Assurance Activities Report
For a Target of Evaluation

Oracle Identity Manager

Version 11g Release 2

Security Target (Version 1.0)

Assurance Activities Report (AAR)
Version 1.0

08/28/2015

Evaluated by:

Booz | Allen | Hamilton

Booz Allen Hamilton Common Criteria Test Laboratory
NIAP Lab # 200423
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090

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
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090

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

Evaluation Personnel:
Christopher Gugel – CC Technical Director
Christopher Rakaczky
Dave Cornwell

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

1 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.

2 TOE Summary Specification Assurance Activities

The evaluation team completed the testing of the Security Target (ST) 'Oracle Identity 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 Identity and Credential Management, version 2.1' [ICMPP]. 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 ICMPP 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 (ICMPP) that defines where the most up-to-date TSS Assurance Activity was defined.

ESM_EAU.2.1

The Assurance Activity states that the TSS must describe the TSF as requiring authentication in order to use it and also describes the authentication mechanism that is used for each type of user and/or IT entity that authenticates to it.

The TSS states that "In order to manage the TOE, administrators must provide valid authentication credentials. The TOE uses the identity store in the Operational Environment to define its administrators, so they can authenticate to the TOE by using the same username/password that they use to access other organizational resources. Administrators provide a username and password to the TOE through an administrative interface. The TSF then initiates an authentication request to the environmental identity (Active Directory, OID, or OUD) store using LDAP."

ESM_EAU.2.2

Same as ESM_EAU.2.1

ESM_EID.2.1

This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.

ESM_EID.2.2

Same as ESM_EID.2.1

ESM_ICD.1.1

The Assurance Activity requires the TSS to identify compatible ESM products and describe the identity and credential data that is used by those products.

The TSS states "Any product or application that can make authentication and authorization decisions based on the contents of the organizational user store is compatible with the TSF. Specifically, the TSF manages the following types of external data that might typically be used by an organization to govern access to its resources:

- Basic identity attributes: information that can be used to uniquely identify an individual user such as first name, last name, user ID, and email address.
- Extended identity attributes: information that is defined by the organization that can be used to define properties of an individual such as department, title, and geographic region.
- Credential data: hashes of user passwords.

The TOE also introduces its own identity and credential data that is used by the TSF to govern changes to the environmentally-stored data and to define user permissions on environmental objects via connectors. This data includes:

- Enterprise permissions: users can be assigned to roles based on some combination of basic and extended identity attributes. These roles can then be associated with account and entitlement configuration settings for entities in the Operational Environment such that users are given identity-based permissions to interact with enterprise resources.
- User status: determines whether the user is allowed to authenticate to organizational resources. User status values include active, locked, disabled, deleted, and disabled until a specific date/time.
- Credential status: determines whether the user password is active or expired.
- Credential data: determines if, when, and how a user can change their password. Includes credential expiration date, password history (stored as hashed data), a flag to prompt the user to change their password on next login, and security questions and answers."

ESM_ICD.1.2

Same as ESM_ICD.1.1

ESM_ICD.1.3

Same as ESM_ICD.1.1

ESM_ICD.1.4

Same as ESM_ICD.1.1

ESM_ICD.1.5

Same as ESM_ICD.1.1

ESM_ICD.1.6

Same as ESM_ICD.1.1

ESM_ICD.1.7

Same as ESM_ICD.1.1

ESM_ICD.1.8

Same as ESM_ICD.1.1

ESM_ICT.1.1

This Assurance Activity requires the TSS to ensure the assignments within the SFR to be completed in a manner that is consistent with the application notes taken from the PP. It also requires the TSS to describe the ESM data that the TSF transmits and the circumstances that cause it to be transmitted.

The TSS states "When new identity and credential data elements are created on the TOE or updates to identity and credential data are made on the TOE, the TSF immediately propagates the information maintained in the Identity Store to that repository. Additionally, for user attributes that have been defined by the TSF, LDAP synchronization can be enabled to periodically synchronize the TSF data with the Identity Store."

FAU_GEN.1.1

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

The TSS discusses the different auditable events and also specifies the data that each logged event should contain. Within the TSS is references table 6-2 of the ST that lists all of the events.

FAU_GEN.1.2

Same as FAU_GEN.1.1

FAU_STG_EXT.1.1

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.

The TSS describes the location of the stored audit data to be in the local file system as well as the environmental RDBMS. It also discusses the security of the transmission of audit data to be secured using JDBC with TLS encryption.

FAU_STG_EXT.1.2

Same as FAU_STG_EXT.1.1

FAU_STG_EXT.1.3

Same as FAU_STG_EXT.1.1

FCS_CKM.1.1

This SFR does not contain any TSS Assurance Activities.

FCS_CKM_EXT.4.1

The Assurance Activity requires the TSS to describe all of the secret key, private keys, and CSPs; when they are zeroed; and the type of procedure that is performed to do this.

Section 8.3.2 of the TSS describes all of the keys used as well as how they are zeroized. All cryptographic data is stored in volatile memory so are zeroized in the same manner.

FCS_COP.1.1(1)

This SFR does not contain any TSS Assurance Activities.

FCS_COP.1.1(2)

This SFR does not contain any TSS Assurance Activities.

FCS_COP.1.1(3)

This SFR does not contain any TSS Assurance Activities.

FCS_COP.1.1(4)

This SFR does not contain any TSS Assurance Activities.

FCS_HTTPS_EXT.1.1

This Assurance Activity requires the TSS to clearly discuss how HTTPS uses TLS to establish an administrative session. Also to verify how the cryptographic functions are being used to perform encryption functions.

The TSS states "The TOE uses the RSA Crypto-J version 5.0 cryptographic module to secure administrator access to the web GUI using HTTPS over TLS, consistent with RFC 2818. The TOE's HTTPS implementation uses the digital signature services specified in FCS_COP.1(2) to authoritatively identify the web site that contains the GUI application. The underlying TLS implementation that secures the application layer communications uses the symmetric key cryptography defined in FCS_COP.1(1) to encrypt and decrypt data that is transmitted over this remote interface."

FCS_HTTPS_EXT.1.2

Same as FCS_HTTPS_EXT.1.1

FCS_RBG_EXT.1.1

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.

The TSS states "The TOE uses the RSA Crypto-J version 5.0 cryptographic module to generate random numbers used for other cryptographic operations performed by the TSF. The deterministic random bit generator is an HMAC implementation of NIST SP 800-90 (CAVP certificate #57). Because the TOE is a software product that can be installed on a general-purpose computer, the RSA Crypto-J version 5.0 cryptographic module is designed to seed its random number generator with entropy that is collected from the Operational Environment. For more information about the collection and conditioning of entropy, refer to the supplemental Entropy Documentation and Assessment document."

FCS_RBG_EXT.1.2

Same as FCS_RBG_EXT.1.1

FCS_TLS_EXT.1.1

This Assurance Activity requires the TSS to describe the implementation of TLS and specify any optional characteristics. The TSS should also ensure the ciphersuites specified are identical to those listed in the SFR. 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.

