Oracle Identity Governance 12c

Security Target

Version 1.5

October 2024

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
0.1	6 April 2022	Initial draft for client review.
0.2	20 June 2022	Incorporated developer comments. Initial draft for evaluation.
0.3	8 March 2023	Addressed evaluator ORs.
1.0	12 September 2023	Addressed CB ORs.
1.1	16 October 2023	Addressed CB ORs.
1.2	3 June 2024	Removed SPML Interface from scope. Removed FCS_TLS claims. Updated guidance. Addressed evaluator ORs.
1.3	14 August 2024	Addressed CB ORs.
1.4	1 October 2024	Addressed CB ORs.
1.5	3 October 2024	Updated AGD reference version.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Oracle Identity Governance 12c Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 Oracle Identity Governance (OIG) is an Enterprise Security Management (ESM) software application that is used as a method to centralize the management of the roles and privileges of user accounts within an organization. It enforces the association of user attributes with different sets of privileges preventing unauthorized access to resources in the Operational Environment.

3 The TOE allows for administrative configuration of identity and credential information as well as a self-service component so that users can change their own passwords. Administrators are able to provision subjects by enrolling new users into an organizational repository, associates and disassociates users with organizationally-defined attributes, and configures environmental system accounts and privileges based on these associations.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Oracle Identity Governance 12c, Build 12.2.1.4, with patches 36822804, 36770738, 36553894, 1221422, 36805124, and 36513778 **Note**: The TOE name is displayed as “Oracle Identity Self Service” in the UI banner.
Security Target	Oracle Identity Governance 12c Security Target, v1.4

1.3 Conformance Claims

4 This ST supports the following conformance claims:

a) CC version 3.1, Revision 5

i) CC Part 2 extended

ii) CC Part 3 conformant

b) Standard Protection Profile for Enterprise Security Management Identity and Credential Management (PP_ESM_ICM), v2.1

NIAP Technical Decisions per

c) Table 2

Table 2: NIAP Technical Decisions

TD #	Name	Source	Applicability Rationale
0042	Removal of Low-level Crypto Failure Audit from PPs	PP_ESM_ICM	Applicable
0055	Move FTA_TAB.1 to Selection-Based Requirement	PP_ESM_ICM	Applicable
0066	Clarification of FAU_STG_EXT.1 Requirement in ESM PPs	PP_ESM_ICM	Applicable
0079	RBG Cryptographic Transitions per NIST SP 800-131A Revision 1	PP_ESM_ICM	N/A. FCS_RBG_EXT.1 is not claimed.
0573	Update to FCS_COP and FCS_CKM in ESM PPs	PP_ESM_ICM	N/A. FCS_COP and FCS_CKM are not claimed.
0574	Update to FCS_SSH in ESM PPs	PP_ESM_ICM	N/A. FCS_SSH_EXT.1 is not claimed.
0576	FTP_ITC and FTP_TRP Updated	PP_ESM_ICM	Applicable
0621	Corrections to FCS_TLS_EXT.1 in ESM PPs	PP_ESM_ICM	N/A. FCS_TLS_EXT.1 is not claimed.
0794	Correction to FCS_SSH_EXT.1.7 Test 2	PP_ESM_ICM	N/A. FCS_SSH_EXT.1 is not claimed.
0844	Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim	PP_ESM_ICM	N/A. Flaw remediation is not claimed.

1.4 Terminology

Table 3: Terminology

Term	Definition
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
ESM	Enterprise Security Management
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ICF	Identity Connector Framework
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
OAM	Oracle Access Manager
OID	Oracle Identity Directory
OIG	Oracle Identity Governance
OS	Operating System
OSP	Organizational Security Policy
OUD	Oracle Unified Directory
PDF	Portable Document Format
PP	Protection Profile
RDBMS	Relational Database Management System
RFC	Request for Comments
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SPML	Services Provisioning Markup Language
SSH	Secure Shell

Term	Definition
ST	Security Target
TD	Technical Decision
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
UTF	Unicode Transformation Format

2 TOE Description

2.1 Type

5 The TOE is an enterprise identity and credential management solution.

2.2 Usage

6 The TOE, shown in the red boxes below, is deployed to allow administrators to manage user identity and credential information.

