued." No TD has been issued as of the conclusion of this evaluation but will be issued afterwards.

The second TRRT request concerned the following test for FPT_RPL.1: "The evaluator shall test this capability by configuring replay detection in a manner specified by the operational guidance (if applicable), running a packet sniffer application (such as Wireshark) on the local network with the TOE, sending a valid policy to it, and observing the packets that comprise this policy…." This paragraph and the paragraph that follows it mandates that these packets be retransmitted to the TOE and that User Data Protection testing is performed to ensure only the first policy transmitted is enforced. The lab argued that because policy transmission is done using TLS, replay attacks are inherently mitigated and thus the test is not necessary. The lab's full explanation can be found in the Testing section of the AAR for FPT_RPL.1. The Validation Team agreed under the condition that the lab can show through testing that TLS is used in policy transmission and not merely implemented in the TOE. The TRRT agrees in its current response that this condition is sufficient for meeting the intent of the requirement for this evaluation; however, it is not clear whether a TD will be issued or not, or whether the requirement will be re-worded with the condition added.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Oracle Access Manager Suite Version 11g Release 2 Security Target v1.0*, dated July 13, 2017.

13 List of Acronyms

Acronyms / Abbreviations	Definition
AC	Access Control
CC	Common Criteria
ESM	Enterprise Security Management
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IT	Information Technology
J2EE	Java 2 Enterprise Edition
JDBC	Java Database Connectivity
JDK	Java Development Kit
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OAM	Oracle Access Manager
OES	Oracle Entitlements Server
OID	Oracle Internet Directory
OUD	Oracle User Directory
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PM	Policy Management
PP	Protection Profile
RBG	Random Bit Generation
RDBMS	Relational Database Management System
rDSA	RSA Digital Signature Algorithm
RFC	Request for Comment
RMI	Remote Management Interface
SAR	Security Assurance Requirements
SDK	Software Development Kit
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TLS	Transport Layer Security
TSF	TOE Security Function
TSFI	TOE Security Function Interface
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WLS IAP	WebLogic Server Identity Assertion Provider

14 Terminology

Term	Definition
Administrator	A general term for any individual with permissions to manage some aspect of the TSF.
Domain Administrator	An administrator of the TOE that has the ability to modify the access control SFP for a limited set of resources.
End User	A general term for any individual who is attempting to interact with resources that are protected by the access control SFP.
Identity Store	A repository that contains identity and credential data for end users and/or administrators and is used to provide information that the TSF can use to determine whether or not a user’s request to access a resource or an administrator’s request to manage the TOE is authorized.
Security Module	A component of OES that is used to enforce access control policies against activities performed within a web application.
System Administrator	An administrator of the TOE that has unlimited ability to manage the TSF.
Webgate	A component of OAM that is used to enforce access control policies against requests to access URLs on a web application.

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 Access Manager Suite Version 11g Release 2 Security Target v1.0, dated July 13, 2017
6. Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria v1.0, dated March 2017