The TSS states "The TOE uses the RSA Crypto-J version 5.0 cryptographic module to secure connections between itself and remote entities in the Operational Environment using TLSv1.0 or TLSv1.2. The ciphersuites supported are TLS_RSA_WITH_AES_128_CBC_SHA and TLS_RSA_WITH_AES_256_CBC_SHA. The implementation of these ciphersuites requires the use of the symmetric encryption defined by FCS_COP.1(1), the asymmetric encryption defined by FCS_CKM.1 and FCS_COP.1(2), and the cryptographic hashing defined by FCS_COP.1(3). In the evaluated configuration, no optional characteristics such as extensions or client authentication are supported.

FIA_USB.1.1

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.

The TSS states that the ability to manage the TSF is role based. A session cookie is created when administrators authenticate to the TOE. The TSS goes on to explain that the administrator's subject identity is not explicitly associated with the administrator's web session so any change in their permissions while they are authenticated will take immediate effect.

FIA_USB.1.2

Same as FIA_USB.1.1

FIA_USB.1.3

Same as FIA_USB.1.1

FMT_MOF.1.1

This Assurance Activity requires the TSS to discuss the assignments that were competed in the SFR and ensure they are consistent with the guidance. Also, the TSS should describe how the TSF performs the management functions and what authorizations are required to perform those functions.

The TSS specifies the two applications available to manage the TOE by authorized administrators. The TSS references table 6-3 in the ST that defines the roles and the management functions that the different roles are authorized to manage. The assignments that are in the SFR are consistent with the application notes that were used as guidance.

FMT_MTD.1.1

The evaluator shall review the TSS in order to determine the repository in which the authentication data used by the TOE is stored. The evaluator shall also determine how communications with this repository is secured.

According to the TSS, the authentication data is stored in the Identity Store and communication is protected using TLS.

FMT_SMF.1

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

The TSS states "For each of the security functions that are defined as part of the TSF, the TOE either provides administrators with the capability to manage the function or the function automatically operates exclusively in a secure manner once the initial configuration of the TOE has been completed."

FMT_SMR.1.1

This Assurance Activity requires the TSS to discuss the roles defined and that they are consistent with how management authorizations are determined.

The TSS references table 8-2 which lists the different Administrator roles and their privilege summary.

FMT_SMR.1.2

Same as FMT_SMR.1.1

FPT_APW_EXT.1.1

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.

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. The TSS explains that the password data is store in the Identity Store and RDBMS which lies in the Operational Environment and is hashed before it is transmitted. The data is stored in reversible encryption in the RDBMS

FPT_APW_EXT.1.2

Same as FPT_APW_EXT.1.1

FPT_SKP_EXT.1.1

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.
The TSS states "Keys and cryptographic parameter data used by the TSF at run-time is stored in plaintext in volatile memory only. The key data is stored in a keystore file within the WebLogic server's domain configuration directory. The password for this keystore file is stored in the Credential Store within the RDBMS. There is no interface to the TOE that allows an administrator to access this data in the clear."

FTP_ITC.1.1

This Assurance Activity requires the evaluator shall to check the TSS to see that it identifies the trusted channels that are established and the protocols that they use. If third-party cryptography is used, the evaluator shall check to ensure that the specific third-party products that are used are identified along with the channel(s) that they are responsible for securing. The evaluator shall also check the TSS to ensure that a discussion is provided on the means by which secure communications are facilitated.

The TSS describes the trusted channels that are established between the TOE and Identity Store, RDBMS, and any distributed connectors. All secure remote communications are protected using TLS 1.0 or TLSv1.2. Also, some connector communicate using SSH which is provided by the OS.

FTP_ITC.1.2

Same as FTP_ITC.1.1

FTP_ITC.1.3

Same as FTP_ITC.1.1

FTP_TRP.1.1

The evaluator shall check the TSS to ensure that it identifies the protocol(s) used to establish the trusted path. If third-party cryptography is used, the evaluator shall check to ensure that the specific third-party products that are used are identified.

The TSS specifies TLS/HTTPS as its trusted path for the webGUI and T3 and also uses RSA Crypto-J version 5.0 to implement the secure communications protocols used to establish the path.

FTP_TRP.1.2

Same as FTP_TRP.1.1

FTP_TRP.1.3

Same as FTP_TRP.1.1

Additionally, the assurance activity for ALC_CMC.1 requires the ST to identify the product version that meets the requirements of the ST such that the identifier is sufficiently detailed to be usable for acquisitions. The ST clearly identifies the product model numbers that comprise the Oracle Identity Manager (OIM).

3 Operational Guidance Assurance Activities

The evaluation team completed the testing of the Operational Guidance, which includes the review of the *Oracle Identity Manager 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 Identity and Credential Management, version 2.1 [ICMPP]. The Supplemental AGD contains installation, configuration and operational documentation for the use of Oracle Identity Manager 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 Identity Manager guidance documents were reviewed to assess the Operational Guidance Assurance Activities. The Supplemental AGD contains references to these documents in Chapter 6 and these references can also be found below:

- Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management (Installation Guide) - http://docs.oracle.com/cd/E52734_01/core/INOAM/toc.htm
- Oracle Fusion Middleware Administering Oracle Identity Manager (Administering OIM Guide) – http://docs.oracle.com/cd/E52734_01/oim/OMADM/toc.htm
- Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager (Performing Self Service Guide) - http://docs.oracle.com/cd/E52734_01/oim/OMUSG/toc.htm
- Enterprise Deployment Guide for Oracle Identity and Access Management (Deployment Guide) - http://docs.oracle.com/cd/E52734_01/core/IMEDG/toc.htm
- Oracle Identity Manager Version 11g Release 2 Common Criteria Evaluation Security Target (ST)
- Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite

(Integration Guide) - https://docs.oracle.com/cd/E52734_01/oim/IDMIG/toc.htm
- Fusion Middleware Developer's Guide for Oracle Identity Manager (Developer's Guide) - http://docs.oracle.com/cd/E27559_01/dev.1112/e27150/toc.htm
- Oracle® Fusion Middleware Administrator's Guide (Administrator's Guide) - http://docs.oracle.com/cd/E52734_01/core/ASADM/toc.htm

The evaluators reviewed the ICMPP 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 ICMPP that have been claimed by the TOE (some SFRs are conditional or optional) as well as the AGD SAR, 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.

ESM_EAU.2 – The AA for this SFR requires that the operational guidance contain information on how to determine if a user of the TOE requesting access has been authenticated and how the TOE validates the authentication credentials. The Supplemental AGD section 4.1 discusses the process in which an administrator is authenticated to the TOE. In the evaluated configuration, OIM uses OAM as its authentication server. Once the administrator provides the credentials, OAM compares them to what is stored in the Identity Store that is being used for authentication. Once the credentials have been confirmed the administrator is then redirected to OIM. This addresses all required information in the AGD AA for this SFR.

ESM_EID.2 – The ICMPP does not contain an AGD AA for this SFR.

ESM_ICD.1 – The AA for this SFR requires that the operational guidance contain an indication as to how identity and credential data are supplied to the TOE and that the data are identified. Identity and credential data are supplied to the TOE by performing reconciliation from IT entities within the operational environment or creating the data within OIM. Chapter 12 of the Administering OIM Guide describes the reconciliation process. Chapter 15.2 of the Performing Self Service Guide describes the steps necessary to create users in OIM. Once users are created, the administrator is able to request accounts to any of the IT entities within the OE. However, if a non-administrator user requests the account, they must wait for approval from an administrator in order to receive access to that account. Chapter 5.3.1 of the Performing Self Service Guide describes the process of requesting accounts.

