Assurance Activities Report
For a Target of Evaluation

ORACLE®

Oracle Access Manager Suite

Version 11g Release 2

Assurance Activities Report (AAR)
Version 1.0

7/24/2017

Evaluated by:

Booz | Allen | Hamilton

Booz Allen Hamilton Common Criteria Test Laboratory
NIAP Lab # 200423
304 Sentinel Drive
Annapolis Junction, MD 20701

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Oracle Corporation
100 Oracle Parkway
Redwood City, CA 94065

The Author of the Security Target:
Booz Allen Hamilton Common Criteria Test Laboratory
NIAP Lab # 200423
304 Sentinel Drive
Annapolis Junction, MD 20701

The TOE Evaluation was sponsored by:
Oracle Corporation
100 Oracle Parkway
Redwood City, CA 94065

Evaluation Personnel:
Christopher Gugel – CC Technical Director
Joshua Jones
Herb Markle
Chris Rakaczky

Applicable Common Criteria Version

Common Criteria for Information Technology Security Evaluation, September 2012 Version 3.1 Revision 4

Common Evaluation Methodology Version

Common Criteria for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1 Revision 4

Table of Contents

Purpose

The purpose of this document is to serve as a non-proprietary attestation that this evaluation has satisfied all of the TSS, AGD, and ATE Assurance Activities required by the Protection Profiles/Extended Packages to which the TOE claims exact conformance.

1 TOE Summary Specification Assurance Activities

The evaluation team completed the testing of the Security Target (ST) 'Oracle Access Manager Security Target v1.0' and confirmed that the TOE Summary Specification (TSS) contains all Assurance Activities as specified by 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 evaluators were able to individually examine each SFR's TSS statements and determine that they comprised sufficient information to address each SFR claimed by the TOE as well as meet the expectations of the ESM_ACPP and ESM_PMPP Assurance Activities.

Through the evaluation of ASE_TSS.1-1, described in the ETR, the evaluators were able to determine that each individual SFR was discussed in sufficient detail in the TSS to describe the SFR being met by the TSF in general. However, in some cases the Assurance Activities that are specified in the claimed source material instruct the evaluator to examine the TSS for a description of specific behavior to ensure that each SFR is described to an appropriate level of detail. The following is a list of each SFR, the TSS Assurance Activities specified for the SFR, and how the TSS meets the Assurance Activities. Additionally, each SFR is accompanied by the source material (ESM_ACPP and ESM_PMPP) that defines where the most up-to-date TSS Assurance Activity was defined.

[PM] ESM_ACD.1

"The evaluator shall do the following:

- *Verify that the TSS identifies one or more compatible Access Control products*
- *Verify that the TSS describes the scope and granularity of the entities that define policies (subjects, objects, operations, attributes)*
- *Review STs for the compatible Access Control products and verify that there is correspondence between the policies the TOE is capable of creating and the policies the Access Control products are capable of consuming*
- *Verify that the TSS indicates how policies are identified*

The evaluator shall review the operational guidance to ensure that that it indicates the compatible Access Control product(s) as well as the allowable contents and means of identification of the access control policies that can be defined by the TOE."

Section 8.1.1 of the TSS states:
1. The OAM Suite is an integrated product that is both a Policy Management and Access Control product. The OAM Suite includes the OAM Server and OES Server, both of which have their own graphical user interface.
2. Every operation that the AC component is capable of controlling is able to be defined in a policy by the PM component. This includes subjects, objects and operations.
3. Every operation that the AC component is capable of controlling is able to be defined in a policy by the PM component. This includes subjects, objects and operations.
4. Webgate polices are defined by a unique name and Security Module policies are defined by a unique name and a sequential version number.

[PM] ESM_ACT.1

"The evaluator shall check the TSS and ensure that it summarizes when and how policy data will be transmitted to Access Control products. This includes the ability to specify the product(s) that the policy data will be sent to."

Section 8.1.2 of the TSS states that after the OAM administrator creates or modifies a policy, the relevant Webgates are notified and will query the OAM server when a user attempts to access the protected resource. Also, when the OES administrator creates or modifies a policy, the policy data is pushed directly to the Security Module when the administrator pushes the “distribute” button in the OES Console.

[PM] ESM_ATD.1
“The evaluator shall check the TSS to ensure that it describes the object attributes that are defined by the TOE and the purpose for their definition.”

Section 8.1.3 of the TSS states an administrator or OAM can associate URL and file objects with a required authentication level for webservers that are protected by Webgates. Also, the TSF can define arbitrary attributes that can be applied to objects within a protected application.

[PM] ESM_ATD.2
“The evaluator shall check the TSS to ensure that it describes the subject attributes that are defined by the TOE and the purpose for their definition.”

Section 8.1.4 of the TSS states that the OES Server is able to associate subjects that represent end users (defined in an Identity Store) with arbitrary administrator-defined attributes.

[PM] ESM_EAU.2
“The evaluator shall check the TSS in order to determine that it describes the TSF as requiring authentication to use and that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF.”

Section 8.1.5 of the TSS states that administrators must authenticate to an external Identity store via the TOE’s interfaces before being able to perform any management functions. Authentication is performed by an external Identity store when the administrator supplies valid authentication credentials (username/password).

The SFR consistently represents each authentication mechanism that is described in the TSS.

[AC+PM] ESM_EID.2
NOTE: The Policy Management AA is satisfied in ESM_EAU.2.1
[AC] “*The evaluator shall check the TSS and ensure that it describes where the subject identity data that the TOE uses to make access control decisions comes from. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each identification mechanism that is used by the TSF.”*

[PM] “*The evaluator shall check the TSS and ensure that it describes where the subject identity data that the TOE uses to make access control decisions comes from. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each identification mechanism that is used by the TSF.”*

Section 8.1.6 of the TSS states that the TSF uses an external identity store to identify and authenticate end users who attempt to access protected objects.

The SFR consistently represents each authentication mechanism that is described in the TSS.

[AC+PM] FAU_GEN.1

[AC] "The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records."

[PM] "The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records."

Section 8.2.1 of the TSS describes the audit data that is generated by each component of the TOE (OES Server, OAM Server, and Security Modules). The TSS specifically states that audit data for the Webgate is generated by the OAM Server. The TSS also describes the contents of the audit records that include but are not limited to date, time, subject information, event type.

[AC] FAU_SEL.1.1
"*The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to configure selective auditing for an Access Control product and that it summarizes the mechanism(s) by which auditable events are selected for auditing."*

Section 8.2.2 of the TSS states that the TSF has four levels of selective auditing that is configured in the OAM Server. This controls the audit level for the Webgates as well as the OAM Server. All user activity that is mediated by Webgates is audited when configured at a log level of MEDIUM or ALL. All administrative activity on the OAM Server are logged when the audit level is configured to be LOW, MEDIUM, or ALL.The selective auditing is also configurable for the OES Server and Security Module; however, this is not done on the TSF but in the underlying OS platform. By default, the OES Server and Security Module is set to generate all audit data.

[PM] FAU_SEL.1
"The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to have selective auditing and that it summarizes the mechanism(s) by which auditable events are selected for auditing."

Section 8.2.2 of the TSS states that the TSF has four levels of selective auditing that is configured in the OAM Server. This controls the audit level for the Webgates as well as the OAM Server. All user activity that is mediated by Webgates is audited when configured at a log level of MEDIUM or ALL. All administrative activity on the OAM Server are logged when the audit level is configured to be LOW, MEDIUM, or ALL.The selective auditing is also configurable for the OES Server and Security Module; however, this is not done on the TSF but in the underlying OS platform. By default, the OES Server and Security Module is set to generate all audit data.

[PM] FAU_SEL_EXT.1
"The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to configure selective auditing for an Access Control product and that it summarizes the mechanism(s) by which auditable events are selected for auditing."

Section 8.2.4 of the TSS states that administrators are able to use the OAM console to define the events that are logged by the Webgates. The events that are audited depending on the level selected are discussed in FAU_SEL.1.

[AC] FAU_STG.1
"The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally, what happens when the local audit data store is full, and how these records are protected against unauthorized access."

Section 8.2.5 of the TSS states that all audit data generated by the TSF is transmitted to the underlying local file system. The TOE does not provide the ability to modify or delete the audit data that is stored in this manner.

[AC+PM] FAU_STG_EXT.1

[AC] "The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit."

[PM] "The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit."

Section 8.2.6 of the TSS states audit data is recorded to the local filesystem as well as stored in a remoted database. The path to the remote database is uses JDBC protected by TLS to assure the data is safe from unauthorized disclosure and modification.

[AC] FCO_NRR.2

"The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it discusses how the TOE identifies itself to the Policy Management product and how it provides evidence of the policy's consumption to the Policy Management product."

Section 8.3.1 of the TSS states that during configuration of the Webgate, a unique ID and password are defined. Policies that are assigned to the Webgate include a unique host identifier which includes the absolute relative path of the URL that the policy is applicable to. The combination of the host identifier and resource level of a given rule allows for unambiguous identification of the object the rule applies to.

Security modules are registered to the OES Console and are given unique name. During initial installation and configuration of the Security Module, the administrator creates the new Security Module in the OES Console and assigns a unique name. The administrator then enrolls the installed Security Module with the unique name that was given in the console as well as the specific server information (hostname/ip and port#). The Security Module is then attached to that specific OES Console.

[AC+PM] FCS_CKM.1

[AC] "In order to show that the TSF complies with 800-56A and/or 800-56B, depending on the selections made, the evaluator shall ensure that the TSS contains the following information:

- *The TSS shall list all sections of the appropriate 800-56 standard(s) to which the TOE complies.*
- *For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE;*
- *For each applicable section of 800-56A and 800-56B (as selected), any omission of functionality related to "shall" or ―"should" statements shall be described;*
- *Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described."*

[PM] "In order to show that the TSF complies with 800-56A and/or 800-56B, depending on the selections made, the evaluator shall ensure that the TSS contains the following information:

- *The TSS shall list all sections of the appropriate 800-56 standard(s) to which the TOE complies.*

- *For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE;*
- *For each applicable section of 800-56A and 800-56B (as selected), any omission of functionality related to "shall" or —"should" statements shall be described;*
- *Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described."*

Section 8.4.1 of the TSS states that the TOE meets the key pair generation requirements of NIST SP 800-56B and identifies the sections of the 800-56B standard that are met by the TOE. This section also references the CAVP RSA certificate #1850.

The description of this standard also matches the selection in the SFR. The TSS does not include any additional information for options that require further explanation per the remaining three bullets because they do not apply to the TOE.

[AC+PM] FCS_CKM_EXT.4
[AC] "The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and critical security parameters used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write")."

[PM] "The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and critical security parameters used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write")."

Section 8.4.2 of the TSS states that the TOE uses RSA BSAFE Crypto-C Micro Edition version 4.1.2 cryptographic module and states that it was FIPS 140-2 validated (CMVP certificate #2300). This module provides the ability to zeroize cryptographic data when no longer needed. The TSS also states "The specific keys generated and maintained by the cryptographic module are listed in Table 2 of the RSA BSAFE Crypto-C Micro Edition Security Policy. As these keys are only used ephemerally for the establishment of secure communications, they are not stored persistently and are destroyed upon session termination."

[AC+PM] FCS_COP.1.1(1)
[AC+PM] This SFR does not contain any TSS Assurance Activities. Section 8.4.3 of the ST references the CAVP AES certificate #3596.

[AC+PM] FCS_COP.1.1(2)

[AC+PM] This SFR does not contain any TSS Assurance Activities. Section 8.4.4 of the ST references the CAVP RSA certificate #1850.

[AC+PM] FCS_COP.1.1(3)
[AC+PM] This SFR does not contain any TSS Assurance Activities. Section 8.4.5 of the ST references the CAVP SHS certificate #2958.

[AC+PM] FCS_COP.1.1(4)
[AC+PM] This SFR does not contain any TSS Assurance Activities. Section 8.4.6 of the ST references the CAVP HMAC certificate #2293.

[AC+PM] FCS_HTTPS.EXT.1
[AC] "The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes—for each platform identified in the ST—the interface(s) used by the TOE to invoke this functionality."

[PM] "The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes—for each platform identified in the ST—the interface(s) used by the TOE to invoke this functionality."

Section 8.4.7 of the TSS

1. States that HTTPS connection is established through the web server (using RSA BSAFE) when a user access the TOE via the web browser.
2. Points to section 8.4.9 FCS_TLS_EXT.1 of the ST to describe how the cryptographic function. This section states that TLS protocol is used by invoking the RSA BSAFE cryptographic module to encrypt remote communications.
3. States that the TOE provides the ability for remote administrators to connect to the OAM Console and OES Console using HTTPS as specified in RFC 2818.

[AC+PM] FCS_RBG.EXT.1
[AC] "The evaluator shall review the TSS section to determine the version number of the product containing the RBG(s) used in the TOE. The evaluator shall also review the TSS to determine that it includes discussions that are sufficient to address the requirements described in Appendix C.6 Entropy Documentation and Assessment. This documentation may be included as a supplemental addendum to the Security Target."

[PM] "The evaluator shall review the TSS section to determine the version number of the product containing the RBG(s) used in the TOE. The evaluator shall also review the TSS to determine that it includes discussions that are sufficient to address the requirements described in Appendix C.9 Entropy Documentation and Assessment. This documentation may be included as a supplemental addendum to the Security Target."

Section 8.4.8 of the TSS states that RSA BSAFE Crypto CME v4.1.2 cryptographic module is used for DRBG functions. This section also references the CAVP DRBG certificate #931.

The vendor has supplied an Entropy Assessment Report that discusses the requirements described in Appendix C.9.

[AC+PM] FCS_TLS.EXT.1

[AC] "The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported, client authentication supported) are specified, and the ciphersuites supported are specified as well. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall perform the following activities:

a. Ensure the ST contains a list of representative platforms (hardware and software) compromising the operational environment.
b. Check the TSS to ensure it describes-for each platform identified in the ST-the interface(s) used by the TOE to invoke this functionality.
c. For each platform identified in the ST, check the OE documentation to ensure the interfaces identified in the previous step exist."

[PM] "The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported, client authentication supported) are specified, and the ciphersuites supported are specified as well. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall perform the following activities:

a. Ensure the ST contains a list of representative platforms (hardware and software) compromising the operational environment.
b. Check the TSS to ensure it describes-for each platform identified in the ST-the interface(s) used by the TOE to invoke this functionality.
c. For each platform identified in the ST, check the OE documentation to ensure the interfaces identified in the previous step exist."

Section 8.4.9 of the TSS states that the TOE uses TLS v1.0 and 1.1 to encrypt remote communications. It also specifies the TLS_RSA_WITH_AES_128_CBC_SHA and TLS_RSA_WITH_AES_256_CBC_SHA ciphersuites are used.