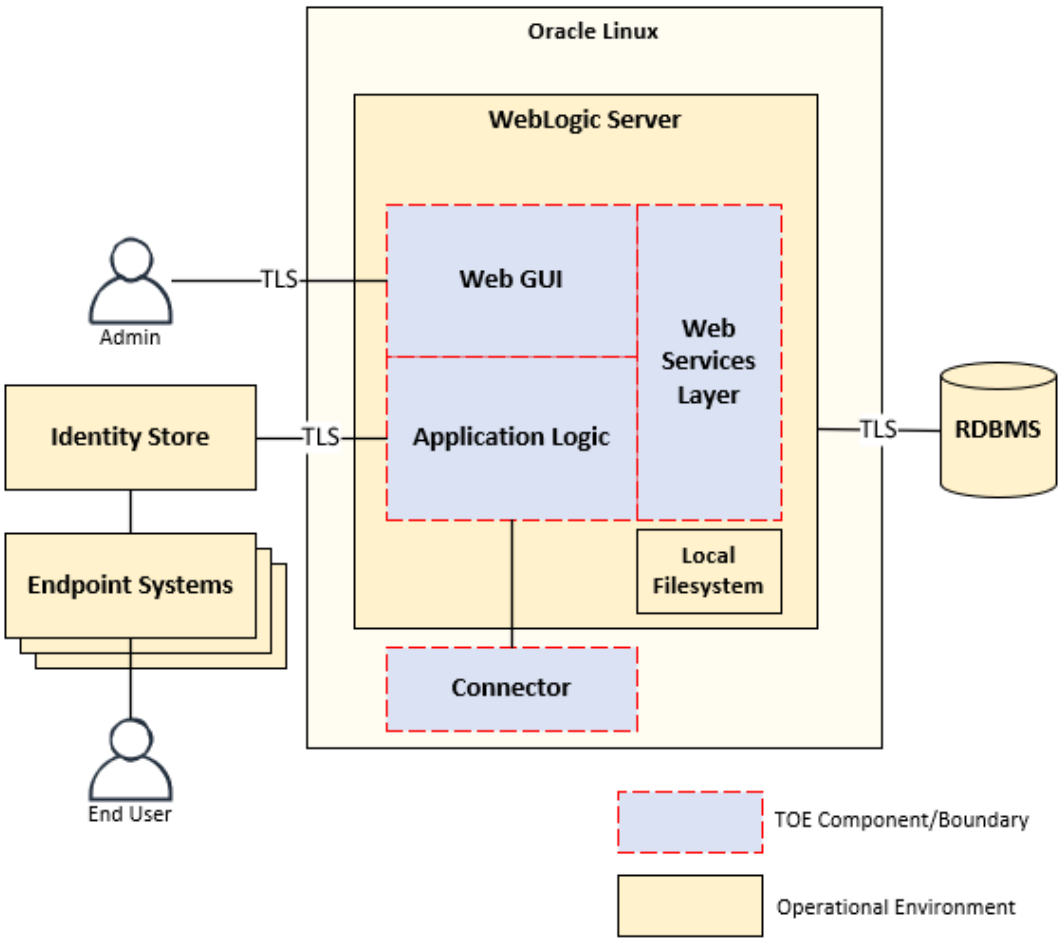

Figure 1: TOE Usage Example

7 To come under identity management, an administrator provisions subjects by enrolling new users into an organizational repository, associates and disassociates users with organizationally-defined attributes, and configures environmental system accounts and privileges based on these associations.

8 Communications with remote administrators and remote data stores (Identity Store, RDBMS) are protected by TLS.

2.3 Logical Scope

2.3.1 Enterprise Security Management

9 The primary functionality of the TOE is to maintain the identity and credential lifecycle for organizational users. The TSF can define and maintain the organizational attributes of users, enroll and unenroll users, and impose controls that ensure that their authentication credentials (passwords) are sufficiently secure. Additionally, the TSF can associate various user attributes with the notion of an “identity” such that environmental systems and applications are configured for different users based on this identity.

10 For example, the TSF can associate a number of different office locations with a region and give users who are located in this region a certain set of permissions. As users enter the organization, leave the organization, or change their location, the change will be detected by the TSF so that the user permissions can be updated automatically. Administrators can also manually assign different attributes to organizational users. All updates to identity and credential data that require the TSF to connect to an external server are secured using TLS.

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

2.3.2 Security Audit

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

2.3.3 Identification and Authentication

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

2.3.4 Security Management

14 The TOE is managed by authorized administrators using a web GUI. Administrative privileges are defined by the TSF using identity data that is defined in the Operational Environment. The TOE can also define workflow steps such that administrative activities can be subjected to an approval process.