This information describes all available methods of supplying identity and credential data to the TOE, sufficiently addressing the AGD AA for this SFR.

ESM_ICT.1 – The AA for this SFR requires that the AGD describe (1) how to create and update identity, credential, and attribute data, (2) circumstances under which new or modified data are transmitted to ESM products, and (3) how to configure these circumstances. An administrator is capable of creating and modifying identity and credential data within OIM. Chapter 15.2 of the Performing Self Service Guide describes the steps necessary to create users in OIM. After this data is created/modified, the data is immediately provisioned to the target entity in the operational environment. This provisioning takes place immediately and there is no configuration available to change this action. Chapter 5.3 of the Performing Self Service Guide describes the necessary steps for system administrators to request accounts for themselves and for other users. Non-administrator users may also request accounts and modify their own identity and credential data, however, approval by an administrator may be necessary to receive the

accounts and/or provision the data. Based on the above information, all information required by the AGD AA for this SFR has been provided.

FAU_GEN.1 – The AA for this SFR requires that the operational guidance (1) list all auditable events along with a description of each type of record's contents and (2) provide all audit format types along with a description of each field. The AA also requires that the evaluator (3) check to make sure every PP mandated audit type is described and that the description of the fields contains the information required in FAU_GEN.1.2 and Table 3 of the PP. Section 4.2 of the Supplemental AGD discusses auditing/logging performed by OIM. It summarizes the auditable events and audit record contents created by administrator action as follows: "Audit logs are generated for security-relevant events that occur to OIM data such as creation and modification of users, roles, organizations, policies, organization members, and unauthorized actions (violations).

Audit logs are stored in the AUDIT_EVENT table in the RDBMS and contain the following security relevant attributes:

- event_id – unique identifier for the event
- event_action – operation performed (create, modify, delete, etc.)
- event_date – timestamp of the operation
- event_actor_name – authenticated name of the user that performed the action
- event_mechanism – method that caused the event (self-service, admin, request, policy-based)
- event_request_id – ID value of the request if the event that caused the event was a request
- event_status – outcome (success or failure) of the event
- event_fail_reason – descriptive reason for any failed events (policy violation, locked account, request rejected)"

In addition, the AGD references Oracle's existing documentation for a full list of auditable events and audit record contents.

FAU_STG_EXT.1 – The AA for this SFR requires the operational guidance to describe (1) any configuration steps necessary to set up audit storage and (2) a description of the interface to external audit repositories, including how the connection is established to it, how data are passed to it, and what happens when the connection is lost and re-established. The Supplemental AGD section 3.1 discusses the initial installation of the TOE and the environmental components that are included in the evaluated configuration. The database that stores the audit data is installed prior to installing the TOE. Configuration of the TOE to connect to the database is discussed in Section 8.13 of the Deployment Guide. However, this section does not include the secure communications configuration. Configuring the TOE for secure communications using TLS is discussed in Section 3.5 of the Supplemental AGD. Section 4.2 of the Supplemental AGD document provides a description of the interface in which the TOE connects to the database. When the connection from the TOE to the database is lost, the TOE will cease to function. An administrator will not be able to access the TOE until the connection is restored. Based on the above information, the AGD AA requirements for this SFR have been sufficiently addressed.

FCS_TLS_EXT.1 – The AA for this SFR requires the operational guidance to ensure that it contains instructions on configuring the TOE 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). Chapter 3 of the Supplemental AGD discusses step by step procedures for configuring the TOE to conform to the TLS requirements. Section 3.4 of the Supplemental AGD specifies which TLS cipher suites should be defined and restricted in order to meet this requirement.

FIA_USB.1 – The AA for this SFR requires that the operational guidance specify the manner in which external data sources and invoked and mapped to user data controlled by the TSF. The Oracle database used by OIM stores a replicated copy of the administrator identity data for the purpose of mapping the authenticated administrator to their assigned privileges. Section 12.2 of the Administering OIM Guide discusses how the TOE can reconcile user data from external data sources (Identity Stores). Once the user data is reconciled, OIM will look for matching accounts that are stored in the database and link them with

the accounts from the Identity Store. Administrators can choose to ignore this automatic link and perform an "Ad-HOC" link to another account within OIM.

FMT_MOF.1 – The AA for this SFR requires (1) that the operational guidance specify the manner in which management functions are restricted and (2) how the TSF enforces those restrictions. (1) Chapter 16 of the Performing Self Service Guide specifies that the TSF restricts management functions through role-based access control. Roles determine what privileges an administrator has. The System Administrator has all of the privileges for each role. The other administrator roles have a sub-set of these privileges. Multiple roles can be assigned to an administrator. Chapter 16 of the Performing Self Service Guide also discusses how to manage these roles. This addresses the two items for this AGD AA.

FMT_MTD.1 – The AA for this SFR requires that the operational guidance specify (1) the data that can be managed and (2) who is allowed to manage those data. The operational guidance specifies that Identity (i.e. username/password) credential data can be managed, along with the attributes for each user." The Supplemental AGD references the vendor documentation that discusses non-administrator users managing their own identity and credential data and the process in which to do so (Chapters 3-5 of the Performing Self Service Guide). Chapter 15.4 of the Performing Self Service Guide discusses the process in with Administrators can manage the identity and credential data of other users.

FMT_SMF.1 – The AA for this SFR requires that the operational guidance defines the management functions that can be performed, how they are performed, and what they accomplish. Chapter 4 of the Supplemental AGD describes management function claimed in FMT_SMF.1 or references specific documentation that provides information on how to perform those functions the results of performing those functions. The management functions provided by OIM to securely administer the product in the evaluated configuration are referenced throughout this the Supplemental AGD under their associated security functional requirements (SFR).
Because all the management functions are addressed in the detail required by the AA, the AGD AA for this SFR is sufficiently addressed.

FMT_SMR.1 – The AGD AA for this SFR requires that (1) the operational guidance provides instructions on how to assign users to roles and (2) if the TSF provides only a single role that is automatically assigned to all users, that this is detailed. (1) Section 4.5 of the Supplemental AGD contains a brief summary of the roles that OIM provides. It also references the vendor documentation and points to the specific chapters where instructions on how to assign users to roles can be found.

FPT_APW_EXT.1 – The ICMPP does not contain an AGD AA for this SFR.

FPT_SKP_EXT.1 – There are no administrative functions associated with the protection of stored credentials. Administrative credentials are always stored securely and this is not configurable.

FTP_ITC.1 – The AA for this SFR requires that the operational guidance specify the manner in which secure communications are enabled. Configuration of trusted communications is performed by following the relevant steps outlined in Chapter 3 "Secure Installation and Configuration" portion of the Supplemental AGD. This information addresses the requirements of the AGD AA for this SFR.