The ciphersuites that are specified in the TSS are consistent with what is listed in the SFR. The protocols used in this SFR are provided by invoking the RSA BSAFE cryptographic module and this is consistent with the other FCS requirements in the ST.

[AC] FDP_ACC.1

"*The evaluator shall check the TSS in order to verify that the TOE is capable of mediating the activities that are defined in Table 6 above and that the access control policy enforcement mechanism is described. The evaluator shall also check the TSS to determine that the method by which access control rules are applied is sufficiently detailed to allow for the creation of scenarios that allow for thorough positive and negative testing of the policy enforcement mechanism based on the types of policy rules and their contents."*

Section 8.5.1 of the TSS describes the capability of the TOE to enforce access control policies based upon rules. The rules define the subject-object-operation combinations that are mediated by the TOE. Furthermore, the TSS states "Subjects as defined by the TOE's access control security function policy (SFP) are any organizationally-defined users that can be identified by a web server, objects are anything that is hosted on a web server (URLs, files, scripts, forms), and operations are any activities that a user would perform against these objects in the course of interacting with the web server (accessing a URL with an HTTP GET or POST request, downloading a file, executing a script, submitting a form, etc.)." This is consistent with the table in the AA as well as the table in section 6-3 in the ST.

[AC] FDP_ACF.1

"*The evaluator shall check the TSS in order to verify that the TOE is capable of mediating the activities that are defined in Table 6 above and that the access control policy enforcement mechanism is described. The evaluator shall also check the TSS to determine that the method by which access control rules are applied is sufficiently detailed to allow for the creation of scenarios that allow for thorough positive and negative testing of the policy enforcement mechanism based on the types of policy rules and their contents."*

Sections 8.5.1 and 8.5.2 of the TSS describe the capability of the TOE to enforce access control policies based upon rules. The rules define the subject-object-operation combinations that are mediated by the TOE. Furthermore, the TSS states "Subjects as defined by the TOE's access control security function policy (SFP) are any organizationally-defined users that can be identified by a web server, objects are anything that is hosted on a web server (URLs, files, scripts, forms), and operations are any activities that a user would perform against these objects in the course of interacting with the web server (accessing a URL with an HTTP GET or POST request, downloading a file, executing a script, submitting a form, etc.)." Section 8.5.2 further describes the enforcement of the access control policies by the Webgates and Security Modules based upon the rules created using these subject, objects, and operations. This is consistent with the table in the AA as well as the table in section 6-3 in the ST.

[PM] FIA_USB.1

"The evaluator shall check the TSS in order to determine that it describes the security attributes that are assigned to administrators and the means by which the administrator is associated with these attributes, both during initial assignment and when any changes are made to them."

Section 8.6.1 of the TSS states that the administrator is defined in terms of username, role and administrative scope. Any changes made to the administrator's attributes while the administrator is authenticated to the TOE will be updated at the next login.

[PM] FMT_MOF.1

The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it describes the ability of the TSF to perform the required management functions and the authorizations that are required to do this.

The assignments in the SFR were completed in a consistent manner with the application notes. The TSS discusses the different roles that are able to perform administrative functions on each console.

Section 8.7.1 of the TSS states that the system administrator has full authority to create and configure Webgates/Security Modules, define and assign privileges to new administrators, and to configure global characteristics of the administrative interfaces' behavior. Furthermore, the TSS discusses that the system administrator is able to define domain administrators that are only able to administer policies with in the assigned domain. This information is consistent with the selections and assignments within the SFR.

[AC] FMT_MOF.1(1)

"*The evaluator shall check the TSS in order to determine that it summarizes how the management functions described in the SFR are performed (or, if their behavior is fixed, why this is the case) and how the TSF determines that the management request is authorized."*

Section 8.7.2 of the TSS states the TSF has the ability to configure and monitor the behavior of Webgates and Security Modules. It is capable of configuring the events that are audited by Webgates and the access control policies that Webgates and security modules enforce. The OES and OAM interfaces each define their own system administrator role. A system administrator can perform all security-relevant functionality for their respective interface.

[AC] FMT_MOF.1(2)
"*The evaluator shall check the TSS in order to determine that it indicates the ESM products (or distributed TOE components if multiple ESM PPs are claimed) that are authorized to query the TOE and that this includes, at minimum, a Policy Management component."*

Section 8.7.3 of the TSS states that communication occurs between the OES Server and Security Module as well as the OAM Server and Webgate. This communication only occurs with the components are in the same deployment.

[PM] FMT_MOF_EXT.1
"The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it summarizes the Access Control product functions that the TOE is able to manage and the authorizations that are required in order to manage these functions."

Section 8.7.4 of the TSS refers to sections 8.7.2 and 8.7.3 of the ST for the administration functions the TSF is capable of performing against access control enforcement capability. The referenced sections describe the function as well as the privileged roles that are able to perform those functions.

Also, the assignments in the SFR were consistently completed with the application notes from the PP.

[AC] FMT_MSA.1
"The evaluator shall review the TSS and the operational guidance to confirm that the indicated attributes are maintained by the TOE."

Section 8.7.5 of the TSS indicate that the TOE is a single product that implements both access control and policy management functions. Thus, the TOE controls the ability to control any action on the security attributes defining the access control policy by enforcing an access control policy on the ability of administrators to configure the access control policy through OAM Console or OES Console.

[AC] FMT_MSA.3
"The evaluator shall review the TSS in order to determine how the TSF puts restrictive default values into place (for example, access control policies should operate in deny-by-default mode so that the absence of an access control rule doesn't fail to restrict an operation) and what authorizations are required in order to override these defaults."

Section 8.7.6 of the TSS states that the TOE implements a deny-by-default policy to protected resources by default. The administrator is able to define policies that allow access to the resources by either explicitly permitting subjects to access or excluding operations from enforcement.

[PM] FMT_MSA_EXT.5
"The evaluator shall review the TSS and in order to determine that it explains what potential contradictions in policy data may exist. For example, a policy could potentially contain two rules that

permit and forbid the same subject from accessing the same object. Alternatively, the TOE may define an unambiguous hierarchy that makes it impossible for contradictions to occur. If the TOE does not allow contradictory policy to exist, the evaluator shall verify that this assertion has been made in the TSS and that justification is provided to support the assertion."

Section 8.7.7 of the TSS clearly explains the behavior of the TOE in the case that contradictory policies are created. For example, the TSS discusses the following resolution for the OAM Console/Webgate, "When an administrator defines an authorization policy, the presence of explicitly contradictory rules (e.g. the same subject-object-operation combination at the same level of detail results in both a permit and a deny result) will prevent the policy from being saved." The TSS also describes the behavior of the OES Console/Security Module in the event that contradictory rules exist. The TSS also states that the OES Console provides a policy simulator option to confirm the impact of a policy before it is implemented.

[AC+PM] FMT_SMF.1
[AC] "The evaluator shall check the TSS in order to determine what Policy Management and Secure Configuration Management product(s) (if applicable) are compatible with the TOE."

[PM] "The evaluator shall check the TSS in order to determine that it summarizes the management functions that are available."

Section 8.7.8 of the TSS clearly summarizes each management function and how the TSF either implements the function or explains why the function is not applicable. The evaluation team has confirmed that this list agrees with the set of functions called out as required in the PP.

Section 8.7.8 of the TSS states that the OES Console and OAM console are used to specifically administer Security Modules and Webgates. Also, Security Modules and Webgates are only able to be managed by the OES console and OAM console components, respectively.

[AC+PM] FMT_SMR.1
[AC] "The evaluator shall examine the TSS to verify that it describes how management authority is delegated via one or more roles and how an authorized Policy Management product is associated with those roles."

[PM] "The evaluator shall review the TSS to determine the roles that are defined for the TOE. The evaluator shall also review the TSS to verify that the roles defined by this SFR are consistently referenced when discussion how management authorizations are determined."

Section 8.7.9 of the TSS states the OAM Console and OES Console each define their own sets of administrators. Each console has a default system administrator and has full control of the TSF. Additionally, each system administrator is able to define domain administrators that are able to manage the domains that are assigned. Each interface of the TOE uses the same Identity Store for identification and authentication for the management authorizations.

[AC+PM] FPT_APW_EXT.1
[AC] "The evaluator shall examine the TSS to determine that it details all authentication data , other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts). The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS."

[PM] "The evaluator shall examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts). The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS."

Section 8.8.1 of the TSS states that the TOE uses identity and credential data that is defined in the operational environment. The TOE does not persistently store nor does the TSF retain any of the data after authentication occurs.

[AC] FPT_FLS_EXT.1.1
"*The evaluator shall check the TSS in order to determine that it describes how the SFP(s) defined in FDP_ACC.1 are enforced when the TOE cannot communicate with the Policy Management product that provided the enforced policy. If communications are not expected to be severed (for example, if the TOE and Policy Management product run on the same system), the evaluator shall check the TSS in order to determine that this assertion has been made. If the assignment is chosen to define an alternate failure state behavior, the evaluator shall verify that the failure state behavior is documented in sufficient detail to be unambiguously verifiable."*

Section 8.8.2 of the TSS states that once a Webgate has made a decision based on a policy defined in the OAM Server, it will continue to enforce that decision until a new policy is available that would override it. Once a Security Module receives a policy from the OES Server, it will continue to enforce that policy until a new or updated policy is pushed to it. This ensures that any communication interruption between the servers and endpoints will not affect the enforcement of the policy.

[AC] FPT_RPL.1
"The evaluator shall check the TSS in order to determine that it describes the method by which the TSF detects replayed data. For example, it may provide a certificate or other value that can be validated by the TSF to verify that the policy is consistent with some anticipated schema. Alternatively, the TOE may use a protocol such as SSL for transmitting data that immunizes it from replay threats."

Section 8.8.3 of the TSS states that the only mechanisms that are able to be used to update policy data for Webgates and Security Modules is the OES/OAM Servers. Manipulation to policy data that resides in the RDBMS is not possible because it is locked down from any unauthorized access. Also, the data in transit between the server components and the PDP is secured using TLS. It is not possible for an attacker to spoof the transfer of data using an existing connection.

[AC+PM] FPT_SKP_EXT.1
[AC] "The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured."

[PM] "The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured."

Section 8.8.4 of the TSS states that the TOE does not provide any interface to view secret key data. All cryptographic data used by the TOE is protected from unauthorized disclosure by the FIPS-compliant cryptographic module and is described in the Security Policy documentation.

[AC] FRU_FLT.1
"*The evaluator shall check the TSS in order to determine that describes how the TSF ensures that it is enforcing the most up-to-date policy. If an a malicious user was able to disconnect their system and the TOE misses a policy update from Policy Management during this outage, it is expected that the updated policy will be received once communications are resumed."*

Section 8.9.1 of the TSS states that "a Webgate or Security Module will enforce decisions it has previously made or whatever policy is currently has regardless of whether or not it is able to communicate with the server components of the TOE." Also, the TSS states that if communication between the Webgate or Security Module fail with their respective server, the Webgate/Security Module will periodically attempt to query the server until it is available.

[PM] FTA_TSE.1
"*The evaluator shall examine the TSS to determine that all of the attributes on which a session can be denied are specifically defined."*

Section 8.10.1 of the TSS states that a Webgate can enforce denial of session establishment by limiting a subject's access to a protected resource based on day or time.

[AC+PM] FTP_ITC.1
[AC] "The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST."

[PM] "The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST."

Section 8.11.1 of the TSS states that for each of the identified channels, the TOE uses a third-party cryptographic module (RSA BSAFE Crypto-C Micro Edition v4.1.2) using TLS. The cryptographic module is FIPS 140-2 validated and included in the OAM Suite.

[PM] FTP_TRP.1
"The evaluator shall repeat the assurance activity for FTP_ITC.1 for each interface and cryptographic protocol that is provided by the TOE for remote administration."

Section 8.11.2 of the TSS states "The TOE uses a third-party cryptographic module, RSA BSAFE Crypto-C Micro Edition version 4.1.2, to implement trusted paths from a remote administrator to the OAM Console and OES Console using HTTPS."

2 Operational Guidance Assurance Activities

The evaluation team completed the testing of the Operational Guidance, which includes the review of the *Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria v1.0* (Supplemental AGD) document, and confirmed that the Operational Guidance contains all Assurance Activities as specified by the 'Standard Protection Profile for Enterprise Security Management Policy Management , version 2.1 [PMPP] and Standard Protection Profile for Enterprise Security Management Access Control [ACPP] , version 2.1. The Supplemental AGD contains installation, configuration and operational documentation for the use of Oracle Access Manager (OAM) and Oracle Entitlement Server (OES) in its evaluated configuration. The Supplemental AGD includes references to other guidance documents that must be used to properly install, configure, and operate the TOE in its evaluated configuration. The Supplemental AGD and its references to other Oracle Access Manager Suite guidance documents were reviewed to assess the Operational Guidance Assurance Activities. The Supplemental AGD contains references to these documents in Chapter 7 and these references can also be found below:

- 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 Access Manager Suite Version 11g Release 2 Common Criteria Evaluation Security Target v1.0
- 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
  Mainly focus on chapter 13 (Configuring Secure Sockets Layer Authentication) and chapter 14 (Using Oracle Wallet Manager)
- 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

The evaluators reviewed the PMPP and ACPP to identify the security functionality that must be discussed for the operational guidance. This is prescribed by the Assurance Activities for each SFR and the AGD SARs. The evaluators have listed below each of the SFRs defined in the PMPP and ACPP that have been claimed by the TOE (some SFRs are conditional or optional) as well as the AGD SARs, along with a discussion of where in the operational guidance the associated Assurance Activities material can be found.

If an SFR is not listed, one of the following conditions applies:

- There is no Assurance Activity for the SFR.
- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a different Assurance Activity (a testing Assurance Activity for the same SFR, a testing Assurance Activity for a different SFR, or a guidance Assurance Activity for another SFR).
- The Assurance Activity for the SFR does not specify any actions to review the operational guidance.

[PM] ESM_ACD.1 – *"The evaluator shall review the operational guidance to ensure that that it indicates the compatible Access Control product(s) as well as the allowable contents and means of identification of the access control policies that can be defined by the TOE."*

Section 5.3 of the Supplemental AGD discusses how the OAM Suite bundle includes the access control components that are associated with the OAM and OES Consoles. Once the suite is installed and configured, the OAM and OES consoles are the only policy management products that are authorized to manage the access control endpoints. This section also details how policies are defined by the administrator for each console and how each policy is given a unique name and/or identifier.