15 The TOE provides a set of out-of-the-box administrative roles with fixed privileges to manage different aspects of the TSF. In addition to direct administration, an organizational user can perform self-service by updating their organizational password or updating some of their personal attributes. These users can also initiate requests to be assigned privileges that can be subjected to a workflow approvals process to ensure that users can quickly be given appropriate privileges to perform their organizational responsibilities.

2.3.5 Protection of the TSF

16 The TOE ensures that administrator credentials are hashed before being sent to the Operational Environment. If a user forgets their password and uses the recovery feature to access their account, the password will be reset. Similarly, the answers to user security questions (used for password recovery) are stored in a hashed format. The TOE also protects secret and private key data such that there is no mechanism to disclose this information and compromise the security of trusted communications.

2.3.6 Trusted Path/Channels

17 The TOE allows trusted channels to be established between itself and the remote data stores (Identity Store, RDBMS) that it interfaces with. These trusted channels are secured using TLS. In addition, the TOE establishes a trusted path between authorized administrators and the TSF using HTTPS for the web GUI and REST API. The TLS and HTTPS protocols are implemented by the underlying OS.

2.4 Physical Scope

2.4.1 Software

18 The TOE is the following software:

a) Oracle Identity Governance 12c, Build 12.2.1.4

b) Patches 36822804, 36770738, 36553894, 1221422, 36805124, and 36513778

c) Oracle OID Connector 12.2.1.3.0 with patch 36910321

19 OIG 12c is downloaded by users from the Oracle Identity & Access Management Downloads page at: https://www.oracle.com/security/identity-management/technologies/downloads/.

20 All patches are downloaded by users from the My Oracle Support page at: https://support.oracle.com.

21 The OID Connector is downloaded by users from the Oracle Identity Manager 12c Connectors Downloads page at: https://www.oracle.com/security/identity-management/technologies/oim-connectors-downloads/.

22 **Note**: The OID connector 12.2.1.3.0 may also be referred to as the "ODSEE/OUD/LDAPV3 Connector 12.2.1.3.0" in TOE guidance and GUI pages.

2.4.2 Evaluated Components

23 The physical boundary of the TOE includes the OIG software that is installed on top of the environmental WebLogic application server and the connectors that are used to provision endpoint systems.

24 The following table describes the TOE components in the evaluated configuration:

Note: The TOE must be deployed by Oracle Support to ensure it is in the evaluated configuration.

Table 4: Evaluated Components

Component	Description/Details
Application Logic	A component that runs on the environmental WebLogic server and is responsible for all back-end TSF behavior.
Connectors	Components that translate the TSF's application logic into configuration instructions that can be interpreted by endpoint systems. There are three types of connectors: • Identity Connector Framework (ICF) connectors – ICF is a Java-based framework for decoupling applications from the method used to interact with them. The TOE will provision ICF-compatible systems and applications by transmitting ICF objects instead of invoking APIs and the endpoint will translate the ICF object into its native equivalent. • Legacy connectors – a predecessor to ICF that interfaces with the target application by invoking its native APIs.
Web GUI	A component that runs on the environmental WebLogic server and is responsible for providing a visual administrative interface to the application logic.

2.4.3 Guidance Documents

25 The TOE includes the following guidance documents downloaded in PDF format:

a) [CC Guide] - Oracle Identity Governance 12c Common Criteria Guide, v1.4:

https://www.oracle.com/corporate/security-practices/assurance/development/external-security-evaluations/common-criteria/certifications.html

b) [ADMIN] Oracle Fusion Middleware Administering Oracle Identity Governance, 12c (12.2.1.4.0), E95926-14:

https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omadm/administering-oracle-identity-governance.pdf.

c) [SELF] Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance, 12c (12.2.1.4.0), E95920-08:

https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omusg/performing-self-service-tasks-oracle-identity-governance.pdf.

d) [HELP] Oracle Fusion Middleware Help Topics for Oracle Identity Governance, 12c (12.2.1.4.0), E95917-05:

https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omhlp/help-topics-oracle-identity-governance.pdf.