FTP_TRP.1 – The AA for this SFR requires that the operational guidance describe (1) the methods in which users interact with the TOE, (2) the mechanism by a which the corresponding trusted path is established, and (3) if the TSF relies on any environmental components for its establishment. The Supplemental AGD section titled, "TOE Components" states that the OIM WebLogic Server Application is used to administer OIM via a web GUI and that no other method of administration is supported. Chapter 3 of the Supplemental AGD discusses step by step procedures to configure the TOE to use TLS for secure communications using the webGUI. This sufficiently addresses the requirements for this AA.

AGD_OPE.1 – The Assurance Activity for AGD_OPE.1 states that most of the Assurance Activities for the operational guidance are already covered in the separate activities for each SFR. However, an additional AA is specified for AGD_OPE.1 which requires the guidance to provide instructions for configuring the

cryptographic engine associated with the evaluated configuration of the TOE. The Security Target states that the TSF uses RSA Crypto-J version 5.0 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. These instructions are provided in Chapter 3 of the Supplemental AGD. This addresses the AGD requirements for this AA.

AGD_PRE.1 – The AA for AGD_PRE.1 requires the documentation to address all platforms of the TOE claimed in the evaluation. The TOE is a software-based solution that can be installed on compatible operating systems. As a result, 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. This addresses the AGD requirements for this AA

4 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).

4.1 Platforms Tested and Composition

The TOE is a software-based TOE. Depending on which Operating System that the user installs the TOE on determines the software that comes with the TOE. For instance, if the user installs the TOE on a Oracle Linux O/S, the software that comes with the TOE will be compatible with Oracle Linux. The evaluation team set up 2 test environments for the independent functional testing. One environment was using Oracle Linux 6 O/S and the other used Solaris 11 O/S. This allowed the evaluation team to perform all test assurance activities across the TOE and over the relevant interfaces showing that the results are consistent regardless of which O/S the TOE is installed on. 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.

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

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

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

Operating Systems:	Solaris 11

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

4.2 Equivalency Justification

TOE is a software only product that is capable of being installed on 3 different operating systems Oracle Linux 6, Redhat Linux 6, or Solaris 11. The evaluation team set up two test environments each consisting of all of the components listed in the evaluated configuration portion of this document. One environment was installed using the Oracle Linux 6 operating system and the other was installed using the Solaris 11 operating system. The Redhat Linux 6 operating system was not chosen for testing because the Oracle Linux 6 operating system is binary compatible with Redhat Linux 6 and the difference between these operating systems is that Oracle Linux has the option to support the same Redhat kernel as well as a more modern kernel only supported by Oracle. The differences in kernels would have no impact on this application which is installed on top of an application server running in user space. The Oracle Linux 6 and Solaris 11 test environments are configured with overlapping operational environment components with a variance on the connectors tested in each test environment. Additionally, the evaluation team created a sample of test cases where a majority of test cases were performed on both environments. The overlapping operational environment as well as test cases for the two test environments was devised to demonstrate that the TOE operated the same regardless of the operating system on which the TOE was installed. Thus, if the test steps, expected results and actual results were the same for where the test environments and testing overlapped, the evaluation team could reasonably conclude that the testing would be the same across both environments and the functionality of the TOE is operating system independent. Additionally, if the testing between the Oracle Linux 6 and Solaris 11 environments produced no differences between the test steps, expected results, and actual results for this overlap, the evaluation team could also conclude that the same would hold true for two operating systems that are binary compatible.

Each test environment also included connectors to allow the TOE to send and receive data to and from the IT entities within the operational environment such as the Identity Stores. Oracle separates these connectors into 3 groups; Identity Connector Framework connector, Legacy connector, and Remote Manager Connector. The evaluation team took a connector from each group as a sampling and installed and configured them for testing. All connectors have two functional parts: (1) an API component, for endpoint specific APIs to read and write to the endpoint system (2) an encryption component, for secure communications between the connector and the endpoint/TOE depending on the connector group. During the testing the evaluation team observed no differences in how the connectors operated, regardless of group or endpoint system. The TOE's GUI provides the same operations to an administrator for all managed endpoints which further justifies that the impact of the connectors is only in the manner data is read and written based on the APIs specific to the endpoint's method of managing its data. Additionally, the testing performed has a majority overlap between the two environments to validate that the TOE performs the same regardless of the specific operating system on which the TOE is installed as well as each type of connector that is installed.

The principal architecture for OIM 11gR2 is the Identity Connector Framework (ICF). This framework is the platform for the preponderance of OIM connectors, including any newly developed connectors. The connector framework, including its installation, API, and security, is identical across all ICF connectors. Individual connectors differ only by the minimum required by each endpoint. The architecture for the ICF is described in the Fusion Middleware Guide for Oracle Identity Manager, Chapter 9, "Understanding the Identity Connector Framework"

(https://docs.oracle.com/cd/E27559_01/dev.1112/e27150/icf.htm#OMDEV3264). Any ICF connector will meet the same standards; two (OID and OUD) were chosen for evaluation.

However, a small population of legacy connectors are used by customers. Such connectors do not use the Identity Connector Framework. Of these, older versions of the Active Directory connector are most often deployed. The evaluation chose a representative legacy connector, the Active Directory connector 9.1.1.7, described here: http://docs.oracle.com/cd/E11223_01/doc.910/e11197/toc.htm. In addition, another legacy connector supporting the Human Resources application E-Business Suite was also chosen (http://docs.oracle.com/cd/E11223_01/doc.910/e11203/toc.htm).

In general, the legacy connectors do not share the same architecture. This is however not considered a serious argument against general equivalency, as almost all connectors available in OIM 11gR2 use the ICF. For example, the Active Directory connector is also available in an ICF version; public documentation recommends that installations of the evaluated OIM (11gR2) use that newer connector. The older version was evaluated with the express purpose to examine the special case of a legacy connector.

The evaluation team performed testing of the TSF functionality across both of the installed environments. The testing performed on each environment, validated that the internal processing of the TOE would produce the same results regardless of the specific operating system on which the TOE is installed. Also, the testing performed on each connector, validated that the TOE would produce the same results regardless of the connector that was used to communicate with IT entities.

4.3 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 Management Identity and Credential Management, version 2.1' [ICMPP]. The evaluators reviewed the ICMPP 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 OPE. 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

001a - ESM_EAU.2 Reliance on Enterprise Authentication (OAM authentication against external LDAP store case)

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.	
Dependency:	None	
Setup:	1. Configure OIM to authenticate administrators using OAM connected to an external LDAP Store (OUD) 2. Create users in the OUD.	
Test Procedures:		**Expected Results:**
1. Log into the OIM System Administrator interface as the system administrator and perform an LDAP reconciliation. 2. Attempt to login to OIM using a valid username and password. 3. Attempt to login to OIM using a valid username and invalid password. 4. Attempt to login to OIM using an invalid username and valid password. Examine the audit records for evidence of the authentication attempts.		• After the recon, the user account that was created in the setup will be created in OIM. • The authentication attempt will be accepted. • The authentication attempt will be rejected. • The authentication attempt will be rejected. • All successful and failed authentication attempts are logged and contain the information required.
Actual Results:	Pass	

001b - ESM_EAU.2 Reliance on Enterprise Authentication (security question case)		
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.	
Dependency:	None	
Setup:	1. Create a user within OIM or select a user that resides in an identity store that is linked to OIM. 2. Define a set of security questions and answers for the user within the user's profile. Question – Favorite color Answer - red	
Test Procedures:		**Expected Results:**
1. On the OIM self-service login page, click the "Forgot Password" link. 2. In the "User Login" box enter an invalid username and click next. 3. Click OK to exit the error. 4. In the "User Login" box enter a valid username and click next.		• An error will appear stating that the system cannot proceed with the password reset.