[PM] ESM_ACT.1 – *"The evaluator shall review the operational guidance to determine how to create and update policies, and the circumstances under which new or updated policies are transmitted to consuming ESM products (and how those circumstances are managed, if applicable)."*

Section 5.3 of the Supplemental AGD provides references to Oracle guidance documentation for detailed instruction for the administrator to create and update policies with in the TOE. Specifically, section 17 of Oracle Fusion Middleware Administrator's Guide for Oracle Access Management **[2]** discusses how to define policies in the OAM Console and section 4 of Oracle Fusion Middleware Administering Oracle Entitlements Server **[1]** discusses creation, modification and deletion of policies using the OES Console. The OES Console is the only console that transmits policies to its endpoint. Section 6 in the Oracle Fusion Middleware Administering Oracle Entitlements Server **[1]** discusses how the administrator transmits the policies to the Security Module for enforcement.

[PM] ESM_ATD.1 – *"The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure the object attributes."*

OAM
Section 5.3 of the Supplemental AGD states that the OAM Administrator is able to define a policy by the authentication level of the user. The Supplemental AGD also points to section 17 in the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management **[2]** for more detailed discussion and instructions for defining such a policy.

OES
Section 5.3 of the Supplemental AGD states that administrators are able to define policies according to attributes of the object being protected. The example that is given describes that a policy can be defined to only allow books with a specific author to be borrowed. The creation process of the policy is discussed in section 4 of Oracle Fusion Middleware Administering Oracle Entitlements Server **[1].**

[PM] ESM_ATD.2 – *"The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure these attributes."*

Section 5.3 of the Supplemental AGD states similar information to what is described in ESM_ATD.1, the OES administrator are able to define policies according to subject attributes. The example that is provided states that a policy can be defined to restrict or allow users with a specific attribute that is defined in the identity store. The creation process of the policy is discussed in section 4 of Oracle Fusion Middleware Administering Oracle Entitlements Server **[1].**

[PM] ESM_EAU.2 – *"The evaluator shall check the operational guidance in order to determine how the TOE determines whether an interactive user requesting access to it has been authenticated and how the TOE validates authentication credentials or identity assertions that it receives. If any IT entities authenticate to the TOE, the evaluator shall also check the operational guidance to verify that it identifies how these entities are authenticated and what configuration steps must be performed in order to set up the authentication."*

Section 5.1 of the Supplemental AGD states that the TOE is able to rely on external identity stores for its authentication. In the evaluated configuration, each console is protected by a Webgate that will call identity store to compare the stored credentials with what is entered by the user. The 'Configuring TLS for Identity Store (OID)' instruction in section 4 of the Supplemental AGD includes the configuration steps for the TOE to communicate with the identity store to make authentication decisions.

[PM] ESM_EID.2 – "*This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2."*

The description under the **[PM] ESM_EAU.2** operational guidance justification above demonstrates the necessary documentation for this functionality.

[AC+PM] FAU_GEN.1 – *[AC] "The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record. Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.*

"The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event."

[PM] "The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record. Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.

"The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event."

Section 5.4 of the Supplemental AGD discusses auditing/logging performed by OAM Suite. It summarizes the auditable events and audit record contents created by administrator as well as access attempts made against protected resources: "Audit data for OAM Suite is generated for both administrative activity and for access attempts made against resources that are being protected by the product." Below is list of the required fields within the audit record and an example taken directly from a record generated by the TOE.

Date and time of the event - 2016-07-19 21:23:40.948
Type of Event - PolicyCreation
Subject Identity – oamadmin
Outcome of the event – true

Section 5.4 of the Supplemental AGD also includes a table that displays an audit record for each of the requirements being claimed in the evaluation.

[AC] FAU_SEL.1 – *"The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target."*

Section 5.4 of the Supplemental AGD discusses how to change the level of audit that OAM will record and lists the different levels that the administrator can select and briefly describes each setting. The levels match those described in Section 8.2.2 of the ST.

OES is capable of selective auditing, however, the configuration for this setting is done by modifying a configuration file that resides on the underlying server that the TOE resides on and is considered to be in the operational environment. Thus, Section 5.4 of the Supplemental AGD states that in the evaluated configuration OES settings will not be configurable.

[PM] FAU_SEL.1 – *"The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target."*

Section 5.4 of the Supplemental AGD discusses how to change the level of audit that OAM will record and lists the different levels that the administrator can select and briefly describes each setting. The levels match those described in Section 8.2.3 of the ST.

OES is capable of selective auditing, however, the configuration for this setting is done by modifying a configuration file that resides on the underlying server that the TOE resides on and is considered to be in the operational environment. Thus, Section 5.4 of the Supplemental AGD states that in the evaluated configuration OES settings will not be configurable.

[PM] FAU_SEL_EXT.1 – *"The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target."*

Section 5.4 of the Supplemental AGD discusses how to change the level of audit that OAM will record and lists the different levels that the administrator can select and briefly describes each setting. The levels match those described in Section 8.2.2 and 8.2.3 of the ST.

OES is capable of selective auditing, however, the configuration for this setting is done by modifying a configuration file that resides on the underlying server that the TOE resides on and is considered to be in the operational environment. Thus, Section 5.4 of the Supplemental AGD states that in the evaluated configuration OES settings will not be configurable.

[AC] FAU_STG.1 – *"The evaluator shall examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and ―cleared‖ periodically by sending the data to the audit server."*

The supplemental AGD in Section 5.4 states that all of the audit data generated by the TOE is stored locally on the underlying server's file system. The audit data is also able to be transmitted simultaneously to an external database for storage.

[AC+PM] FAU_STG_EXT.1 – *[AC] "The evaluator shall check the operational guidance in order to determine that it lists any configuration steps required to set up audit storage. If audit data is stored in a remote repository, the evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established,* *how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established."*

[PM] "The evaluator shall check the operational and preparatory guidance in order to determine that they describe how to configure and use an external repository for audit storage. The evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established."

(1) The Supplemental AGD Section 4 discusses the initial installation of the TOE. The database that stores the audit data is installed prior to installing the TOE. Per Section 5.4 of the Supplental AGD, configuration of the TOE to connect to the database is discussed in Section 8.7.1 of Oracle Fusion Middleware Administrator's Guide for Oracle Access Management **[2]**. However, Section 8.7.1 does not include the secure communications configuration. Configuring the TOE for secure communications using TLS is discussed in Section 5.4 of the Supplemental AGD. (2) Section 5.4 of the Supplemental AGD document provides a description of the interface in which the TOE connects to the database. (3) Section 5.4 of the Supplemental AGD document states that when the connection from the TOE to the database is lost, the audit data will still be stored locally on the underlying server. When the connection to the database is restored, the audit data will be sent automatically for storage.

[AC] FCO_NRR.2 – *"The evaluator shall check the operational guidance in order to determine how the TOE confirms evidence of received policy data back to the Policy Management product that originally sent it that policy data. This should include the contents and formatting of the receipt such that the data that it contains is verifiable."*

Section 5.3 of the Supplemental AGD states that once the policy is consumed by the Security Module, the OES console is updated with the status of the Security Module and the policy version applied is displayed.

[AC+PM] FCS_TLS_EXT.1 – *[AC] "The evaluator shall check the operational guidance to ensure that it contains instructions on configuring the TOE in the Operational Environment so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements or an administrator is expected to deploy a particular client to access the TOE)."*

[PM] "The evaluator shall check the operational guidance to ensure that it contains instructions on configuring the TOE in the Operational Environment so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements or an administrator is expected to deploy a particular client to access the TOE)."

Section 4 of the Supplemental AGD discusses step by step procedures for configuring the TOE to conform to the TLS requirements. The configurations include information for the connections between the TOE and the operational environment components and includes restrictions on TLS versions and ciphersuites in order to meet this requirement.

[AC] FDP_ACF.1 – *"The evaluator shall check the operational guidance in order to verify that it provides instructions on how it receives access control policy data. For example, if the TOE receives policy rules in some defined language, the operational guidance shall indicate the statements in this language that correspond with the activities that are defined in Table 15 above.*

The evaluator shall also check the operational guidance to verify that it provides information about how the TOE's rule processing engine. This allows administrators to design access control policies with appropriate expectations for how they will be enforced."

(1) Section 5.3 of the Supplemental AGD indicates that OAM Suite includes both the policy management and access control components. Thus, the TOE maintains its own access control policy data and does not receive it from a third-party source. (2) Section 5.3 also describes that the TOE acts on a deny-by-default basis for protected resources, how rules are created, and the manner in which rules are processed.

[PM] FIA_USB.1 – *"The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF."*

Sections 5.1 and 5.2 of the Supplemental AGD indicate that the TOE has web applications for both OAM and OES components and the administrators using these interfaces have their credentials and roles stored in an external identity store called the 'system store'. Configuration of the 'system store' can be found in section 4.4 of the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management **[2]**. Section 5.3 of the Supplemental AGD also states "When enforcing access control policies, Security Modules rely on subject data provided by environmental identity stores. Information about how to configure an identity store to be associated with a Security Module can be found in Fusion Middleware Administering Oracle Entitlements Server under Section 10.3, "Configuring Identity Directory Service Profiles"."

[PM] FMT_MOF.1 – *"The evaluator shall review the operational guidance in order to determine what restrictions are in place on management of these attributes and how the TSF enforces them. For example, if management authority is role-based, then the operational guidance shall indicate this."*

Section 5.2 of the Supplemental AGD describes the administrative roles for the OAM and OES components. This section also describes that the administrative roles are stored in the 'system store' and directs to Section 4.4 of the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management **[2]** for its configuration. Section 5.2 also refers to Section 11.5 in the Oracle Fusion Middleware Administering Oracle Entitlements Server **[1]** for the ability of the System Administrator to delegate Policy Domain Administration to other users.

[AC] FMT_MOF.1(1) – *"The evaluator shall check the operational guidance in order to determine that it describes the process by which the TOE can be associated with a Policy Management product and how that product is subsequently used to manage the TOE."*

Section 5.3 of the Supplemental AGD indicates that OAM Suite includes both the policy management and access control components. Thus, the TOE provides the ability to manage itself. Section 4 of the Supplemental AGD describes the overall installation and configuration of the TOE, to include connections between various components. Section 5.2 of the Supplemental AGD describes the overall administrative roles and privileges for managing the TOE. The Supplemental AGD as a whole and the specific sections of other documents to which it refers describe the ability to manage the TOE.

[PM] FMT_MOF_EXT.1 – *"The evaluator shall check the operational guidance in order to determine that it provides instructions for how to connect to an Access Control product and what privileges are required to perform management functions on it once the connection has been established."*

Section 5.3 of the Supplemental AGD indicates that OAM Suite includes both the policy management and access control components. Thus, the TOE provides the ability to manage itself. Section 4 of the Supplemental AGD describes the overall installation and configuration of the TOE, to include connections between various components. Section 5.2 of the Supplemental AGD describes the overall administrative roles and privileges for managing the TOE. The Supplemental AGD as a whole and the specific sections of other documents to which it refers describe the ability to manage the TOE.

[AC] FMT_MSA.1 – "*The evaluator shall also confirm that the operational guidance defines how authorizations to manage the defined security attributes are derived so that an administrator will know how to configure separation of duties."*

Section 5.2 of the Supplemental AGD describes the administrative roles for the OAM and OES components. This section also describes that the administrative roles are stored in the 'system store' and directs to Section 4.4 of the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management **[2]** for its configuration. Section 5.2 also refers to Section 11.5 in the Oracle Fusion Middleware Administering Oracle Entitlements Server **[1]** for the ability of the System Administrator to delegate Policy Domain Administration to other users.

[AC] FMT_MSA.3 – *"The evaluator shall review the operational guidance in order to ensure that it warns the reader of the restrictive nature of default values and provides instructions on how to override them."*

Section 5.3 in the Supplemental AGD provides a warning to readers that states the TOE provides a "deny-by-default" rule to all of the protected resources. Additionally, Section 5.3 of the Supplemental AGD discusses how to define policies and references Oracle documentation in order to override the initial "deny-by-default" rule.

[PM] FMT_MSA_EXT.5 – *"If the TOE requires manual intervention in order to resolve contradictory policy data, the evaluator shall review the operational guidance in order to verify that it provides a summary of contradictory policy situations and the steps that must be taken in order to resolve them. If the TOE's policy engine prevents such contradictions, the evaluator shall review the operational guidance in order to verify that it describes how the TSF reconciles any contradictory policy data (such as different rules simultaneously allowing and denying a certain behavior)."*

Section 5.3 of the Supplemental AGD describes the possible scenarios that contradictory policies may occur. In each scenario, the policy engine resolves the contradiction as described in this section.

[AC+PM] FMT_SMF.1 – *[AC] "The evaluator shall check the operational guidance in order to ensure that it describes how to configure the TOE to interface with the compatible products discussed in the TSS. The evaluator shall also check the operational guidance to verify that it provides instructions for performing each of the defined management functions."*

[PM] "The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish."

Section 5.3 of the Supplemental AGD indicates that OAM Suite includes both the policy management and access control components. Thus, the TOE provides the ability to manage itself. Section 4 of the Supplemental AGD describes the overall installation and configuration of the TOE, to include connections between various components. Section 5 of the Supplemental AGD describes management function claimed under FMT_SMF.1 and in some instances, references specific sections of other Oracle documentation that provide additional information on how to perform those functions and the results of performing those functions. All management functions claimed under FMT_SMF.1 were associated with an SFR that was also reviewed under the Operational Guidance Assurance Activities within this AAR.

[AC+PM] FMT_SMR.1 – *[AC] "The evaluator shall review the operational guidance in order to verify that it discusses the various administrative role(s) that are used to manage the TSF and any applicable steps that are required for an administrator to assume such a role."*

[PM] "The evaluator shall review the operational guidance in order to verify that it provides instructions on how to assign users to roles. If the TSF provides only a single role that is automatically assigned to all users, then the evaluator shall review the operational guidance to verify that this fact is asserted."

Section 5.2 of the Supplemental AGD describes the administrative roles for the OAM and OES components. This section also describes that the administrative roles are stored in the 'system store' and directs to Section 4.4 of the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management **[2]** for its configuration. Section 5.2 also refers to Section 11.5 in the Oracle Fusion Middleware Administering Oracle Entitlements Server **[1]** for the ability of the System Administrator to delegate Policy Domain Administration to other users.

[AC] FPT_FLS_EXT.1 – *"The evaluator shall check the operational guidance (and developmental evidence, if available) in order to determine that it discusses how the TOE is deployed in relation to other ESM products. This is done so that the evaluator can determine the expected behavior if the TOE is unable to interact with its accompanying Policy Management product."*

Section 5.3 of the Supplemental AGD indicates that OAM Suite includes both the policy management and access control components. Thus, the TOE provides the ability to manage itself. Section 4 of the Supplemental AGD describes the overall installation and configuration of the TOE, to include connections between various components. Section 5.5 of the Supplemental AGD discusses how the Webgate and Security Module protect the resources if the communication between itself and the OAM/OES Server becomes severed. The Webgate will enforce the last decision that was made prior to the outage and the Security Module will continue to enforce the policies that have been stored locally.