2.4.4 Non-TOE Components

26 The TOE operates with the following components in the environment.

Table 5: Non-TOE Components

Component	Description/Details
Application Server	WebLogic application server software that is used as a framework to run the OIG application. • Oracle Linux 8.4 UEK 5 • Oracle WebLogic Server 12.2.1.4.0 • jdk 1.8.0_421
Database Server	Physical system on which the RDBMS is installed. • Oracle Database 19c
Endpoint Systems	Systems and their associated applications that end users access to perform their organizational duties.
Provisioned Applications	External applications that consume TSF data: • Identity Store (Oracle Unified Directory / Oracle Internet Directory 12c) • OL7 (interfaces with OUD as an end-user system)
Local Filesystem	System storage on the Server that is used to store some configuration and log data for the Application Server.
Administrator System	Web Browser
User System	Web Browser

27 The minimum system requirements for the components identified in Table 5 can be found online at: https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/sysrs/system-requirements-and-specifications.html#GUID-A077A2B4-5967-42E0-A063-0F7A0A2254FB.

2.5 Excluded Functionality

28 This CC evaluation only covers the functionality identified in section 2.3 when the TOE is configured in accordance with [CC Guide].

29 The following features/components were not evaluated.

2.5.1 Excluded Features/Components

30 **Oracle Access Manager (OAM)** - Authentication/authorization application that governs access to the TOE's administrative interface.

31 **SMTP Server** - Email server used to send notifications and self-service data to administrators and end users.

32 **OIG Design Console** - A local server application that is used to set initial configuration parameters for OIG that are not pertinent to the security functionality of the TOE.

33 **Connectors** – The TOE supports many connectors. Only the OID connector will be evaluated. The list of supported connectors can be found here: https://www.oracle.com/security/identity-management/technologies/oim-connectors-downloads/.

2.5.2 Excluded Interfaces

34 **Connectors** - Some connectors communicate with the Operational Environment by invoking the native SSH implementation of the host OS on which the target application resides. Because the SSH functionality is provided entirely by the OS and is completely independent of OIG, this is not considered to be part of the TSF.

35 **SPML** – The Services Provisioning Markup Language (SPML) Interface may be used to manage the TOE. It is disabled by default and requires configuration prior to use. The SPML Interface was not configured, used or tested in the evaluated configuration.

3 Security Problem Definition

36 The Security Problem Definition is reproduced from the claimed PP.

3.1 Threats

Table 6: Threats

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

3.2 Assumptions

Table 7: Assumptions

Identifier	Description
A.CRYPTO (optional)	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ENROLLMENT	There will be a defined enrollment process that confirms user identity before the assignment of credentials.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.FEDERATE	Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.
A.ROBUST (optional)	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME (optional)	The TOE will receive reliable time data from the Operational Environment.

37 **Note**: The TSF satisfies A.ESM by establishing a secure connection to one or more environmental identity stores that other ESM products may use for administrator identification, authentication, and/or administration. The TOE is not expected to connect directly to other ESM products to share this data; it will be shared with other ESM products through updating a data store that is in the Operational Environment of other ESM products.

3.3 Organizational Security Policies

Table 8: OSPs

Identifier	Description
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

38 **Note**: As per NIAP TD0055, this objective is expected to be satisfied by the OUD component in the TOE's Operational Environment. The TOE relies on this component for authentication, which includes display of the login page that is subsequently redirected to the TOE when authentication is successful.

4 Security Objectives

39 The security objectives are reproduced from the claimed PP.

4.1 Security Objectives for the TOE

Table 9: Security Objectives for the TOE

Identifier	Description
O.ACCESSID	The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.EXPORT	The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.
O.IDENT	The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.
O.INTEGRITY	The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.
O.MANAGE	The TOE will provide Assignment Managers with the capability to manage the TSF.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTCRED	The TOE will be able to protect stored credentials.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.

4.2 Security Objectives for the Operational Environment

Table 10: Security Objectives for the Operational Environment

Identifier	Description
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.CRYPTO (optional)	The Operational Environment will provide cryptographic mechanisms that are used to ensure the confidentiality and integrity of communications.
OE.ENROLLMENT	The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.
OE.FEDERATE	Data the TOE exchanges with trusted external entities is trusted.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.MANAGEMENT	The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.ROBUST (optional)	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME (optional)	The Operational Environment will provide reliable time data to the TOE.

5 Security Requirements

5.1 Conventions

40 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text (for added text) and strikethroughs (for deleted text).

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated with a sequential number in parentheses following the element number of the iterated SFR.