5. Attempt to answer the question by entering an invalid answer in the box. 6. The next screen will appear asking to enter a new password. Enter any password. Enter any password. 7. Repeat step 1 and 4. 8. Enter the correct answer to the question. 9. Enter the new password and confirm with the same password. 10. Examine the audit records for evidence of the authentication attempts	• An error will appear stating the answers do not match what is stored. • The user's password will be successfully changed and the user is logged into the OIM. • All successful and failed authentication attempts are logged and contain the information required.
Actual Results:	Pass

002 – ESM_ICD.1.1 Identity and Credential Definition TEST1 (Creating/Modifying/Deleting Identity and Credential data and sending for consumption)	
Test Purpose:	The evaluator shall test this capability by using the TOE to create identity and credential data and sending this data to the compatible ESM product(s) for consumption. These tests shall exercise each capability described in the SFR, including the ability to enforce credential complexity requirements. The evaluator will then perform basic identity and credential-related actions on the compatible ESM products that use the identity and credential data in order to confirm that the data was applied appropriately.
Dependency:	None
Setup:	1. Ensure that OIM is connected to a valid Identity Store
Test Procedures:	**Expected Results:**
1. Create a user in OIM (Self Service). 2. Request accounts in the Identity stores (AD, OID, OUD) 3. Access the Identity Store directly and verify that the user data was provisioned. 4. Modify user data in OIM 5. Access the Identity Store and verify that the user data that was modified was provisioned. 6. Delete the user from OIM 7. Access the Identity Store and verify that the user data that was removed. Review audit data for the creation and modification of the data.	• User will be created in OIM. • User data will be provisioned to the Identity Store • User data will be provisioned to the Identity Store • The user data will be removed from the Identity Store. • Logs are generated for the creation and modifications to the user's identity data and contain the required information.

Actual Results:	Pass

003 ESM_ICD.1.2 Identity and Credential Definition		
Test Purpose:	To verify that identity attributes and the constraints that govern credential attributes defined in the Security Target can be applied to users or organizations as appropriate	
Dependency:	None	
Setup:	1. Ensure that OIM is connected to a valid Identity Store 2. Ensure that OIM is deployed to control at least one endpoint in the environment. NOTE: Specific steps (for setting up the endpoints themselves and for defining them in OIM) will depend on the endpoints used and can be listed while on site	
Test Procedures:		**Expected Results:**
For a given user defined by the Identity Store, perform the following steps to verify that the user has appropriate attributes defined for it. **Credential Lifetime** 1. Define a credential lifetime of one day for the user's password. 2. Reset the user's password. 3. Use the password to authenticate the user and verify that it is accepted. 4. Wait one day (or modify the relevant system clock(s) to make it appear as if one day has passed) and verify that the password is not accepted and the user is prompted to change it. **Basic Identity Attributes** 1. For each out-of-the-box user identity attribute (first name, last name, email address, etc.), verify that they can be changed within OIM. 2. List the attributes that cannot be changed (user id?) and verify that OIM provides no mechanism to change them. 3. For each security-relevant identity attribute, perform some activity using OIM or mediated by OIM before and after the change to ensure that the correct data is being used. **Extended Identity Attributes** 1. Define an arbitrary extended attribute called Test Attribute. 2. Enter Test Attribute in the field just created. 3. Verify that a user can be assigned these two values for this attribute.		• Password is reset • User is forced to change password • Attributes can be changed • Change in attributes has an observable effect • Only **Object GUID** attribute cannot be changed. • Attribute is created • Attributes can be assigned

Credential History (Disallow Past Passwords) 1. Configure OIM such that a user's password cannot be any of their previous 3 passwords. 2. As the System Administrator, change the password for a user within OIM that has accounts in the environment (AD, OID etc…) 3. Login to an endpoint to show that the password is implemented. 4. Attempt to change the user's password to the password originally set for step 2. 5. Arbitrarily change the user's password a 3rd time. 6. Repeat step3 7. Repeat step 4.	• User logs in successfully • Password cannot be changed. • Password is changed • User logs in successfully • Password cannot be changed
User Status 1. Ensure the user account is enabled. 2. Log in as the user and verify that this is allowed. 3. Set the user account to be disabled. 4. Attempt to log in as the user and verify that this is not allowed. Review logging to determine that each event of the creation, modification, and/or assignment of user attributes performed above is logged.	• User logs in successfully • User does not log in successfully • Verify the changes to the user's identity data were logged by OIM • Logs are generated for the creation and modifications to the user's identity data and contain the required information.
Actual Results:	Pass

004 – ESM_ICD.1.3 Identity and Credential Management Definition (User Enrollment)	
Test Purpose:	To verify that enterprise users managed by OIM can be enrolled through an external product and recognized by OIM.
Dependency:	None
Setup:	The OIM environment is configured such that the Identity Store used by OIM is configured to work with an HR system.

Test Procedures:	**Expected Results:**
1. Create a user using the JXPlorer application connected to the OID. 2. In OIM, create a user with the username "bahtest004" 3. Run the OID Connector user search reconciliation job. 4. Repeat step 1 and create the user in AD. (bahtest004ad) 5. Repeat step 2 except create user bahtest004ad. 6. Repeat step 3 except run the AD target user recon job.	• A list of users is displayed • The users that were created in step 1 and 4 are now reconciled to OIM and linked to the user account created in OIM.

Capture the audit logs that are generated for the reconciliation of the user to OIM.	• Logs are generated for the reconciliation (enrollment) of the users to OIM and the log contains all information required.
Actual Results:	Pass

005 – ESM_ICD.1.7 Identity and Credential Management Definition (Externally Updated Credentials)	
Test Purpose:	To verify that user credentials modified in OUD are reconciled to OIM.
Dependency:	None
Setup:	Create a user in OUD. This can be the same user that was created in Test001a. NOTE: If using the existing user, go directly to step 2.

Test Procedures:	**Expected Results:**
1. In the System Admin interface of the TOE, conduct the LDAP User Create and Update Full Recon. Job.	• The user created will be reconciled to OIM.
2. Log in to the TOE using as the user created in OUD in the setup procedures.	• This will log the user in the TOE and prove that the credentials created are reconciled to OIM.
3. In OUD, change the password to the user created.	
4. Repeat step 1.	• The password will reconcile to OIM
5. Repeat step 2.	• User will be logged into OIM with the new password.
Review and capture any log files that show the data being sent to the TOE.	• Log files are generated for the update of user credential data and all information required is included.
Actual Results:	Pass

006 – ESM_ICD.1.8 Identity and Credential Definition (Password Policy)	
Test Purpose:	For password-based credentials, the evaluator shall identify that all password composition, configuration, and aging requirements specified in the ST are discussed in the TSS and AGD and test these capabilities one at a time (for example: set minimum password length to 6, observe that a 7 character password and a 16 character password are both accepted, then change the minimum length to 8, observe that a 7 character password is rejected but that a 16 character password is accepted)
Dependency:	None
Setup:	Create a user from an endpoint within the environment (This can be a user that already exists in the environment.)