[AC] FPT_RPL.1 – *"If the method of replay detection is configurable, the evaluator shall check the operational guidance in order to determine that it provides instructions for setting up and configuring the replay detection mechanism. This may be simple (e.g. setting up and enabling a TLS channel with shared secret) or complex (e.g. defining specific policy attributes that are positively associated with unauthorized changes), depending on how specifically replay detection is implemented by the TSF."*

Section 4 of the Supplemental AGD discusses how to configure the OAM/OES Server to communicate with its corresponding Webgate/Security Module using TLS. This section points to Oracle documentation for specific instructions. Also, Section 5.5 of the Supplemental AGD states the Webgate/Security Module is only able to be managed by the authorized OAM/OES Server that it is enrolled to.

[AC] FRU_FLT.1 – *"The evaluator shall check the operational guidance in order to verify that it discusses how the TSF receives the latest policy from the Policy Management product once a communications failure has been resolved, including any options that an administrator has in configuring this capability."*

Section 5.5 in the Supplemental AGD states that the Webgate will countinuously attempt to query the sever to see if it is available and whether or not there is an updated policy. Thus, once a connection is re-established the Webgate will download any new policies. Section 5.5 also states that policy distribution will need to be re-initiated after restoration of connectivity.

[AC] FTA_TSE.1 – *"The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS."*

Section 5.6 of the Supplemental AGD references Oracle documentation for the instructions to define policies based on the day and time attributes.

[AC+PM] FTP_ITC.1 – *[AC]* "*The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity."*

[PM] "The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity."

Configuration of trusted communications is performed by following the relevant steps outlined in Section 4 "Secure Installation and Configuration" portion of the Supplemental AGD. This information addresses the requirements of the AGD AA for this SFR.

[PM] FTP_TRP.1 – *"The evaluator shall repeat the assurance activity for FTP_ITC.1 for each interface and cryptographic protocol that is provided by the TOE for remote administration."*

Configuration of trusted communications is performed by following the relevant steps outlined in Section 4 "Secure Installation and Configuration" portion of the Supplemental AGD. This information addresses the requirements of the AGD AA for this SFR.

AGD_OPE.1 – *[AC] "The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE."*

[PM] "The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE."

The Security Target states that the TSF uses RSA BSAFE Crypto-C Micro Edition version 4.1.2 running in a FIPS-compliant mode of operation. There is no configuration required to the TOE to enter FIPS mode. However, the TOE does not communicate with the external IT entities in a secure manner by default. This configuration needs to be performed by the installer in order to be compliant with the FCS requirements. Section 3 in the Supplemental AGD includes the same description as the Security Target, the necessary cryptographic engine warning, and informs the reader of the need to configure TLS which is covered by Section 4 of the Supplemental AGD.

AGD_PRE.1 – *[AC] "As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST."*

[PM] "As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST."

The TOE is a software-based solution that can be installed on compatible operating systems. Thus, the evaluated configuration is not based on hardware platforms as long as the minimum requirements are met. Additionally, the section of the Supplemental AGD titled, "Evaluated Configuration of the TOE," specifies the components to be used in the operational environment to work with the TOE in its evaluated configuration. This is the same list of operational environment components shown in the ST.

3 Test Assurance Activities (Test Report)

The following sections demonstrate that all ATE Assurance Activities for the TOE have been met. This evidence has been presented in a manner that is consistent with the "Reporting for Evaluations Against

NIAP-Approved Protection Profiles" guidance that has been provided by NIAP. Specific test steps and associated detailed results are not included in this report in order for it to remain non-proprietary. The test report is a summarized version of the test activities that were performed as part of creating the Evaluation Technical Report (ETR).

3.1 Platforms Tested and Composition

The TOE is a software-based TOE. The evaluation team set up the test environment for the independent functional testing using the operational environment components listed in the table below:

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
Identity Store	• Oracle Internet Directory 11g • Oracle Unified Directory 11g
Web Browser (for administrative UI access)	• Firefox 50

This allowed the evaluation team to perform all test assurance activities across the TOE and over the relevant interfaces. The evaluation team performed testing of the TSF functionality through the web UI, which is the only management interface available to the TOE. The testing is consistent with the use of the interfaces defined within the ST. Thus, the testing of the interfaces was based upon testing SFR functionality related to user actions over each interface.

3.2 Assessment of the Oracle Test Environment

The purpose of this section is ensure that Oracle's test environment and Booz Allen's use of this environment during testing conforms with the expectations of NVLAP Handbooks 150 and 150-20, and Labgram #078/Valgram #098.

3.2.1 Physical Assessment

Oracle Headquarters located in Redwood City, CA is the physical location for the Oracle Access Manager Suite test environment. Booz Allen reviewed the physical security controls of the test environment and interviewed Oracle employees to ensure that the Oracle Access Manager Suite testing environment was secure. Booz Allen has found that Oracle Headquarters has similar access controls to Booz Allen's CCTL. The Oracle location requires a person to be an Oracle employee to enter the building or be escorted as a visitor by an Oracle employee. The building is primarily controlled by a badge access system for employees whereas visitors must sign in and wear a temporary visitor nameplate. The laboratory where the underlying servers that OAM Suite was installed on are located in a secured internal room located at the Oracle Headquarters location. Thus, physical access to the OAM and OES servers would require a person to pass through the badge access control by being an Oracle employee or a visitor being escorted by an Oracle employee as well as have access to the internal room where the servers are located. The evaluator conducted a daily inspection of the space and equipment for any signs of tampering of the space or equipment and found no such evidence of malicious tampering. Booz Allen finds that these physical access controls are satisfactory to protect the environment from unwanted physical access.

3.2.2 Logical Assessment

The only method to access the server was locally with the proper credentials (username/password). Thus, the functional testing could not be executed remotely from the physical test environment. At the end of each work day, the servers were locked in a secure room. Any configuration performed by Oracle personnel during the functional testing timeframe was conducted using the Supplemental AGD as guidance and under the supervision of the evaluators. Booz Allen finds these logical access controls are satisfactory to protect the environment from unwanted logical access.

3.3 Test Cases

The evaluation team completed the functional testing activities within the vendor's laboratory environment. The evaluation team conducted a set of testing that includes all ATE Assurance Activities as specified by 'Standard Protection Profile for Enterprise Security Policy Management, version 2.1' [PMPP] as well as 'Standard Protection Profile for Enterprise Security Access Control, version 2.1' [ACPP]. The evaluators reviewed both PPs to identify the security functionality that must be verified through functional testing. This is prescribed by the Assurance Activities for each SFR.

If an SFR is not listed, one of the following conditions applies:

- The Assurance Activity for the SFR specifically indicates that it is simultaneously satisfied by completing a test Assurance Activity for a different SFR.
- The Assurance Activity for the SFR does not specify any actions related to ATE activities.

Note that some SFRs may not have Assurance Activities associated with them at the element level. In such cases, testing for the SFR is considered to be satisfied by completion of all Assurance Activities at the component level.

The following lists the test objective, test instructions, test steps, and test results for each ATE Assurance Activity. Note that unless otherwise specified, the test configuration is to be in the evaluated configuration as defined by the Supplemental AGD. For example, if some tests require the TOE to be brought out of the evaluated configuration, a note will be included in the test item to that effect.

3.3.1 Enterprise Security Management

001	**[PM]ESM_ACD.1**
Test Purpose:	The evaluator shall test this capability by using the TOE to create a policy that uses the full range of subjects, objects, operations, and attributes and sending it to a compatible Access Control product for consumption. The evaluator will then perform actions that are mediated by the Access Control product in order to confirm that the policy was applied appropriately. The evaluator will also verify that a policy identifier is associated with a transmitted policy by querying the policy that is being implemented by the Access Control product.

Test Procedures:

OAM

1. In the OAM console select the “webgate1” resource and view the authentication and authorization policies that are attached.

OES

1. In the OES Console, select a domain that has a resource attached.
2. Click the “Policy Distribution” tab and view the Security Modules and the version of policy that is attached.

Synopsis

The first portion (paragraph) of this assurance activity describes creating policies that cover the full range of subjects, objects, operations, and attributes. FDP_ACF.1 (Test Case 012) satisfies this requirement as the evaluator created policies that covers this range. FDP_ACF.1 (Test Case 012) has a test scenario that covers each of the capabilities listed:

- **Subject: User, Object: URLs, Operation: Access via HTTP operation - This was tested in test case 012 under "Webgate URLs".**
- **Subject: User, Object: Forms, Operation: HTTP GET - This was tested in test case 012 under "Webgate Forms".**
- **Subject: User, Object: Forms, Operation: HTTP POST - This was tested in test case 012 under "Webgate Forms".**
- **Subject: User, Object: Files, Operation: Open - This was tested in test case 012 under "Open and Download protected file".**
- **Subject: User, Object: Files, Operation: Download - This was tested in test case 012 under "Open and Download protected file".**
- **Subject: User, Object: Executable Script, Operation: Execute was tested in Test Case 012 under "Executable Script".**
- **Subject: User, Object: Executable Script, Operation: Enable was tested in Test Case 012 under "Executable Script".**
- **Subject: User, Object: Executable Script, Operation: Disable was tested in Test Case 012 under "Executable Script".**

Please refer to Test Case 012 within this test plan as well as the test matrix for an explanation of each of the tests scenarios that were completed.

The second portion of this assurance activity requires the evaluator to query the policy that was transmitted on the console. The test procedures for this are handled by Test Case 001 above.

Test Result	Pass

002	**[PM]ESM_ACT.1**
Test Purpose:	The evaluator shall test this capability by obtaining one or more compatible Access Control products and configuring the TOE to manage them. Then, following the procedures in the operational guidance for both the TOE and the Access Control product, the evaluator shall create a new policy and ensure that the new policy defined in the by the TSF is successfully transmitted to, consumed by, and enforced in an Access Control product, in accordance with the circumstances defined in the SFR. In other words, (a) if the selection is completed to transmit after creation of a new policy, then the evaluator shall create the new policy and ensure that, after a reasonable window for transmission, the new policy is installed; The evaluator shall then make a change to the previously created policy and then repeat the previous procedure to ensure that the updated policy is transmitted to the Access Control component in accordance with the SFR-specified circumstances. Lastly, as updating a policy encompasses deletion of a policy, the evaluator shall repeat the process a third time, this time deleting the policy to ensure it is removed as an active policy from the Access Control component.

Test Procedures:

Security Module:

1. Using the OES Console create a Security Module policy with the name Library.
   a. From the “Authorization Management” tab, click on “Applications” and then click the icon for a new application.
   b. Name the application “library” and click “Save”. Close the tab.
   c. Click the application that was just created. Under “Resource Type” click “New”.
   d. In the “Actions” create “buy, sell, review, any”
   e. Name the resource type “Book”. Click “New” and give the resource type the action or buy and click “Save” and close the tab. **NOTE: each action needs to be entered in separately**.
   f. Under “Resource” click “New” and name the resource. “Book4Sell” **NOTE: The resource name should be whatever resource that is being protected.**
   g. From the same tab, click “Create Policy”. Name the policy “Policy4BookSell”
   h. Ensure that the “Permit” radio button is selected and click green plus to add a principal to the policy. **NOTE: Every policy is a deny by default. The permit button allows whichever principal that is selected here access to the resource.**
   i. In the “Users” tab click “search”. Select the user that was created in the setup and click “add selected” and then click “Add Principals”.
   j. On the “Authorizations Policies” tab, click the arrow next to the resource under the “targets” section. Check read and write buttons and then click “Save”.
   k. In the “System Configuration” tab, click on “Security Modules”. Select the security module that was installed and configured in the setup and click “add”. In the pop-up search for the application created in step a and click “add”.
   l. In the “Authorization Management” tab, open the application and click “policy distribution”.
   m. Select the security module and click distribute.
2. After the policy has been deployed, ensure the policy is being enforced by performing the actions that were included in the authorizations policy as the user that was added as a principal and a user that is not a principal.
3. In the OES console query the policy by clicking the “Application” that was created and searching for the policy that was deployed.
4. Repeat step 10. It will fail because no 2 policies can be created with the same UID (policy name).

5. Modify the policy that was created in step 8 and distribute to the endpoint.
6. Perform an action to show the policy has taken effect.

7. Query the policy to show the UID.
8. Delete the policy and perform an action that will show that the resource is no longer protected.
9. Collect audit records that were generated for the creation, modification and deletion of the policy. Ensure that the Policy Name (Application Domain) (unique identifier) of the policy is included in the record.
10. Collect audit records for ‘Transmission of policy to Access Control products’ and ensure that the destination of the policy is included in the record.

Synopsis

This AA is testing the ability of the Policy Management product to transmit a policy to the Access Control product for consumption and enforcement. Lastly the AA is testing the ability to delete the policy and ensure the policy is removed.

Step 1 of this test case involves creating the policy on the OES Console and distributing the policy to the Security Module.
Step 2 of this test case is proving that the policy has been absorbed by and is being enforced by the Security Module.
Step 5 and 6 of this test case is modifying the current policy, deploying the new policy and ensuring the change to policy has taken affect.
Step 8 and 9 of this test case is deleting the policy and ensuring that the policy is no longer enforced by the Security Module.

The policies that are distributed by the OES Console are pushed to the Security Module as soon as the administrator pushes the “distribute” button. There is no configuration to allow the policies to be deployed at periodic intervals.

Test Results	PASS

003	**[PM]ESM_ATD.1**
Test Purpose:	The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the subject attributes that were associated with the policy

Test Procedures:

Webgate (Authentication Level)

1. Using the OAM Web Console, create a Webgate policy with the name “CCTL Policy 01”.
    - a. From the Launch Pad, click “Application Domains”.
    - b. Click “Create Application Domain”.
    - c. Give the Application Domain the Name: “Webgate1”.
    - d. Click “Apply” to create the Application Domain.
    - e. Click the “Resources” tab, then “Create” to Create Resource.
    - f. Choose Resource Type “HTTP”.
    - g. Choose the target host for the Host Identifier.
    - h. In the Resource URL input the resource to be protected: “/welcome_classic.html”. Apply the configuration.
    - i. On the “Authentication Policy” tab create a new Authentication Policy with the name “Test Policy1”. **Note: This authentication policy has a higher level of authentication.**
    - j. Add a Resource to TestPolicy1”. Apply the configuration.
    - k. On the “Authorization Policy” tab use the default policy “Protected Resource Policy”.
        - i. In the “Conditions” tab click “add”.
        - ii. Name the Condition “Identity” and make the type Identity.
        - iii. On the same tab under conditions, click “add” “Users and groups”. Search for the user “test2”.
        - iv. On the rules tab, add the identity condition to the “selected conditions” under the Allow rule and remove “TRUE”.
    - l. Add a Resource to “Protected Resource Policy”. Apply the configuration.
2. Repeat the steps above for creating a different resource using “index.html”

3. After the policy has been created ensure that it is being enforced by performing an action that will enforce the policy.
    - a. Navigate to the protected HTTP resource and verify that it behaves according to the policy
4. Change the authentication policy for the resource “index.html” to “Protected Resource Policy”.
5. Repeat step 3.