5.2 Extended Components Definition

41 The following Extended Components are defined in Chapter 5 of the ESM_PP_ICM:

Table 11: Extended Components

Requirement	Title
ESM_EAU.2	Reliance on Enterprise Authentication
ESM_EID.2	Reliance on Enterprise Identification
ESM_ICD.1	Identity and Credential Definition
ESM_ICT.1	Identity and Credential Transmission
FAU_STG_EXT.1	External Audit Trail Storage
FPT_APW_EXT.1	Protection of Stored Credentials
FPT_SKP_EXT.1	Protection of Secret Key Parameters

5.3 Functional Requirements

Table 12: Summary of SFRs

Class Name	Component Identification	Component Name
Enterprise Security Management	ESM_EAU.2	Reliance on Enterprise Authentication
	ESM_EID.2	Reliance on Enterprise Identification
	ESM_ICD.1	Identity and Credential Definition
	ESM_ICT.1	Identity and Credential Transmission
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_STG_EXT.1	External Audit Trail Storage
Identification and Authentication	FIA_USB.1	User-Subject Binding
Security Management	FMT_MOF.1	Management of Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_APW_EXT.1	Protection of Stored Credentials
	FPT_SKP_EXT.1	Protection of Secret Key Parameters
Trusted Path /Channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

5.3.1 Class ESM: Enterprise Security Management

ESM_EAU.2 Reliance on Enterprise Authentication

ESM_EAU.2.1 The TSF shall rely on [[*the Identity store in the Operational Environment*]] for subject authentication.

ESM_EAU.2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject

ESM_EID.2 Reliance on Enterprise Identification

ESM_EID.2.1 The TSF shall rely on [[*the Identity store in the Operational Environment*]] for subject identification.

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

ESM_ICD.1 Identity and Credential Definition

ESM_ICD.1.1 The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2 The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, [*required authentication level, administrator-defined attributes, security questions and answers*].

ESM_ICD.1.3 The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4 The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5 The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

Application Note: There is currently no published Protection Profile for ESM Authentication Server. However, the evaluated configuration includes several common authentication server products in the Operational Environment that could be used to update enterprise user credential data if desired.

ESM_ICD.1.8 The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

a) For password-based credentials, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: [*UTF-8*] that include the following values [*U+0021 (!) through U+007E (~)*]; and

Application Note: This character set includes 93 unique characters.

2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

ESM_ICT.1 Identity and Credential Transmission

ESM_ICT.1.1 The TSF shall transmit [identity and credential data] to compatible and authorized Enterprise Security Management products under the following circumstances: [immediately following creation or modification of data, at a periodic interval].

5.3.2 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions; and

b) All auditable events identified in Table 13 for the [not specified] level of audit; and

c) [*no other auditable events*].

Application Note: Auditing for FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1) through FCS_COP.1(4), and FCS_RBG_EXT.1 has been omitted from the list of auditable events because they are not required as per NIAP TD0042.

Table 13: Auditable Events

Component	Event	Additional Information
ESM_EAU.2	All use of the authentication mechanism	None
ESM_ICD.1	Creation or modification of identity and credential data	The attribute(s) modified
ESM_ICD.1	Enrolment or modification of subject	The subject created or modified, the attribute(s) modified (if applicable)
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed

Component	Event	Additional Information
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*additional information in Table 13*].

FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [*remote RDBMS, local filesystem*].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

Application Note: There is no TOE-internal storage of audit data.

5.3.3 Class FIA: Identification and Authentication

FIA_USB.1 User-Subject Binding

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

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*user is associated with their assigned role(s) when authenticated to the TSF*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*the user's administrative role is checked each time an action requiring authorization is performed*].

5.3.4 Class FMT: Security Management

FMT_MOF.1 Management of Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions: [*management activity specified in* Table 14] to [*authorized roles for each function specified in Table 14*].