Test Procedures:	**Expected Results:**
1. Log into the OIM Self Service interface as the system administrator and create an organization called Test006.	
2. Click on Policy from the main menu and select Password Policy.	• The password policy

3. Set the password policy and name it Test005 4. Add the created password policy to the organization Test006. (Created in Step 1) 5. Add the user to the organization. (Test006) 6. Logout of OIM and log in as the user from step 5d. 7. Navigate to Manage →Users → "user" →Reset Password 8. Attempt to change the password to something that is inconsistent to the password policy. 9. Log in to the AD server using the password that was just changed. 10. Change the password policy. 11. Navigate to Manage →Users → "user" →Reset Password 12. Attempt to change the password to something that is inconsistent to the password policy. (NOTE: By clicking on the blue "i" button next to the "New Password" the password policy will show.) **13.** Log into the OID using the changed password. **(NOTE: We conducted an LDAPSEARCH command using the username and password that was just changed. This is the only way to show the password works.)** 14. Request an account to OUD and then reset the password again. 15. Repeat step 13 and conduct ldap search with OUD. Review and capture the logs for the creation and modification of the password policy.	"Test005" will be created • The password policy will be attached to the organization. • The password policy will enforced for every user in the Test organization • Step 8a/b - The password change will be rejected • Step 8c - The password change will be accepted • The user will log into AD Server • Step 12a/b - The password change will be rejected • Step 12c - The password change will be accepted • The LDAP search will show that the password was accepted. • The creation and modification of the password policy is logged and contains all required information.
Actual Results:	Pass

007 – ESM_ICT.1 Identity and Credential Transmission

Test Purpose:	The evaluator shall test this capability by obtaining the compatible ESM products. Following the procedures in the operational guidance for both the ICM and other ESM products, the evaluator shall create the indicated data (i.e., identity, credential, and potentially object attribute data) and ensure that the defined evaluator shall create the indicated data (data is transmitted and installed successfully in compatible ESM products, in accordance with the circumstances defined in the SFR. In other words, (a) if the selection is completed to transmit after creation of new data, then the evaluator shall create the new data and ensure that, after a reasonable window for transmission, the new data is installed; (b) if the selection is completed to transmit periodically, the evaluator shall create the new data, wait until the periodic period has passed, and then confirm that the new data is present in the appropriate ESM components; or (c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the data, use the Secure Configuration Management component to request transmission, and the confirm that the appropriate ESM components have received and installed the data. If the ST author has specified "other circumstances", then a similar test shall be executed to confirm transmission under those circumstances. The evaluator shall then make a change to the previously created data, and then repeat the previous procedure to ensure that the updated data is transmitted to the compatible ESM components in accordance with the SFR-specified circumstances. Lastly, as updating data encompasses deletion of data, the evaluator shall repeat the process a third time, this time deleting the data to ensure it is removed as active data from the compatible ESM components.
Dependency:	None
Setup:	Endpoints are set up in the environment. 1. The user that is defined in the ID store needs to be reconciled with an account in OIM.

Test Procedures:	**Expected Results:**
Changes to Identity Store from OIM (after creation of new data) 1. View all attribute data for a given user in the Identity Store/Endpoint using a mechanism other than OIM. (OID,AD,Exch) 2. Log into the OIM as the system administrator and click on the manage tab → Users → Search for the user that is in the ID Store and reconciled to OIM. 3. Click on "Accounts" tab and select the account that is on an endpoint and then select "Modify Accounts". 4. Change an attribute that is in the account. 5. Click "Update" and the "Submit". 6. Repeat step 1 and observe that the changes made by OIM were transmitted to the Identity Store.	• Account will be modified. • The Identity Store is updated.
Delete the data 7. Look in the ID store and ensure a user account is linked to OIM user. 8. From OIM, delete the user account to the ID Store. 9. From the ID store, look for the user in step 11.	• The user account in the ID store is deleted • The deleted account is reflected in OIM.

Review the log data for modification and the transmission of data.	• The log data shows the transmission of data and the modifications to the attribute data.
Actual Results:	Pass

008 – FAU_GEN.1 Audit Data Generation		
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 that revokes a credential from a user, the audit log for the event should correctly indicate a revocation operation.	
Dependency:	None	
Setup:	None	
Test Procedures:		**Expected Results:**
1. Log into the System Administration interface as the System Administrator. 2. Click "Scheduler" on the left side of the page. 3. In the System Configuration tab, find the "User profile audit data collection level" property name and enter "None" as the value. 4. To turn this back on, simply enter Resource Form in the Value field.		• OIM will produce an audit record for the shutting off of auditing. • OIM will produce an audit record when auditing is turned on.
Actual Results:	Pass	

009 – FAU_STG_EXT.1 External Audit Trail Storage

Test Purpose:	The evaluator shall test this function in conjunction with testing of FAU_GEN.1 by confirming that the same set of audit records are received by each of the configured audit destinations. 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.	
Dependency:	None	
Setup:	None	
Test Procedures:		**Expected Results:**
1. Make the RDBMS unavailable to the TOE so that the audit records are not able to be sent to the database. (Turn off or disconnect from the TOE.) 2. Attempt to navigate to the OIM web interface.		• Audit records will be generated for disconnect. • Create some sort of evidence that shows the TOE as being unable to perform any authentication/functional administrative tasks.
Actual Results:	Pass	

010 – FCS_TLS_EXT.1 TLS		
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).	
Dependency:	ESM_ICT.1, FTP_ITC.1, FTP_TRP.1	
Setup:	None	
Test Procedures:		**Expected Results:**
1. For each method of secure remote communications that use TLS (user to web browser, OIM to connectors, OIM to RDBMS, OIM to Identity Store, etc.), capture traffic between OIM and the remote endpoint. 2. Review the traffic captures to identify the TLS cipher suites allowed by OIM.		• All traffic described as using TLS in the Security Target and Functional Specification are observed to use TLS. • Supported cipher suites are consistent with what is listed in the Security Target.
Actual Results:	Pass	

012 – FIA_USB.1 – User Subject Binding

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 a certain set of data, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF, they do not have write access to that data. 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.
Dependency:	None
Setup:	1. In the environment, an ID store must be configured as a Trusted Source. A trusted source is able to store user data and replicate users to the TOE.