6. Collect the audit records for the association of the attributes to the objects being protected.

Security Module (Administrator-defined attribute)

1. Create a policy within the OES that protects a resource.
    - a. Within the policy add only allow users access to review a book with the author name “Jones”.
2. Deploy the policy to the Security Module.
3. Attempt to access the resource as a user that does not have the attribute.
4. Access the resource as a user that has the role.
5. Collect the audit records for the association of the attributes to the objects being protected.

Synopsis **This AA requires the evaluator to create and distribute a policy that contain object attributes. According to the Security Target the attributes that belong to individual objects are "Authentication Level" and "Administrator-defined attributes". Webgate (Authentication Level) describes the test steps testing the authentication level policy and Security Module (Administrator-defined attribute) describes the test steps for testing the administrator defined attribute policy.**	
Test Results	PASS

004	**[PM]ESM_ATD.2**
Test Purpose:	The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the subject attributes that were associated with the policy
Test Procedures: **Security Module (Administrator-defined attribute)** 1. Create a policy within the OES that protects a resource. a. Within the policy add only allow users access to review a book with the author name "Jones". 2. Deploy the policy to the Security Module. 3. Attempt to access the resource as a user that does not have the attribute. 4. Access the resource as a user that has the role. 5. Create a policy within the OES that protects a resource. a. Within the policy add only allow users with a specific attribute defined (mail=john@oestest.com) to access the resource. 6. Deploy the policy to the Security Module. 7. Attempt to access the resource as a user that does not have the attribute. 8. Access the resource as a user that has the role 9. Collect the audit records for the association of the attributes to the subjects. **Synopsis** **This AA requires the evaluator to create and distribute a policy that contain subject attributes. According to the Security Target the attributes that belong to individual subjects "Administrator-defined attributes". In this test case, the administrator-defined attribute is the email address "mail=john@oestest.com" that is attached to the user account being used in this test.**	
Test Results	PASS

005	**[PM]ESM_EAU.2**
Test Purpose:	The evaluator shall test this capability by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied. If any IT entities authenticate to the TOE, the evaluator shall instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF. Note that positive testing of the identification and authentication is assumed to be tested by other requirements because successful authentication is a prerequisite to manage the TSF (and possibly for the TSF to interact with external IT entities).
Test Procedures: **NOTE: Perform these tests on both the OAM and OES Consoles.** **LDAP (OUD)** 1. Authenticate to the server with a valid username and valid password. 2. Attempt to authenticate to the server using an invalid username and valid password. 3. Attempt to authenticate to the server using a valid username and invalid password. 4. Attempt to authenticate to the server using an invalid username and valid password. 5. Collect audit records for all use of the authentication mechanism. (successful and unsuccessful attempts) **LDAP (OID)** 6. Repeat the steps in the OUD section except use a user that is created in the OID. 7. Collect audit records for all use of the authentication mechanism. (successful and unsuccessful attempts)	
Test Results	PASS

3.3.2 Security Audit

006	**[AC+PM]FAU_GEN.1**
Test Purpose:	The evaluator shall test the TOE’s audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST. This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.

Test Procedures:

Starting and stopping of Auditing

OAM Console
Turn Auditing Off

1. Authenticate to the OAM GUI.
2. Click on the “Configuration” tab.
3. In the “Settings” area, click “View” and select “Common Settings”
4. At the “Filter Preset” menu select “None” and click “Apply” at the top right corner of the page.
5. Collect the audit record that is produced from the configuration change.

Turn Auditing On

6. Repeat steps 1-3 above.
7. At the “Filter Preset” menu select “All” and click “Apply” at the top right corner of the page.
8. Collect the audit record that is produced from the configuration change.

OES Console
Modify the “jps-config.xml” file.

9. In the auditing portion of the file change the following setting
   <property name="audit.filterPreset" value="None"/>
10. Save the file and restart the server.

Modify the “jps-config.xml” file.

11. In the auditing portion of the file change the following setting
    <property name="audit.filterPreset" value="ALL"/>
12. Save the file and restart the server
13. Collect the audit record that is produced from the configuration change.

NOTE: Audit records are not generated because this is done in the operational environment not on the TOE itself.

The remainder of this assurance activity is satisfied with the collection of audit records from the other tests in the evaluation. The audit records collected in the course of the testing were compared to the information defined within the test case that produced the audit record as well as the correct presentation of the audit record as defined in the Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria version 1.0. All audit records defined in the Security Target were generated through the course of this testing.

Test Results	PASS

007	[AC+PM]FAU_SEL.1/[PM]FAU_SEL_EXT.1
Test Purpose:	The evaluator shall test this capability by using a compatible ESM Policy Management or ESM Secure Configuration Management product to configure the TOE in the following manners: - All selectable auditable events enabled - All selectable auditable events disabled - Some selectable auditable events enabled For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded.

Test Procedures:

OAM:

1. Navigate to the Oracle Access Management (OAM) Console: https://linux61.cctl.com:7504/oamconsole
2. Authenticate to the OAM Console as the administrator.
3. Click on “Configuration” on the top-right navigation bar.
4. Click on “View” under Settings and choose “Common Settings”.
5. Ensure the “Filter Enabled” checkbox is checked.
6. Choose “All” from the Filter Preset drop-down.
7. Click “Apply” to commit the configuration change.
8. Restart AdminServer and OAM Servers
   a. Restart AdminServer by navigating to the IAM Access Domain WebLogic Server: https://linux61.cctl.com:7504/console
   b. Authenticate to the IAM Access Domain WebLogic Server as the WebLogic administrator
   c. Under “Domain Structure” navigate to “IAMAccessDomain” > “Environment” > “Servers”. Click on the “Control” tab.
   d. Ensure the checkbox for “AdminServer(admin)” is checked and then Shutdown and Start the server instance.
9. Perform a subset of functions that are in the “AuditFilter.txt” file.
10. Review the audit log file and database to verify that the events performed in Step 9 were logged or not logged according to the Level. (i.e. None, Low, Medium, or All)
11. Repeat Steps 1-5.
12. Choose “None” from the Filter Preset drop-down.
13. Repeat Steps 7-10.
14. Repeat Steps 1-5.
15. Choose “Low” from the Filter Preset drop-down.
16. Repeat Steps 7-10.
17. Repeat Steps 1-5.
18. Choose “Medium” from the Filter Preset drop-down.
19. Repeat Steps 7-10.
20. Collect audit records for ‘All modifications to audit configuration’

Synopsis:

The purpose of this Test is not to verify that the TOE produces all audit records when it is in its default configuration of auditing all events. This is accomplished through Test 006 [AC+PM]FAU_GEN.1 and the remainder of the tests performed in the evaluation. The audit records collected in the course of the testing were compared to the information defined within the test case that produced the audit record as well as the correct presentation of the audit record as defined in the Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria version 1.0. Note: This Test does satisfy Test 006 [AC+PM]FAU_GEN.1 reliance on the other tests to validate the entire audit record set because step 20 requires the tester to collect the audit records for ‘All modifications to audit configuration’ as defined by

[AC]FAU_SEL.1, [PM]FAU_SEL.1 and [PM]FAU_SEL_EXT.1 produced by this Test. **The purpose of this Test is to verify when the TOE has been configured to audit less than all auditable activities, that the TOE only audits the activities it is supposed to at that level. Through the completion of this test the evaluation team changed the audit level from All to None to Low to Medium (Steps 6, 12, 15, 18), performed a set of functions that would either result in audit records at each level or not result in audit records at each level (Step 9 – repeated), and then reviewed the audit log file to verify that it contained the audit records that were supposed to be produced at each level and did not contain the audit records that were not supposed to be produced at each level (Step 10 – repeated). In all cases, when the evaluation team reviewed the audit log file and database during Step 10, the evaluation team found that the TOE audited or did not audit the functions as described by the ST.**	
Test Results	PASS

008	**[AC]FAU_STG.1**
Test Purpose:	The evaluator shall test this capability by attempting to access locally-stored audit data without authorization and observe that the attempts fail. They shall also observe that the space allocated for audit storage is consistent with the TSF's capabilities.
Test Procedures: The audit data is not stored locally within the TSF. All audit data is either sent to the underlying platform or to an external database. There is no mechanism for any user to access this data from within the TOE.	
Test Results	N/A

009	**[AC+PM]FAU_STG_EXT.1**
Test Purpose:	The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.

Test Procedures:
OAM:

1. Sever the connection between the external remote database and the OAM Web Console so that audit records generated by the OAM Web Console are unable to be transmitted to the external remote database.
   a. On the server where the remote DB resides, navigate to the DB home.
   b. Shutdown the database using the following commands - ./sqlplus / as SYSDBA
   Shutdown immediate
2. Attempt to authenticate to the OAM Web Console using invalid credentials.
3. Restore the connection between the external remote database and the OAM Web Console so that audit records that were generated by the OAM Web Console while the connection to the database was unavailable are synchronized with the external remote database.
   a. On the server where the remote DB resides, navigate the DB home.
   b. Start the database using the following commands - ./sqlplus / as SYSDBA
   startup
4. Ensure that the audit records residing on the underlying filesystem are transmitted to and received by the external remote database upon connection restoration.

OES:

5. Sever the connection between the external remote database and the OES Web Console so that audit records generated by the OES Web Console are unable to be transmitted to the external remote database.
   a. On the server where the remote DB resides, navigate the DB home.
   b. Shutdown the database using the following commands - ./sqlplus / as SYSDBA
   Shutdown immediate
6. Attempt to authenticate to the OES Web Console using invalid credentials.
7. Restore the connection between the external remote database and the OES Web Console so that audit records that were generated by the OES Web Console while the connection to the database was unavailable are synchronized with the external remote database.
   a. On the server where the remote DB resides, navigate the DB home.
   b. Start the database using the following commands - ./sqlplus / as SYSDBA
   startup
8. Ensure that the audit records residing on the underlying filesystem are transmitted to and received by the external remote database upon connection restoration.

Synopsis

The first portion of this AA requires the evaluator to configure the TOE to send audit data to external storage and ensure that the local audit data and the external audit data is identical.

The evaluation team verified audit data in the external storage is identical to the audit records stored on the underlying file system.

The second portion of this AA requires the evaluator to sever the connection between the TOE and the external audit server and ensure the audit data is sent upon the connection being re-established. **The test steps above describe how this portion of the AA was satisfied. The evaluator observed through Wireshark that the connection was interrupted and re-established.** **Lastly, the AA requires this channel to be encrypted as described in FTP_ITC.1 (Test Case 027). The trusted channel and all of the supporting evidence is described in FTP_ITC.1 test case.**

Test Results	PASS

3.3.3 Communications

010	**[AC]FCO_NRR.2**
Test Purpose:	The evaluator shall test this capability by configuring an environment such that the TOE is allowed to accept a policy from a certain source, sending it a policy from that source, observing that the policy is subsequently consumed, and that an accurate receipt is transmitted back to the Policy Management product within the time interval specified in the ST. The evaluator confirms accuracy by using the Policy Management product to view the receipt and ensure that its contents are consistent with known data.

Test Procedures:

OES Console

1. In an application domain, create a policy that allows a user to open a file and distribute the policy to the Security Module.
2. From the Authorization Management tab click the arrow on the left of “Applications”. Select the application that is being used from step 1.
3. Select the “Policy Distribution Tab”
4. Select the Security Module that the policy was distributed to and click the arrow to the left.
5. Modify the policy to deny the user the ability to open the same file from step 1.
6. Repeat step 4 and see that the version # has been updated.
7. Collect the audit record for ‘The invocation of the non-repudiation service’ and ensure that it contains identification of the information, the destination, and a copy of the evidence provided

Synopsis

The ability to configuring an environment such that the TOE is allowed to accept a policy from a certain source is completed through the overall configuration of the TOE, particularly the Security Module and the OAM Server. These procedures demonstrate that the currently consumed policy is identified through a version number in the OES Console. Thus, changing the policy and pushing it to the Security Module will result in the policy version number being updated in the OES Console indicating that it was consumed and the OES Server received a confirmation that it was applied. The evaluation team also reviewed the audit records to confirm that a record was produced for the invocation of the non-repudiation service.

NOTE: **The receipt action is immediate (<1 second), so the interval cannot be assessed.**

Test Results	PASS

3.3.4 Cryptographic Support

Test cases for [AC+PM]FCS_CKM.1, [AC+PM]FCS_COP.1(1), [AC+PM]FCS_COP.1(2), [AC+PM]FCS_COP.1(3), [AC+PM]FCS_COP.1(4), and [AC+PM]FCS_RBG_EXT.1 are not included within this section. This is because the ATE Assurance Activities have been satisfied by the vendor having the cryptographic algorithms provided by the TOE's assessment under the CAVP standard. As part of CAVP, the cryptographic algorithms provided by the TOE’s cryptographic module went through CAVS testing which directly maps to these SFRs’ ATE Assurance Activities. Refer to the results of the CAVP certificates which are listed within the Security Target in Section 8.4. The vendor and evaluation team produced an equivalency argument for the CAVP certificates justifying that the TOE’s operational environment was equivalent to the operational environment used during the CAVS testing.

011	**[AC+PM]FCS_TLS_EXT.1**
Test Purpose:	The evaluator shall test this capability by establishing a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a HTTPS session. It is sufficient to observe (on the wire) the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Procedures: **This requirement was satisfied by the testing of FTP_TRP/ITC.**	
Test Results	PASS

3.3.5 User Data Protection

012	**[AC]FDP_ACF.1(1)**
Test Purpose:	The evaluator shall test this capability by using an authorized and compatible Policy Management product to define policies that contain rules for mediating the activities defined in Table 15. For each subject/object/operation/attribute combination, the evaluator shall execute at least one positive and one negative test in order to show that the TSF is capable of appropriately mediating these activities. For example, the policy may define a rule that allows one user to execute a certain process and another that forbids a different user from executing the same process. Once this policy is implemented, the evaluator will access a system as each of these users and observe that the ability to execute the specified process is appropriately allowed or denied. Additionally, for each conditional attribute that is supported (such as time of day restrictions), the evaluator will devise a positive and negative test that proves that the conditional attribute affects whether or not the requested operation is allowed. This activity is then repeated for each other subject/object/operation/attribute tuple. If the TOE enforces any additional access control policy rules, the evaluator shall devise positive and negative tests that cause these to be invoked and observe that appropriate behavior is performed.