Table 14: Management Activities

Management Activity	OIG Permission(s)	Authorized Role(s)
Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	Create Application Instance Modify Application Instance Delete Application Instance	Application Instance Administrator
	Grant/Revoke Account Modify Account	Application Instance Authorizer
	Enable/Disable Account	User Administrator
	Grant/Revoke Account Modify Account	Application Instance Viewer
	Enable/Disable Account	User Viewer
	Add Entitlements Delete Entitlements Update Entitlements	Entitlement Administrator
	Grant/Revoke Entitlement	Entitlement Authorizer
	Grant/Revoke Entitlement	Entitlement Viewer
	Create Role Modify Role Delete Role Manage Role Membership Rules	Role Administrator
	Grant/Revoke Role	Role Authorizer
	Grant/Revoke Role	Role Viewer

Management Activity	OIG Permission(s)	Authorized Role(s)
	Create Application Instance Modify Application Instance Delete Application Instance Add Attributes Modify Attributes Delete Attributes Create Password Policy Modify Password Policy Delete Password Policy	System Configurator
	Lock/Unlock User Change User Password Change Account Passwords Grant/Revoke Entitlements Grant/Revoke Accounts Grant/Revoke Role	User Administrator
Management of credential status	Create Password Policy Modify Password Policy Delete Password Policy	System Configurator
	Associate Password Policy	Organization Administrator
Enrollment of users into repository	Create/Delete User	User Administrator
Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	Reconciliation	System Administrator
Configuration of external audit storage location	Modify System Properties	System Configurator
Management of the threshold for unsuccessful authentication attempts	Modify System Properties	System Configurator
Management of actions to be taken in the event of an authentication failure	Unlock User	User Administrator
	Unlock User (only if locked out due to failed logins)	Help Desk
Definition of default subject security attributes, modification of subject security attributes	Add/Delete Admin Roles	AdminRole Administrator

Management Activity	OIG Permission(s)	Authorized Role(s)
Management of sets of users that can interact with security functions	Create Approval Policies Modify Approval Policies Delete Approval Policies	System Configurator
	Modify Admin Role Membership	AdminRole Administrator
Management of the users that belong to a particular role	Modify Admin Role Membership	AdminRole Administrator
Management of their own identity attributes	Request account entitlements Request changes to identity attributes Request changes to role Modify own password Modify own security questions and answers	Self-Service (implicit)

42 Application Note: The Add / Delete / Update Entitlements functions are only permitted when a disconnected application instance is used. An online application is used in the evaluated configuration.

FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, [*request*]] the [*identity data, account entitlements, user role, password, security questions/answers*] to [*users assigned the authorized role as defined in Table 14*].

FMT_SMF.1 Security Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*management functions listed in Table 15*].

Table 15: Management Functions by SFR

Requirement	Management Activities
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)
ESM_ICD.1	Management of credential status
ESM_ICD.1	Enrollment of users into repository

Requirement	Management Activities
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed
FAU_STG_EXT.1	Configuration of external audit storage location
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF.1	Management of sets of users that can interact with security functions
FMT_SMR.1	Management of the users that belong to a particular role
FTP_ICT.1	Configuration of actions that require trusted channel (if applicable)
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)

FMT_SMR.1 Security Management Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*Application Instance Administrator, Application Instance Authorizer, Application Instance Viewer, Entitlement Administrator, Entitlement Authorizer, Entitlement Viewer, Role Administrator, Role Authorizer, Role Viewer, System Administrator, System Configurator, Organization Administrator User Administrator, AdminRole Administrator, User Viewer, Help Desk, Self-Service (Implicit)*].

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

5.3.5 Class FPT: Protection of the TSF

FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

FPT_SKP_EXT.1 Protection of Secret Key Parameters

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.3.6 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1	The TSF shall be capable of using [TLS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [[*Identity Store, RDBMS, Connectors*]] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
FTP_ITC.1.2	The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for transfer of policy data, [*transfer of authentication data, transfer of audit data, provisioning of user privileges*].
Application Note:	This SFR is altered by TD0576.

FTP_TRP.1 Trusted Path

FTP_TRP.1	The TSF shall be capable of using [HTTPS] to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identifications of its end points and protection of the communicated data from modification, disclosure, and [no other types of integrity or confidentiality violations].
FTP_TRP.1.2	The TSF shall permit remote users to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for initial user authentication and execution of management functions.
Application Note:	This SFR is altered by TD0576.

5.4 Assurance Requirements

5.4.1 Summary of Requirements

43 The TOE security assurance requirements are summarized in Table 16.

Table 16: Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security Objectives for the Operational Environment
	ASE_REQ.1	Stated Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

6 TOE Summary Specification

44 The following describes how the TOE fulfils each SFR included in section 5.3.

6.1 Enterprise Security Management

6.1.1 ESM_EAU.2 & ESM_EID.2

45 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 store (OID, or OUD) using LDAP. The TSF receives the result of this request and abides by that result. This same authentication method is used for user self-service.