Test Procedures:	**Expected Results:**
1. Log into the DB and see that the user created in the setup has no admin privileges.	• DB will show the user has no admin privileges.
2. As the system administrator, assign the user from the setup "System Administrator" role	• The created user data will be propagated to the DB.
3. In the Database, conduct a query that shows the admin roles assigned to the user. (Repeat step 1)	• The DB will show that the user has the SysAdmin privilege.
4. Logout as the System Administrator and log in as the user just granted the "System Administrator" role.	• User will have all of the privileges available as the System Administrator.
5. Navigate through the OIM and ensure that the privileges are accurate for the role assigned. (System Admin as full privileges)	
6. Log out and log back in as the normal System Admin(xelsysadm) and revoke the Sys. Admin privilege from the user and assign a different Admin privilege.	
7. Login in to the OIM as the user and attempt to perform an activity only a System Administrator can perform.	• The action will be denied.
Actual Results:	Pass

013 – FMT_MOF.1 Management of Functions Behavior (Negative Testing)		
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.	
Dependency:	None	
Setup:	None	
Test Procedures:		**Expected Results:**
1. For each authorized role in the Security Target, (System Administrator, System Configuration Administrator, User Administrator, Organization Administrator, Help Desk, User Viewer) 2. Assign the user to System Configuration role. 3. Attempt to perform activities that are not allowed by this role (negative testing). 4. Remove the role from the user. 5. Repeat step 2 for each of the roles listed. 6. Review and capture the log data for the management functions performed. Note: The assurance activity has three parts: 1. "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." 2. "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." 3. "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." The lab conducted testing validated the following: 1. This was tested through the combination of testing the other SFRs. More than one privileged administrator was used to configure and run the tests for the other SFRs and in all cases those administrators	• The user will be assigned the Admin role specified. • The allowable activities are consistent with the permissions defined in the Security Target. Management activities performed by each administrator are logged and contain all required information.	

were able to successfully manage the TOE per Table 6-3 in the Security Target. The assurance activity states that the tester should use "one or more appropriately privileged administrative accounts" and it is important to note that the testing conducted did not include a complete coverage of all management functions and role combinations. 2. This statement does not apply since it is not being managed by a Secure Configuration Management product. 3. This part of the assurance activity states "perform a sampling of the available management functions" and "using one or more unprivileged accounts to observe that the activities are rejected or unavailable".This test case was performed for a sample of roles and security functions to demonstrate authorization control of the TOE perTable 6-3 in the Security Target. It is important to note that the testing conducted did not include a complete coverage of negative tests for all management functions and role combinations.	
Actual Results:	Pass

016 – FMT_SMR.1 Security Management Roles		
Test Purpose:	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.	
Dependency:	None	
Setup:	1. Create a user in OIM. (This could be a user that has already been created from a previous test.)	
Test Procedures:		**Expected Results:**
1. Login to the OIM as the System Administrator. 2. Create an Admin Role and add the user to this custom role. 3. Perform activities that the custom role has the capability.		• The user will be assigned to this role
Actual Results:	Pass	

017 – FPT_APW_EXT.1 Protection of Stored Credentials		
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.	
Dependency:	None	
Setup:	None	
Test Procedures:		**Expected Results:**
Oracle 11g Database 1. Login into the RDBMS as the system administrator using SQLPlus.		• Passwords are obscured via reversible encryption.

2. Search for the user files and query the username and password files. OID 3. Log into the OID using JXplorer. 4. Select any user. Active Directory 5. Log into the AD instance and navigate to c:\Windows\Ntds\ and open the ntds.dit file.	• The attribute list will show that the passwords are obscured via hash. • Passwords stored in this database file are obscured via hash.
Actual Results:	Pass

019 – FTP_ITC.1 Inter-TSF Trusted Channel	
Test Purpose:	The evaluator shall test this capability by enabling secure communications on the TOE and placing a packet sniffer on the local network. They shall then use the TOE to perform actions that require communications to all trusted IT products with which it communicates and observe the captured packet traffic that is directed to or from the TOE to ensure that their contents are obfuscated.
Dependency:	This test can be performed in conjunction with FCS_TLS_EXT.1.
Setup:	1. Setup a test machine with Wireshark on the network between the TOE and the other IT entities. (i.e. RDBMS, Identity Store, connectors)

Test Procedures:	**Expected Results:**
1. Start the Wireshark packet capture on the test machine to monitor traffic from the OIM console. 2. Login to the OIM console and create and send a policy or perform an activity that will send data to the RDBMS. 3. Stop the packet capture. 4. Repeat steps 1 and 2. This time perform an action that will send data to the Identity Store (create a user or change attributes in a user account.) 5. Stop the packet capture. Review and capture the logs for the establishment of the trusted channel.	• Wireshark will capture the packets and show that the data was sent encrypted via TLS. • Wireshark will capture the packets and show that the data was sent encrypted via TLS. • The log files generated show the establishment of the connection and all required information.
Actual Results:	Pass

020 – FTP_TRP.1 Trusted Path

Test Purpose:	The evaluator shall test this capability in a similar manner to the assurance activities for FTP_ITC.1. If data transmitted between the user and the TOE is obfuscated, the trusted path can be assumed to have been established.	
Dependency:	None	
Setup:	1. Setup a test machine with Wireshark on the network between the TOE and the remote GUI. (This could also be the machine in which you connect to the TOE)	
Test Procedures:		**Expected Results:**
1. In Firefox, change the ciphersuites to only allow connection using rsa_aes_cbc_128. (url-about:config) 2. Start the Wireshark packet capture on the test machine to monitor traffic from the IP address of the machine running the remote GUI. 3. Navigate to the url and login to the OIM. 4. Stop the packet sniffer. 5. Repeat steps 1-4 except using rsa_aes_cbc_256 ciphersuite. 6. In the About:config page in Firefox, enable all of the ciphersuites available with the exception of the two that are tested in the previous steps. 7. Repeat steps 2-4 Review and capture the logs.		• The packet sniffer will show the traffic to the OIM and will be obfuscated using the TLS ciphersuite specified in step 1. • The packet sniffer will show the traffic to the OIM and will be obfuscated using the TLS ciphersuite specified in step 1 • There will be no connection to the TOE and the packet sniffer will show that the handshake with the server was terminated and the ciphersuites were disallowed. • The log files generated show the establishment and failure to establish connection and all required information.
Actual Results:	Pass	

021 – FCS_COP.1(1) Cryptographic Operation (for Data Encryption/Decryption)		
Test Purpose:	The evaluators shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", "The XTS-AES Validation System (XTSVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.	
Dependency:	None	
Setup:	None	
Test Procedures:		**Expected Results:**
1. The TOE incorperates the RSA BSAFE Crypto-J version 5.0 (CMVP certificate #1503) which was evaluated on Linux and Solaris operating systems. This CMVP certificate includes the following CAVP certificates which included the testing for this SFR's assurance		The CMVP/CAVP certificates are applicable to the TOE's crypto module and tested the SFR's assurance activity.

activity: • AES (CAVP certificate #1465) • RSA (CAVP certificate #717) • SHA-1, SHA-256, or SHA-384 (CAVP certificate #1328) • HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 (CAVP certificate #863) • DRBG (CAVP certificate #57)	
Actual Results:	Pass

022 – FCS_COP.1(2) Cryptographic Operation (for Cryptographic Signature)	
Test Purpose:	The evaluators shall use the signature generation and signature verification portions of "The FIPS 186-3 Digital Signature Algorithm Validation System (DSAVS)", "The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and "The RSA Validation System (RSAVS)" as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.
Dependency:	None
Setup:	None