Test Procedures:

Webgates User Forms

1. Using the OAM Web Console, create a Webgate application domain or use a pre-existing domain. (Webgate1).
2. Create or use a pre-existing resource within the domain and ensure that the operations only include "GET".
3. Assign the resource an Authentication Policy and an Authorization policy that allows "test2" access to the resource.
4. Navigate to the protected resource and verify the applied operation took place.
5. Modify the resource to allow the "post" operation.
6. Repeat step 4.
7. Collect the audit records for 'Creation or modification of policy', 'Any changes to the enforced policy or policies' and 'All requests to perform an operation on an object covered by the SFP'

Webgates URLs

1. Using the OAM Web Console, create a Webgate application domain or use a pre-existing domain. (Webgate1).
2. Create or use a pre-existing resource within the domain.
3. Assign the resource an Authentication Policy and an Authorization policy.

IP Range

a. Create the policy to deny access to any ip except 10.209.39.114.
b. Modify the policy to allow IPs from .110-113.

Temporal

a. Create the policy to only allow access to the resource for a specific amount of time. (Thursday 18:41-18:46)

Attribute

a. Create a policy that only allows users with the attribute of "Dept. Number 114" access to the resource.

Identity

a. Create a policy that only allows a specific user access to the resource. (test2)

4. Navigate to the protected resource and verify the applied operation took place.
5. Collect the audit records for 'Creation or modification of policy', 'Any changes to the enforced policy or policies' and 'All requests to perform an operation on an object covered by the SFP'

OES Security Modules

Open and Download protected file

1. Using the OES Console create a policy for the SM to allow a user access to open and download a file.
2. As "weblogic" enter the correct password and open and download the protected file.
3. As "weblogic", enter an invalid password.
4. Modify the policy to deny users the ability to download the file.
5. As "weblogic" enter the correct password attempt to download the protected file.
6. Collect the audit records for 'Creation or modification of policy', 'Any changes to the enforced policy or policies' and 'All requests to perform an operation on an object covered by the SFP'

Executable Script

1. Using the OES Console, create a policy for the SM to allow users to watch a video.
   NOTE: This policy has execute and enable operations.
2. As "weblogic" enter the correct password and enable the video.
3. As "weblogic", enter an invalid password.
4. Create a policy that allows all user the ability to execute the script except the user "John"
5. As "John" enter the correct password and attempt to execute the script.
6. As "weblogic" enter the correct password and execute the video
7. Modify the policy to disable the auto execute of the video.
8. As "weblogic" enter the correct password and enable the video.
9. Collect the audit records for 'Creation or modification of policy', 'Any changes to the enforced policy or policies' and 'All requests to perform an operation on an object covered by the SFP'

Synopsis

This is testing each of the Subject/Object/Operation scenarios from Table 6-3 in the Security Target.

- **Subject: User, Object: URLs, Operation: Access via HTTP operation - This was tested in test case 012 under "Webgate URLs".**
- **Subject: User, Object: Forms, Operation: HTTP GET - This was tested in test case 012 under "Webgate Forms".**
- **Subject: User, Object: Forms, Operation: HTTP POST - This was tested in test case 012 under "Webgate Forms".**
- **Subject: User, Object: Files, Operation: Open - This was tested in test case 012 under "Open and Download protected file".**
- **Subject: User, Object: Files, Operation: Download - This was tested in test case 012 under "Open and Download protected file".**
- **Subject: User, Object: Executable Script, Operation: Execute was tested in Test Case 012 under "Executable Script".**
- **Subject: User, Object: Executable Script, Operation: Enable was tested in Test Case 012 under**

"Executable Script".

- **Subject: User, Object: Executable Script, Operation: Disable was tested in Test Case 012 under "Executable Script".**

Also, FDP_ACF.1.2 describes additional rules that the TOE is able to define. These rules are listed below and a reference as to where each was tested.

Webgates are applied to web applications in the Operational Environment

- **This is tested by applying the Webgate to the HTTP Server in the operational environment. This was performed during the initial configuration of the TOE. All of the Webgate tests were conducted on the HTTP server.**

Within a Webgate, authorization policies are applied to Uniform Resource Identifiers (URIs) that are contained with a protected web application

- **For example, the FDP_ACF.1 test steps under "Webgates URLs" produced evidence that shows that the policy created (e.g. IP Range) is applied to the URI of the resource URL in the host identifier (i.e. Webgate1)**

Authorization policies can be enforced on identity, IP address, temporal, and attribute conditions

- **The test evidence produced for FDP_ACF.1 under "Webgates URLs" shows policies are enforced for identity, IP range, temporal access and attributes.**

Rules can be used to define one or more conditions that result in the requested access being allowed or denied using Boolean logic

- **Boolean logic is used any time there is more than one condition defined in the rule. An example of this logic can be seen in FTA_TSE.1 (Test Case 026) under OAM Console. In this instance the day of the week is one condition and the time is the other condition. By default, there is a "TRUE" condition in most rules that will allow access. The evaluation team attempted to gain access when both conditions were TRUE and access was achieved. The evaluation team attempted to gain access where one condition was False and access was not granted.**

Rules can result in additional authentication factors being requested

- **ESM_ATD.1 shows evidence that applying a different authentication level to a specific resource requires additional authentication challenge.**

Responses can be used to transmit data back to the operational environment so that the calling application can take additional action beyond redirecting a subject

- **This is defined as part of creating a policy where some data is provided to the protected application after an access decision is made. The protected application would then use the data to display information and/or perform other actions. This function is more about the protected application receiving and using the data then the TOE performing access control decisions based upon this information. The FCO_NRR.2 (Test Case 010) conducted a test with an application that displayed response data (User's ID).**

If an object is protected by an authorization policy, access to it is controlled on a deny-by-default basis

- **FMT_MSA.3 (Test 018) shows that resource is protected using controlled on a deny-by-default rule. When creating the policy, it is defaulted to deny all access, in which the administrator must permit access to the resource.**

Authorization policies are associated with Security Modules and define the subject-object-operation pairings that will result in access being allowed or denied.

- **FDP_ACF.1 test demonstrates allowed and denied access based upon the subject/object/operation under 'OES Security Modules'. OES is capable of protecting files from open and download. OES is**

also capable of protecting executable scripts from execute, enable and disable. The evidence shows that the policies deployed protect the resources to allow or deny users the ability to perform these operations.

Subjects are identified by username, group membership, or role

- **Subjects are clearly identified by username, group membership or role in each test case covered in the test plan.**

Objects are identified by resource name and type

- **Objects are clearly identified by the resource name and type in each test case covered in the test plan**

An authorization policy is configured either to grant access or deny access if the conditions of the access request apply to it

- **FDP_ACF.1 procedures under 'OES Security Modules' demonstrate that a policy can deny or allow the ability to perform the operation on the protected resource based on the conditions applied (i.e. identity)**

By default, an authorization policy evaluates all actions against a resource that is defined as protected, but specific actions may optionally be excluded from this

- **FDP_ACF.1 procedures under 'Open and Download protected file' demonstrate that the policy allows the specified user the ability to open the file but is denied the ability to download the file.**

Authorization policies may optionally contain multiple conditions that relate to one another using Boolean logic so that combinations of conditions can be used to make an access control decision

- **Boolean logic is used any time there is more than one condition defined in the rule. An example of this logic can be seen in FTA_TSE.1 (Test Case 026) under OAM Console. In this instance the day of the week is one condition and the time is the other condition. By default, there is a "TRUE" condition in most rules that will allow access. The evaluation team attempted to gain access when both conditions were TRUE and access was achieved. The evaluation team attempted to gain access where one condition was False and access was not granted.**

Responses can be used to transmit data back to the operational environment so that the calling application can take additional action beyond redirecting a subject

- **This is defined as part of creating a policy where some data is provided to the protected application after an access decision is made. The protected application would then use the data to display information and/or perform other actions. This function is more about the protected application receiving and using the data then the TOE performing access control decisions based upon this information. The FCO_NRR.2 (Test Case 010) conducted a test with an application that displayed response data (User's ID).**

If multiple authorization policies apply to the same action, a deny result takes precedence over any number of permit results.

- **FMT_MSA_EXT.5 (Test Case 019) demonstrates that if there are contradictory policies for the same action, the deny policy takes precedence.**

Test Results	PASS

3.3.6 Identification and Authentication

013	**[PM]FIA_USB.1**
Test Purpose:	The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.

Test Procedures:

The evaluators demonstrated that administrative privileges are bound to their web browsing session by logging in to the TOE and observing that the privileges that are assigned to the administrator are consistent with what is defined for their account by attempting to perform a collection of authorized and unauthorized administrative actions. The evaluators observed that the session remained persistent until the session was timed out or manually ended. The evaluators also logged in as one administrator account, logged in as a second account on a different system, used the second account to modify the administrative authorities of the first administrator, and observed that the updated permissions took effect as of the next page load performed by the first administrator.

The evaluators performed these test activities on both the OAM Console and OES Console interfaces.

OAM Console (USER)

1. Authenticate to the OAM Console as the "oamadmin" (System Administrator)
2. From the "Launch Pad" click on "Configuration" in the top right side of the page and then click "Administration"
3. Click "Grant" and in the pop-up window enter in the user name of the user that was created in the setup and click search.
4. Click the user that was produced in the search and give the user "System Administrator" role
5. Click "Add Selected"
6. Log out of the console.
7. Log in as the user that was just granted the System Administrator role.
8. Navigate to pages and/or perform tasks that only a user with System Administrator role can perform.
9. Keep the session open but on a different machine, log in to the OAM Console as the "oamadmin"
10. Repeat steps 2-6 except grant the user "Application Administrator" role.
11. Log out of the console and re-authenticate.
12. Perform functions that are allowed by the "Application Administrator" role.
13. Perform Clean up.
14. Collect the audit records from granting/revoking user roles (i.e. Modifications of the members of the management roles).

OAM Console (GROUP)

15. Authenticate to the OAM Console as the "oamadmin" (System Administrator)
16. From the "Launch Pad" click on "Configuration" in the top right side of the page and then click "Administration"
17. Click "Grant" and in the pop-up window enter in the group name of the group that was created that the

user was added to in the setup and click search.

18. Click the group that was produced in the search and give the group "System Administrator" role
19. Click "Add Selected"
20. Log out of the console.
21. Log in as the user that is in the group that was just granted the System Administrator role.
22. Navigate to pages and/or perform tasks that only a user with System Administrator role can perform.
23. Log out and login as a different user in the group.
24. Keep the session open but on a different machine, log in to the OAM Console as the "oamadmin"
25. Repeat steps 17-21 except grant the group "Application Administrator" role.
26. On the original session, navigate to a different page in the console. (the role of the user should change and should be restricted to "Application Administrator" role.
27. Log out of the console and re-authenticate.
28. Perform functions that are allowed by the "Application Administrator" role.
29. Perform Clean up.
30. Collect the audit records from granting/revoking group roles (i.e. Modifications of the members of the management roles).

OES Console (USER)

31. Authenticate to the OES Console as "weblogic" (system administrator).
32. From the "System Configuration" tab, ensure the "Default System Administrator" role is highlighted.
33. Click the "External User Mapping" tab then click "add".
34. In the pop-up window, click "Search". In the results, select the user that you want to give the role to and click "Add Selected" and then "Add Principals"
35. Log out of the console and log in as the user that was just given the system administrator role.
36. Perform a function that only a System Administrator can perform.
37. Repeat steps 31-36, except grant the user Domain Administrator role by right-clicking on the application and assigning a user the admin role for that application.
38. Create and Delete a policy within the domain.
39. Collect the audit records from assigning a user roles (i.e. Modifications of the members of the management roles), creation and deletion of a policy.
40. Login as "weblogic" on 1 machine and "oestest1" on another.
41. As "weblogic" revoke the admin rights from "oestest1".

Synopsis

The evaluators demonstrated that administrative privileges are bound to their web browsing session by logging in to the TOE and observing that the privileges that are assigned to the administrator are consistent with what is defined for their account by attempting to perform a collection of authorized and unauthorized administrative actions. The evaluators observed that the session remained persistent until the session was timed out or manually ended. The evaluators also logged in as one administrator account, logged in as a second account on a different system, used the second account to modify the administrative authorities of the first administrator, and observed that the updated permissions took effect as of the next page load performed by the first administrator.

OAM Console (USER) procedures show describe in steps 1- 6 the evaluator added the user "oamadmin" to the system administrator role. Steps 7 and 8 describe the steps showing the evaluator then authenticated to the OAM Console and navigated through the console that only the system administrator has the privilege to do. Steps 9 and 10 state the evaluator then authenticated to another instance of the TOE while the "oamadmin" user was still active and removed the system administrator role from the user and granted the application administrator role. The result of this shows that the role was removed and granted during the next authentication (Step 11-14).

These same steps were performed on the OAM Console using the group from the LDAP store (Steps 15-30)

and also as a user on the OES Console (Steps 31-41). **The test evidence shows that any user with the "System Administrator" role has access to perform each management function on the TOE. A user with the limited administrator role such as the "Application Administrator" only has access and is only able to perform functions within the application domain that is assigned to that role. This user will not be able to view any tab or perform any function that is not within their scope. For instance, FIA_USB1_User.png shows a screenshot of the user with system administrator role. The user in this shot is able to access each tab on the interface. FIA_USB1_UserApplicationAdmin.png is a screenshot of a user with only the tabs and ability to perform functions within the application assigned. It displays only a fraction of what the system administrator is able to view/perform.**	
Test Results	PASS

3.3.7 Security Management

014	**[PM]FMT_MOF.1**
Test Purpose:	The evaluator shall test this function by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance. If the TSF can be configured by an authorized and compatible Secure Configuration Management product, the evaluator shall also configure such a product to manage the TSF and use this product to perform the defined management activities. In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator shall test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable.

Test Procedures:

OAM Console (Webgate)

1. Authenticate to the OAM Console as “oamadmin” (system administrator).
2. From the “Launch Pad” click on “Configuration” in the top right side of the page and then click “Administration”
3. Click “Grant” and in the pop-up window enter in the user name of the user that was created in the setup and click search.
4. Click the user that was produced in the search and give the user “System Administrator” role
5. Click “Add Selected”
6. Log out of the console.
7. Log in as the user that was just granted the System Administrator role.
8. Perform a subset of management functions from table 6-4 in the ST that only a user with System Administrator role can perform.
9. Log out of the console and re-authenticate as the “oamadmin” user.
10. Repeat steps 2-5 except grant the user “Application Administrator” role.
11. From the “Launch Pad” click on “Application Domain” and select an application domain you wish to add the user as the administrator for.
12. Click the “Administration” tab and click “grant”
13. In the search pop-up window click the “Search” button.
14. Select the username of the user that you gave the “Application Domain” role to.
15. Log out of the console and re-authenticate as the user with application domain role.
16. Perform a subset of actions from table 6-4 of the ST within the domain that the user is assigned to.
17. Attempt to perform management activities in a different domain.
18. Attempt to perform an action that only a system administrator is capable of.
19. Collect the audit records from assigning a user roles.