46 In order to perform self-service, a user may authenticate to the TOE by providing valid authentication credentials as defined by the environmental identity store in the same way that administrators authenticate to the TOE. There are two exceptions to this:

47 If the user is performing self-service to request a forgotten username, the user must identify themselves by providing the email address associated with their username. The username is then sent to that email, where it is assumed the user will have to authenticate in order to view that data.

48 If the user is performing self-service to reset a forgotten password, the user must identify themselves by providing their username. The user is then prompted to answer challenge questions and is only allowed to reset their password if they correctly answer these questions.

49 In other words, security questions can also be used as an enterprise authentication mechanism for end user self-service password management in the event of a forgotten or expired password. In this instance, the identification mechanism is the end user's email address.

6.1.2 ESM_ICD.1

50 The TOE is responsible for configuring and maintaining identity and credential attributes for organizational users. These attributes define a users' place within the organization. Computing resources in the Operational Environment can be configured based on these attributes. In the evaluated configuration, the TOE can be used with OID, or OUD as the Identity Store. The TSF can then be used to manipulate the values in one of these user stores and supplement it with data it introduces to the Operational Environment via the RDBMS.

51 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. Basic identity attributes are provided out-of-the-box by the TSF.
- **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. The TSF can be used to define arbitrary extended attributes of the administrator's choosing.

- **Credential data**: hashes of user passwords.

52 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.

53 While this data is defined by the TSF and maintained in the RDBMS, it is also transmitted to the Identity Store so that it can be used by the Operational Environment.

54 The TSF is also capable of configuring specific external applications based on user identity data (provisioning) through the use of connectors that interface directly with the applications. This provides the ability for administrators to update the configuration of organizational assets in real time as users join the organization, leave the organization, or assume different roles or other characteristics that affect their privileges. The following applications or entities can be provisioned with connectors:

- AS400
- BMC Remedy
- CA
  - ACF2
  - Top Secret
- Database (MS SQL, Oracle, MySQL, DB2, Sybase, generic JDBC database)
  - Application Tables
  - User Management
- Generic
  - Flat File
  - Web Services
- Google Apps
- IBM
  - Lotus Notes/Domino

    - OS/400
    - RACF
- JD Edwards EnterpriseOne
- Microsoft
    - Exchange
    - Windows
- Novell
    - eDirectory
    - GroupWise
- Oracle
    - OAM
    - OUD
    - CRM On Demand
    - E-Business
    - Internet Directory
    - Retail Warehouse Management System
- PeopleSoft
    - Campus
    - Employee Reconciliation
    - User Management
- RSA
    - Authentication Manager
    - ClearTrust
- SAP
    - Employee Reconciliation
    - User Management
    - User Management Engine
- Siebel User Management
- Sun Java System Directory
- Linux/UNIX

55 **Note**: The evaluated configuration only includes the OUD connector.

56 When a new user joins the organization, the TOE can enroll them manually. The user can also be enrolled through the organization's existing systems and the TSF will detect the new entry in the organizational identity store. From there, the TOE can be used to check and manage the user's attributes, including manually expiring a user's password or suspending or disabling a user's account entirely. The TOE can also be used to define policy-based conditions that will cause a user account to automatically be disabled or deleted if these conditions occur.

57 In the evaluated configuration, the organizational identity store is an OID, or OUD LDAP store that is capable of authenticating its users. Additionally, since the TOE consumes the user data directly from this store, any change to user data that is performed by some other organizational system can be interpreted by the TSF. The TOE does not have to be the sole mechanism that is used to manage this data.

58 The TSF is capable of enforcing composition rules for strong user passwords via configuration of the following password policy elements:

- Minimum Length
- Number of Past Passwords to Disallow
- Minimum Age
- Maximum Age
- Maximum Length
- Maximum Repeated Characters
- Minimum Numeric Characters
- Minimum Alphanumeric Characters
- Minimum Alphabet Characters
- Minimum Unique Characters
- Minimum Uppercase Characters
- Minimum Lowercase Characters
- Minimum Number of Special Characters (e.g. !, $, #, ^)

59 Additional password policy options are provided by the product but they are out of scope of the claimed Protection Profile so they are not discussed as part of the TSF.

6.1.3 ESM_ICT.1

60 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. This ensures that it is possible for other entities in the Operational Environment to have the ability to update data in the Identity Store if needed. By default, the synchronization period is 5 minutes.

61 Similarly, when a connector is configured in such a manner that will cause user privileges to be updated, the TSF initiates the provisioning operation as soon as the update is made.