Test Procedures:	**Expected Results:**
1. The TOE incorperates the RSA BSAFE Crypto-J version 5.0 (CMVP certificate #1503) which was evaluated on Linux and Solaris operating systems. This CMVP certificate includes the following CAVP certificates which included the testing for this SFR's assurance activity: • AES (CAVP certificate #1465) • RSA (CAVP certificate #717) • SHA-1, SHA-256, or SHA-384 (CAVP certificate #1328) • HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 (CAVP certificate #863) • DRBG (CAVP certificate #57)	The CMVP/CAVP certificates are applicable to the TOE's crypto module and tested the SFR's assurance activity.
Actual Results:	Pass

023 – FCS_COP.1(3) Cryptographic Operation (for Cryptographic Hashing)	
Test Purpose:	The evaluators shall use "The Secure Hash Algorithm Validation System (SHAVS)" as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.
Dependency:	None
Setup:	None

Test Procedures:	**Expected Results:**
1. The TOE incorperates the RSA BSAFE Crypto-J version 5.0 (CMVP certificate #1503) which was evaluated on Linux and Solaris operating systems. This CMVP certificate includes the following CAVP certificates which included the testing for this SFR's assurance activity: • AES (CAVP certificate #1465) • RSA (CAVP certificate #717) • SHA-1, SHA-256, or SHA-384 (CAVP certificate #1328) • HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 (CAVP	The CMVP/CAVP certificates are applicable to the TOE's crypto module and tested the SFR's assurance activity.

certificate #863) • DRBG (CAVP certificate #57)	
Actual Results:	Pass

024 – FCS_COP.1(4) Cryptographic Operation (for Keyed-Hash Message Authentication)		
Test Purpose:	The evaluators shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.	
Dependency:	None	
Setup:	None	
Test Procedures:		**Expected Results:**
1. The TOE incorperates the RSA BSAFE Crypto-J version 5.0 (CMVP certificate #1503) which was evaluated on Linux and Solaris operating systems. This CMVP certificate includes the following CAVP certificates which included the testing for this SFR's assurance activity: • AES (CAVP certificate #1465) • RSA (CAVP certificate #717) • SHA-1, SHA-256, or SHA-384 (CAVP certificate #1328) • HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 (CAVP certificate #863) • DRBG (CAVP certificate #57)		The CMVP/CAVP certificates are applicable to the TOE's crypto module and tested the SFR's assurance activity.
Actual Results:	Pass	

025 – FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)	
Test Purpose:	Regardless of the standard to which the RBG is claiming conformance, the evaluator performs the following test: Test 1: The evaluator shall determine an entropy estimate for each entropy source by using the Entropy Source Test Suite. The evaluator shall ensure that the TSS includes an entropy estimate that is the minimum of all results obtained from all entropy sources. Implementations Conforming to FIPS 140-2, Annex C The reference for the tests contained in this section is The Random Number Generator Validation System (RNGVS) [RNGVS]. The evaluators shall conduct the following two tests. Note that the "expected values" are produced by a reference implementation of the algorithm that is known to be correct. Proof of correctness is left to each Scheme. The evaluators shall perform a Variable Seed Test. The evaluators shall provide a set of 128 (Seed, DT) pairs to the TSF RBG function, each 128 bits. The evaluators shall also provide a key (of the length appropriate to the AES algorithm) that is constant for all 128 (Seed, DT) pairs. The DT value is incremented by 1 for each set. The seed values shall have no repeats within the set. The evaluators ensure that the values returned by the TSF match the expected values. The evaluators shall perform a Monte Carlo Test. For this test, they supply an initial Seed and DT value to the TSF RBG function; each of these is 128 bits. The evaluators shall also provide a key (of the length appropriate to the AES algorithm) that is constant throughout the test. The evaluators then invoke the TSF RBG 10,000 times, with the DT value being incremented by 1 on each iteration, and the new seed for the subsequent iteration produced as specified in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3. The

	evaluators ensure that the 10,000th value produced matches the expected value. Implementations Conforming to NIST Special Publication 800-90
Test Purpose:	The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality. If the RNG has prediction resistance enabled, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90). If the RNG does not have prediction resistance, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call. The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator. Entropy input: the length of the entropy input value must equal the seed length. Nonce: If a nonce is supported (CTR_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length. Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied. Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.
Dependency:	None
Setup:	None

Test Procedures:	**Expected Results:**
1. The TOE incorperates the RSA BSAFE Crypto-J version 5.0 (CMVP certificate #1503) which was evaluated on Linux and Solaris operating systems. This CMVP certificate includes the following CAVP certificates which included the testing for this SFR's assurance activity: • AES (CAVP certificate #1465) • RSA (CAVP certificate #717) • SHA-1, SHA-256, or SHA-384 (CAVP certificate #1328) • HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 (CAVP certificate #863) • DRBG (CAVP certificate #57)	The CMVP/CAVP certificates are applicable to the TOE's crypto module and tested the SFR's assurance activity.

Actual Results:	Pass

4.4 Assesment 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.

4.4.1 Physical Assessment

Oracle Headquarters located in Redwood City, CA is the physical location for the Oracle Identity Manager (OIM) test environment. Booz Allen reviewed the physical security controls of the test environment and interviewed Oracle employees to ensure that the Oracle Identity Manager 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 OIM is installed on are located is in secured internal room located at the Oracle Headquarters location. Thus, physical access to the OIM 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.

4.4.2 Logical Assessment

The functional testing can be executed remotely from the physical test environment. The only way to access the server is from an Oracle approved laptop that is connected to the Oracle LAN and with the proper credentials (username/password). Booz Allen was supplied an Oracle approved laptop that is located on Oracle's LAN for evaluation purposes and no other personnel had access to this laptop. At the end of each work day, the laptop itself was stored in a secure room locked by a key. Any configuration performed by Oracle personnel during the functional testing timeframe was conducted using the 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.

4.5 Vulnerability Testing

The vulnerability analysis is in a proprietary report prepared by the lab. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerabilities. All vulnerabilities have been addressed through patches and configuration guidance.

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

5 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.

6 Glossary of Terms

Acronym	Definition
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ICF	Identity Connector Framework
ICM	Identity and Credential Management
LDAP	Lightweight Directory Access Protocol
OAM	Oracle Access Manager

OID	Oracle Internet Directory
OIM	Oracle Identity Management
OS	Operating System
OUD	Oracle Unified Directory
PP	Protection Profile
RDBMS	Relational Database Management System
SMTP	Simple Mail Transfer Protocol
SPML	Service Provisioning Markup Language
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

Table 6-1: Acronyms

Term	Definition
Administrator	The subset of organizational users who have authorizations to manage the TSF.
Entitlement	A privilege assigned to an account on a target system that is configured through provisioning.
Identity Store	The repository in the Operational Environment where organizational users are defined along with their credential data and identity attributes.
Organizational User	A user defined in the identity store that has the ability to interact with assets in the Operational Environment.
Provisioning	The process of configuring the settings and/or account information of environmental assets based on the privileges that different types of organizational users need on them to carry out their organizational responsibilities.
Authorized Administrator	The claimed Protection Profile defines an Authorized Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be any user with the 'admin' role.
Security Administrator	Synonymous with Authorized Administrator.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.

Table 6-2: Terminology