OES Console (Security Module)

20. Authenticate to the OES Console as “weblogic” (system administrator).
21. From the “System Configuration” tab, ensure the “Default System Administrator” role is highlighted.
22. Click the “External User Mapping” tab then click “add”.
23. In the pop-up window, click “Search”. In the results, select the user that you want to give the role to and click “Add Selected” and then “Add Principals”
24. Log out of the console and log in as the user that was just given the system administrator role.
25. Perform a subset of management functions from table 6-4 in the ST that only a user with System Administrator role can perform.
26. Remove the “System Administrator” role from the user.
27. Add the user as an Application Administrator and attach it to an application domain that was created.
28. Perform a subset of functions from table 6-4 within the application domain that is assigned.

29. Attempt to perform functions on another domain.
30. Attempt to perform functions only allowed by the system administrator.
31. Collect the audit records from assigning a user roles.

NOTE: If a user does not have privileges, the menu to perform functions related to those privileges are unable to be viewed. Thus, the test proves the user is unable to perform tasks they do not have the ability to perform by demonstrating the function is not present.

Synopsis

The test procedures and the evidence demonstrate that a user was granted the "System Administrator" role and was able to perform management activities that only users with that role were able to perform. Additionally, the evidence demonstrates a user was granted the "Application/Domain Administrator" role. The user with this role was only able to perform management activities within the Application/Domain assigned. The endpoints are within the Application/Domain and are able to be configured by the assigned users.

The test evidence demonstrates that any user with the "System Administrator" role has access to perform each management function on the TOE. A user with the limited administrator role such as the "Application Administrator" only has access and is only able to perform functions within the application domain that is assigned to that role. This user will not be able to view any tab or perform any function that is not within their scope.

This test purpose is also covered by the testing of FIA_USB.1 (Test Case 013).

Test Results	PASS

<table>
<tr><th>015</th><th>[AC]FMT_MOF.1(1) and [PM]FMT_MOF_EXT.1</th></tr>
<tr><td><b>Test Purpose:</b></td><td>The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification.

The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities:
- Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior
- Repository for trusted audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository
- Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP.
- Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP.
- Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied.

Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE.

The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.</td></tr>
<tr><td colspan="2"><b>Test Procedures:</b>

This assurance activity is satisfied by the testing the following SFRs: FAU_SEL.1, FDP_ACF.1, FIA_USB.1, and FMT_MOF.1(2).

<b>Synopsis</b>

<b>The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification."</b></td></tr>
</table>

- **This wording is covered under the management functions performed during FDP_ACF.1 (Test Case 012). For example, evidence of a policy being created, applied to an endpoint, and verification of the behavior can be seen in the audit records for each OAM and OES.**

"The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities:
- Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior."

- **This wording is covered under the management functions performed FAU_SEL.1 (Test Case 007). For example, the audit shows the records for the configuration of the auditing level.**

"Repository for trusted audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository."

- **Modifying the trusted audit repository is not applicable to the TSF because the TOE automatically writes audit data to the RDBMS (for OAM/OES Server components) and the local file system of the underlying platform (for Webgate/Security Module components); this is not configurable and determined to be acceptable for meeting the requirements.**

"Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP."

- **This wording is covered under the management functions performed during FDP_ACF.1 (Test Case 012). Steps 1-5 under the "Webgate URLs" subtitle contain the procedure produced the results that are consistent with this portion of the AA. The results of this test verify these management actions were taken.**

"Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the SFP."

- **This wording is covered under the management functions performed during FDP_ACF.1 (Test Case 012). Steps 1-5 under the "Webgate URLs" subtitle contain the procedure produced the results that are consistent with this portion of the AA. The results of this test verify these management actions were taken.**

"Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied."

- **This is not applicable to the TSF because a Webgate or Security Module will always enforce the last policy it received from the origin point; an active connection is not required for the policy to be enforced as intended and this is not configurable.**

"Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such

that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.” • **This test was satisfied with the testing of FMT_MOF.1(2) (test case 016). The evidence shows that by configuring the Policy Management product such that is not authorized to configure the AC endpoint is either not shown (OES) or is disallowed (OAM).** **Note: The following function and associated audit record are not possible for this TOE as it requires connection to the database (remote audit storage) to operate. Function: “- Repository for trusted audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository.” Audit Record: “Establishment and disestablishment of communications with audit server”**	
Test Results	PASS

016	**[AC]FMT_MOF_EXT.1(2)**
Test Purpose:	The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to query the policy being implemented by the TOE. Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.
Test Procedures: **OAM Console** 1. Create a Webgate with credentials or use a Webgate that is already created (webgate1). 2. Change the password of the Webgate that was created during the configuration. 3. Modify a policy to the disconnected Webgate. **OES Console** 1. Configure the security module in a controlled push mode that requires the enrollment of the security module to the OES console. 2. Create a policy and distribute it to the SM configured in step 1. 3. From another instance of OES, attempt to modify the policy that was just created or consumed by the SM. **NOTE: The other instance of OES will be unable to manage the SM due to the SM is only enrolled into the current console. There will be no option for the administrator of the 2nd console to be able to manage the SM.**	
Test Results	PASS

017	**[AC]FMT_MSA.1**
Test Purpose:	The evaluator shall test this capability by using the associated Policy Management product to confirm that each identified operation against the indicated attributes may be performed, and that the TOE interfaces do not provide the ability for any other roles to perform operations against the indicated attributes.

Test Procedures:

OAM Console

1. Authenticate to the OAM console as the system administrator.
2. Create 2 application domains or use domains that are already created. (TestDomain and IAM Suite)
3. Assign different domain administrators for each of the domains that were created.
    a. Click on the Application Domain that you want to assign the user to.
    b. Click “Administration” and then “Grant”
    c. Search for the users and select the user then click “Add Selected”.

    test1 – TestDomain
    test2 – IAMSuite Domain
4. Logout of the Console and re-authenticate as the domain administrator for “IAM Suite”.(test2)
5. Perform an action change_default, query, modify, delete, [**create**]] within “IAM Suite”.
6. Attempt to perform any of the above actions “TestDomain”
7. Logout of the Console and re-authenticate to the console as the domain administrator for “TestDomain” (test1)
8. Perform an action to configure “TestDomain”
9. Attempt to perform and action that will configure “IAMSuite Domain”
10. Collect audit records for modification of security attributes (i.e. Modifications of the members of the management roles).

OES Console

1. Authenticate to the OES console as the system administrator (weblogic).
2. Create 2 application domains or use domains that are already created. (Library and Test)
3. Assign different domain administrators for each of the domains that were created.
    test1 – Test
    oestest1 – Library
4. Logout of the Console and re-authenticate as the domain administrator for “Test” domain.(test1)
5. Perform an action within “IAM Suite”.
6. Attempt to perform any of the above actions “TestDomain”
7. Logout of the Console and re-authenticate to the console as the domain administrator for “TestDomain” (test1)
8. Perform an action to configure “TestDomain”
9. Attempt to perform and action that will configure “IAMSuite Domain”
10. Collect audit records for modification of security attributes (i.e. Modifications of the members of the management roles).

Synopsis

Steps 1-3 describe how the evaluator created two different domains on the OAM Console and assigned administrators to each. Steps 5-8 describe how the evaluator used the assigned roles and performed the actions specified in the SFR on each domain that was created and assigned to the user. Step 9 shows that the user was not able to modify or perform any of the actions to a domain that was not assigned.

The test evidence shows that the user that is assigned to the specific domain is only able to see or perform the actions in their respective domain.

<table>
<tr><td colspan="2"><b>The audit records that were collected during this test show the audit for creation, deletion, and modification. Change_default would also be the same as create, since the default is deny all and creating a policy to allow access would change this. The only action that is not audited is query.</b></td></tr>
<tr><td><b>Test Results</b></td><td>PASS</td></tr>
</table>

<table>
<tr><th>018</th><th colspan="2">[AC]FMT_MSA.3</th></tr>
<tr><td colspan="2"><b>Test Purpose:</b></td><td>The evaluator shall test this capability by using the associated Policy Management product to confirm that for each identified security attribute and restrictive initial state, the TOE implements the correct restrictive value and that it can be overridden in the manner specified by the operational guidance</td></tr>
<tr><td colspan="3"><b>Test Procedures:</b>

<b>OAM Console</b>
1. In the OAM Console as the system administrator, ensure the application domain’s default authorization policy to deny all access to the resource is applied.
2. Attempt to access the resource using any user.
3. In the “Conditions” tab of the same authorization policy, add a condition to allow a specific user to access the resource by identity.
4. Add the condition to the “Selected Conditions” section of the “Allow Rule”.
5. Access the protected resource that everyone was just given access.
6. Collect audit records for the modification of the application domain.

<b>OES Console</b>
1. In the OES Console, ensure the default policy that denies all users access to the resource is applied to a resource.
2. Attempt to access the resource.
3. Modify the policy to allow user John full access to all operations.
4. Collect audit records for the modification of the policy from deny all users.

<b>Synopsis</b>

<b>During the initial configuration of the TOE the administrator must apply a policy to a resource for the resource to be protected. The default policy that can be applied is a “deny-by-default” policy. The administrator may then modify this policy or create another policy to allow more permissive access to the resource. This test case shows that these default policies apply the deny-by-default rule and that the restrictive value can be overridden (granting access).</b></td></tr>
<tr><td colspan="2"><b>Test Results</b></td><td>PASS</td></tr>
</table>

019	[AC]FMT_MSA.5
Test Purpose:	The evaluator shall test this capability by defining policies that contain the contradictions indicated in the operational guidance and observing if the TSF responds by detecting the contradictions and reacting in the manner prescribed in the ST. If the TSF behaves in a manner that prevents contradictions from occurring, the evaluator shall review the operational guidance in order to determine if the mechanism for preventing contradictions is described and if this feature is communicated to administrators. This feature shall be tested in conjunction with a compatible Access Control product; in other words, if the TOE has a mechanism that prevents contradictions (for example, if a deny rule always supersedes an allow rule), then correct enforcement of such a policy by a compatible Access Control product is both a sufficient and a necessary condition for demonstrating the effectiveness of this mechanism.

Test Procedures:

OAM Console
Group is denied but user within the group is permitted
(This test shows that the more specific rule will take precedence)

1. In the OAM Console as the system administrator, create or modify an application domain to deny a group access to a resource.
2. As a user that is in the group, attempt to access the resource.
3. As the system administrator modify the application domain to allow the specific user access to the resource.
4. As the user, access the resource.
5. As a different user in the group, attempt to access the resource.

A user is a part of 2 different groups

1. Create 2 groups and add the same user to each group.
2. In the OAM Console as the system administrator, create or modify an application domain to deny groupA permission to a resource and allow groupB permission to a resource.
3. Attempt to access the resource from step 2.

Explicit Contradictory Rules

1. In an authorization policy that exists in an application domain, add an entry that allows a user to access the resource and denies the same user access the resource.

OES Console

1. Create a new policy using the OES Console with contradictory rules. (allows and denies a user to borrow a book.).
    - Policy019Permit
    - Policy019Deny
2. In the OES console, use the policy simulator to test whether to policy will be enforced correctly.
3. Attempt to borrow the book using the App.

Test Results	PASS

020	[AC+PM]FMT_SMF.1
Test Purpose:	(for AC) The evaluator shall test this capability by configuring the TOE in a manner that is consistent with the evaluated configuration. For each management function that has been defined in the ST, the evaluator shall perform the function in a manner that is consistent with the operational guidance and verify that the observed behavior is consistent with the expectations of what the function should accomplish. (for PM) The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities.

Test Procedures:
This assurance activity is satisfied by the testing of the other SFR's. Test evidence and audit records are saved according to the SFR. While performing each test, collect and verify the audit records contain all 'use of the management functions' and describe the management function performed.

Synopsis

The following is a list of management functions that are contained in Table 6-4 in the ST and a mapping of the test case where each was performed:

Creation of policies – ESM_ACD.1 (Test Case 001), FDP_ACF.1 (Test Case 012)
Transmission of policies – ESM_ACT.1 (Test Case 002)
Association of attributes with objects – ESM_ATD.1 (Test Case 003)
Association of attributes with subjects - ESM_ATD.2 (Test Case 003)
Configuration of auditable events – FAU_SEL.1 (Test Case 007)
Configuration of auditable events for defined external entities– FAU_SEL.1 (Test Case 007)
Configuration of external audit storage location – FAU_STG_EXT.1 (Test Case 009)
Definition of subject security attributes, modification of subject security attributes – FIA_USB.1 (Test Case 013)
Configuration of the behavior of other ESM products - ESM_ACD.1 (Test Case 001), FDP_ACF.1 (Test Case 012)
Management of sets of subjects that can interact with security attributes – FIA_USB.1 (Test Case 013)
Management of rules by which security attributes inherit specified values – FIA_USB.1 (Test Case 013)
Management of the users that belong to a particular role – FIA_USB.1 (Test Case 013)

Test Results	PASS

021	[AC+PM]FMT_SMR.1

Test Purpose:	(for AC) The evaluator shall use the associated Policy Management product to connect to the TOE and confirm that it is operating in the assigned role. The evaluation shall also confirm that a user or other external entity that has not been authorized for the indicated role cannot assume the indicated role. (for PM) The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities
Test Procedures: This assurance activity was satisfied by the testing of FIA_USB.1 and FMT_MSA.1.	
Test Results	PASS

3.3.8 Protection of the TSF

022	**[AC+PM]FPT_APW_EXT.1**
Test Purpose:	The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.
Test Procedures: The evaluators observed that in the evaluated configuration, all user and administrator identity data is stored in one or more identity stores in the Operational Environment and the TSF does not maintain any identity and credential data. The evaluators observed that the OAM and OES Console interfaces did not provide a method to read credential data in cleartext.	
Test Results	PASS

023	**[AC]FPT_FLS_EXT.1**
Test Purpose:	The evaluator shall test this capability by deliberately inducing the failure states described in the SFR and observing whether or not the TSF reacts in a manner that is consistent with the Security Target’s description of its expected behavior.
Test Procedures: **OAM (Webgate)** 1. Create a policy in the OAM Console (May use a policy that is already created) and ensure the policy is effective. 2. Disconnect the Database (shutdown) from the Servers. a. Go to DB home and type command “./sqlplus / as SYSDBA” b. Once authenticated type “shutdown immediate” 3. Attempt to access the resource that is in the policy from step 1. 4. Collect the audit records for the failure of communication between the Webgate and the OAM Server. Ensure that the connection is to the remainder of the TOE and includes the reason for failure. **OES (Security Module)** 1. Create a policy in the OES Console (May use a policy that is already created) and ensure the policy is effective. 2. Disconnect the Database (shutdown) from the Servers.	

   a. Go to DB home and type command "./sqlplus / as SYSDBA"
   b. Once authenticated type "shutdown immediate"
3. Attempt to access the resource that is in the policy from step 4
4. Collect the audit records for the failure of communication between the Security Module and the OAM Server. Ensure that the connection is to the remainder of the TOE and includes the reason for failure.

Synopisis

This test describes the evaluator putting the TOE in a failure state by shutting down the database (RDBMS) that it is assigned to. The TOE will not operate if the database is not running which causes the failure state. This also demonstrates that the TOE has been configured to communicate with this specific database to perform its functions. The evaluator then, in steps 3 and 7, attempted to access a resource that was protected by the TOE through a policy before the failure state occurred and verified that the resource is still protected by either denying access or requiring the evaluator to authenticate in order to access the resource.

Test Results	PASS

024	**[AC]FPT_RPL.1**
Test Purpose:	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. The evaluator can then take these packets and re-transmit them to the TOE. Once this has been done, the evaluator shall execute an appropriate subset of User Data Protection testing with the expectation that the policy enforced will be the first policy transmitted. If the expected results are met, the TOE is sufficiently resilient to rudimentary policy forgery.

Test Procedures:

OES Server to Security Module

1. Start the Wireshark that is installed on the underlying server. Ensure that it is filtering for the IP of the Security Module.
2. Authenticate to the OES Server using valid credentials. Create or modify a policy and distribute it to the security module.
3. Stop the packet sniffer and locate the packets that were sent and ensure that they are encrypted using TLS.
4. Collect the audit records that were generated with the initiation of the channel from the OES server to the security module.

OAM Server to Webgate (if located on remote server)

1. Start the Wireshark that is installed on the underlying server. Ensure that it is filtering for the IP of the Webgate.
2. Access a protected resource that requires authentication. (In the environment, the Webgate uses OAM Server to talk to the ID store to authenticate the users.
3. Stop the packet sniffer and locate the packets that were sent and ensure that they are encrypted using TLS.
4. Collect the audit records that were generated with the initiation of the channel from the OAM server to the Webgate.

Synopsis

While installing and configuring the TOE per the instructions in Oracle Access Manager Suite 11g Release 2 Supplemental Administrative Guidance for Common Criteria version 1.0 the TOE is configured to use TLS between its separate components. The evaluation team then followed the test purpose by installing wireshark, sending a valid policy and observing the packets that comprise the policy. While observing these packets, it was determined that these packets were encrypted using TLS. The use of TLS was also

confirmed under the testing for FTP_ITC.1 (Test Case 027) which contain the actual results for this test case. Thus, verifying that the TOE is secure against rudimentary policy forgery attacks via replay. **The remaining test steps described in the test purpose were not performed since the use of TLS prevents any modification of the traffic that would be accepted by the receiving TOE component. Additionally, since the policy data is encrypted, it would be impossible to modify the policy in a meaningful manner. A TRRT was submitted to NIAP and approved that the functionality of the TOE met the intent of this test.**	
Test Results	Pass

3.3.9 Resource Utilization

025	**[AC]FRU_FLT.1**
Test Purpose:	The evaluator shall test this capability by severing the network connection between the TOE and the Policy Management product, defining an updated policy, and reestablishing the connection will determine if the TOE appropriately receives the new policy data within the time interval specified in FCO_NRR.2.3. The evaluator shall devise a scenario such that the old policy allows a specific action and that the new policy denies that same action. The evaluator shall then perform that action, observe that it is allowed, sever connection with the Policy Management product, define the new policy during that outage, re-establish the connection, wait for the interval defined by FCO_NRR.2.3, perform the same action again, and observe that it is no longer allowed.
Test Procedures: **OAM (Webgate)** 1. Create a policy in the OAM Console that forces a user to authenticate in order to access a URL (May use a policy that was already created) and ensure that the policy is enforced. 2. Disable the Webgate in the GUI. 3. Modify the policy that denies a user any access to the same URL from step 1. 4. Reconnect the endpoint and 5. Ensure that the deny policy in step 3 takes effect within a few minutes by attempting to access the URL. **OES (Security Module Controlled-push)** 6. Create a policy in the OES Console that permits user “John” to be able to open and download files in a directory. (May use a policy that was already created) 7. As user “John” download a file in the protected directory. 8. Disconnect by detaching the SM from the application “Library”. 9. Modify the policy that denies the user John from downloading a file in the protected directory. 10. Reconnect the endpoint by attaching the SM to the application “Library. 11. As user John, attempt to download a file in the protected directory.	
Test Results	PASS

3.3.10 TOE Access

026	**[AC]FTA_TSE.1**
Test Purpose:	(for AC) The evaluator shall test this capability by performing positive and negative testing for each attribute that can be used to conditionally allow session establishment. For example, if a time of day restriction applies, the evaluator shall successfully log on during an acceptable time and shall be prevented from logging on during an unacceptable time. The evaluator then follows the operational guidance to configure the TOE so that that access is denied based on a specific value of the attribute. The evaluator shall then attempt to establish a session in contravention to the attribute setting (for instance, the location is denied based upon the time of day). The evaluator shall observe that the session establishment attempt fails.
Test Procedures: **OAM Console** 1. Modify a policy that is already created to restrict a URL from being accessed by time of day. a. In the OAM Console, select “Application Domain”	

   b. Click on an application domain that is already created. (Created in a previous test).
   c. Click the “Authorization Policies” tab and then click on “Protected Resource Policy”
   d. Click on the “Conditions” tab and then “Add”
   e. Create a name for the condition and in the “Type” drop down menu select “Temporal” and then click “Add Selected”.
   f. In the Pop up window select the “Start time” and the “End time” as well as one day of the week you want and click ok. (This tests the day selection)
   g. Click on the “Rules” tab and add the conditions that was just created to the “Selected Conditions”. (Be sure to remove any other conditions that may be presented.

2. Access the URL during the allowed time and day that you selected.
3. Attempt to access the URL during a time that is not allowed.
4. Modify the condition by selecting every day of the week and only 1 hour. (This tests the time selection)
5. Repeat steps 2 and 3.
6. Collect audit records for the denial of the session establishment.

NOTE: The OAM portion of this test case was satisfied during the testing of FDP_ACF.1 (Test Case 012). The test steps and the results show that the user was denied/allowed access to the resource depending on the time of day.

OES Console

1. Create a policy using the steps from a previous test and create the authorization policy as follows:
   a. Select the “Allow” radio button.
   b. Click the green + in the Principal section. In the pop-up screen click the “users” tab and then search.
   c. Select the user that you want to use for the test (test2) and click “add selected” then click “add principal”.
   d. Click the green + in the “Target” section. In the pop-up screen click the resource tab and then “search”
   e. Select the target that you want to use and click “add selected” then “add target”.
   f. Click “edit” under the “Condition” tab.
   g. Select “current_datetime” from the menu and click “add”
   h. Enter the time that you want the target to be denied access and click “done”
   i. Click “Save” and continue the steps to finish and distribute the policy.
2. Attempt to access the resource as the user from step c at the time specified in step g.
3. Collect audit records for the denial of the session establishment.

Test Results	PASS

3.3.11 Trusted Path/Channels

027	**[AC+PM]FTP_ITC.1**
Test Purpose:	The evaluator shall also perform the following tests: - Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful. - Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE. - Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext. - Test 4: The evaluator shall ensure, for each communication channel with an authorized IT entity, modification of the channel data is detected by the TOE.

Test Procedures:

OAM Server to Identity Store

1. Start the Wireshark that is installed on the identity store server. Ensure that it is filtering for the IP of the OAM server.
2. Authenticate to the OAM Server using valid credentials.
3. Stop the packet sniffer and locate the packets that were sent and ensure that they are encrypted using the ciphersuites claimed.
4. Collect the audit records that were generated with the initiation of the channel from the OAM server to the Identity store.

OES Server to Identity Store

1. Start the Wireshark that is installed on the identity store server. Ensure that it is filtering for the IP of the OES Server.
2. Authenticate to the OES Server using valid credentials.
3. Stop the packet sniffer and locate the packets that were sent and ensure that they are encrypted using the ciphersuites claimed.
4. Collect the audit records that were generated with the initiation of the channel from the OES Server to the Identity store.

OAM Server to RDBMS

1. Start the Wireshark that is installed on the RDBMS server. Ensure that it is filtering for the IP of the OAM server.
2. Authenticate to the OAM Server using valid credentials.
3. Stop the packet sniffer and locate the packets that were sent and ensure that they are encrypted using the ciphersuites claimed.
4. Collect the audit records that were generated with the initiation of the channel from the OAM server to the RDBMS.

OES Server to RDBMS

1. Start the Wireshark that is installed on the RDBMS server. Ensure that it is filtering for the IP of the OES server.
2. Authenticate to the OES Server using valid credentials.
3. Stop the packet sniffer and locate the packets that were sent and ensure that they are encrypted using the ciphersuites claimed.
4. Collect the audit records that were generated with the initiation of the channel from the OES server to the RDBMS.

OES Server to Security Module

1. Start the Wireshark that is installed on the underlying server. Ensure that it is filtering for the IP of the Security Module.
2. Authenticate to the OES Server using valid credentials. Create or modify a policy and distribute it to the security module.
3. Stop the packet sniffer and locate the packets that were sent and ensure that they are encrypted using the ciphersuites claimed.
4. Collect the audit records that were generated with the initiation of the channel from the OES server to the security module.

OAM Server to Webgate (if located on remote server)

1. Start the Wireshark that is installed on the underlying server. Ensure that it is filtering for the IP of the Webgate.
2. Access a protected resource that requires authentication. (In the environment, the Webgate uses OAM Server to talk to the ID store to authenticate the users.
3. Stop the packet sniffer and locate the packets that were sent and ensure that they are encrypted using the

ciphersuites claimed.

4. Collect the audit records that were generated with the initiation of the channel from the OAM server to the Webgate.

Note: A TRRT was submitted to NIAP regarding Test 4 stating that it should be removed for the same reasons as a Technical Decision for another Protection Profile that also removed this test from FTP_ITC.1 and FTP_TRP.1. NIAP agreed that Test 4 should be removed from all ESM Protection Profiles.

028	**[PM]FTP_TRP.1**
Test Purpose:	The evaluator shall repeat the assurance activity for FTP_ITC.1 for each interface and cryptographic protocol that is provided by the TOE for remote administration.

Test Procedures:

OAM Console

1. In the Mozilla browser type “about:config” as the URL.
2. Disable all of the ciphersuites with the exception of the TLS_AES128_CBC_SHA ciphersuite.
3. Exit out of the browser.
4. Start the packet sniffer.
5. Authenticate to the OAM Console using valid credentials using Mozilla Firefox browser.
6. Stop packet sniffer and ensure the connection was encrypted using the TLS_AES128_CBC_SHA.
7. Repeat step 1 and 2 except disable the TLS_AES128_CBC_SHA ciphersuite and enable TLS_AES256_CBC_SHA ciphersuite.
8. Repeat step 4 and 5.
9. Stop packet sniffer and ensure the connection was encrypted using the TLS_AES256_CBC_SHA.
10. In the Firefox browser disable the TLS_AES256_CBC_SHA ciphersuite and enable any other ciphersuite of your choosing.
11. Repeat steps 4 and 5.

OES Console

1. In the Mozilla browser type “about:config” as the URL.
2. Disable all of the ciphersuites with the exception of the TLS_AES128_CBC_SHA ciphersuite.
3. Exit out of the browser.
4. Start the packet sniffer.
5. Authenticate to the OES Console using valid credentials using Mozilla Firefox browser.
6. Stop packet sniffer and ensure the connection was encrypted using the TLS_AES128_CBC_SHA.
7. Repeat step 1 and 2 except disable the TLS_AES128_CBC_SHA ciphersuite and enable TLS_AES256_CBC_SHA ciphersuite.
8. Repeat step 4 and 5.
9. Stop packet sniffer and ensure the connection was encrypted using the TLS_AES256_CBC_SHA.
10. In the Firefox browser disable the TLS_AES256_CBC_SHA ciphersuite and enable any other ciphersuite of your choosing.
11. Repeat steps 4 and 5.

Collect audit records for all attempted uses of the trusted path.

Test Results	PASS

3.4 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 using the following keywords individually and as part of various permutations and combinations: Oracle Access Manager, Oracle Entitlements Server, WebGate, and Oracle Security Module. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov. The search resulted in two relevant findings that were patched prior to this evaluation's completion.

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
  The TOE's implementation of trusted communications protocols should be correct and should not use weak ciphers or expose sensitive data in a way that would allow an attacker to break the security of the channel and gain access to TSF data in transit.
- Web Interface Vulnerability Identification
  The TOE's web application should be free of any web vulnerabilities that are exploitable. A combination of manual and automatic web penetration testing, including cross-site scripting, SQL injection, directory traversal, and information disclosure attacks were tested.

The TOE successfully prevented any attempts of subverting its security.

Verdict: The evaluation team has completed testing of this component, resulting in a verdict of PASS.

3.5 Security Assurance Requirements

The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation team determined the TOE to be Part 2 extended, and meets the SARs contained the PPs. The evaluation team assessed the TOE and the developer's evidence against the following Security Assurance Requirements during this evaluation:

- ASE_TSS.1
- ASE_REQ.1
- ASE_ECD.1
- ASE_OBJ.1
- ASE_CCL.1
- ASE_INT.1
- ADV_FSP.1
- AGD_OPE.1
- AGD_PRE.1
- ALC_CMC.1
- ALC_CMS.1
- ATE_IND.1
- AVA_VAN.1

A verdict for a Security Assurance Requirement is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The reader of this document can assume that all evaluation activities and work units received a passing verdict. The results of the Security Assurance Requirements are presented in detail in the proprietary ETR.

4 Conclusions

The TOE was evaluated against the ST and has been found by this evaluation team to be conformant with the ST. The overall verdict for this evaluation is: Pass.

5 Glossary of Terms

Acronym	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

Table 6-1: Acronyms

Term	Definition
Administrator	A general term for any individual with permissions to manage some aspect of the TSF.

Term	Definition
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.

Table 6-2: Terminology