6.2 Security Audit

6.2.1 FAU_GEN.1

62 The TSF generates audit records when auditable events occur. The auditable events that are logged are described in Table 13. The auditable event types can be summarized as follows:

- Administrator login/logout
- Product configuration changes
- Startup/shutdown of product
- Establishment/disestablishment of cryptographic channels
- Failure to perform cryptographic operations

63 For each auditable event, the date, time, type, subject identity, and outcome of the event is logged.

6.2.2 FAU_STG_EXT.1

64 Audit data that is generated by the TOE is stored in the local file system of the OS on which the application server is run and in the environmental RDBMS. Server activities such as startup and shutdown of the TOE, cryptographic operations, and web server page loads are stored in the underlying OS' local file system. Logs for application-level administration of the TSF is stored in the RDBMS.

65 No audit data is stored directly within the TOE boundary so the Operational Environment is expected to protect the stored audit data.

6.3 Identification and Authentication

6.3.1 FIA_USB.1

66 The ability to manage the TSF is based on role. When administrators authenticate to the TOE, a session cookie is created by the web server and the administrator's session is established. The administrator's role is defined in the RDBMS and associated with the other identity information for that administrator by the TSF. Every time an administrator submits a request to the server via the web GUI, that request is checked on the back end by the server. The administrator's subject identity is therefore not explicitly associated with the administrator's web session so any change in their permissions while they are authenticated will take immediate effect.

6.4 Security Management

6.4.1 FMT_MOF.1

67 The TOE provides the ability to manage its functions to authorized administrators using a web GUI. An administrator will authenticate to the TOE by providing their organizational user credentials and the TOE will interface with the environmental identity store to determine if the credentials are valid. The TOE will then confirm that the administrator's account has not been locked or disabled and will allow the administrator access to the TSF based on their defined role.

68 Table 14 provides a static list of non-hierarchical roles defined by the TSF that each have a fixed set of authorizations to manage the TOE's functions. The management functions that are defined for the TSF are mapped to the corresponding

authorizations that are defined within OIG itself as well as the roles that are given those authorizations. Note that if a role has the permission to interact with a function or object as described by Table 14, the role also has the permission to “determine the behavior of” (i.e. view) that function or object. Also note that the Application Instance Viewer, Entitlement Viewer, Help Desk, Role Viewer, and User Viewer roles can only perform these management functions by approving the corresponding user self-service requests; they cannot actually initiate the functions directly.

69 In addition to these roles, there is a System Administrator role that has full permissions to manage the TSF. Finally, the TSF implicitly defines an unprivileged user role that only has the authority to perform self-service activities.

6.4.2 FMT_MTD.1

70 In order to minimize the use of administrative resources to maintain organizational user data, the TOE provides the ability for enterprise users to perform self-service for their accounts. This is distinct from administration of the TOE because the user is interacting solely with TSF data rather than managing its functionality. However, the repository (Identity Store) and means of establishing trusted communications (TLS) is the same for both end user data and administrator data. When a user has authenticated to the TOE via the Identity Self Service page of the web GUI, they are given the opportunity to interact with the following data in the following ways:

- Identity data – users are allowed to modify basic identity attributes that may change over the course of their tenure with the organization such as last name or address.
- Accounts and entitlements – users are allowed to view the accounts that they have been assigned on systems or applications in the Operational Environment and may initiate a request to be given additional entitlements.
- User role – users are allowed to view their role information and request new role assignments if their responsibilities within the organization have changed.
- Password – users are allowed to change their password if its age exceeds the minimum age and they are required to change their password if its age exceeds the maximum age.
- Security questions/answers – users are allowed to change the security questions and corresponding answers that are used to validate the user’s identity in the event of a forgotten password.

71 When a user initiates a request for additional authorizations, an administrator in an Application Instance Viewer, Entitlement Viewer, Help Desk, Role Viewer, or User Viewer role is responsible for reviewing the justification provided for the request and ultimately making the change if they determine it should be approved. Policies determining the types of requests that different administrator roles are authorized to approve are managed by the System Configurator role.

6.4.3 FMT_SMF.1

72 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. Table 15 defines the set of management activities that are prescribed by the claimed PP. Note that each of these functions are performed using the OIG web GUI with the exception of configuration of provision objects, which is considered to be part of managing ESM_ICT.1 because it

determines in part when and how identity/credential data is transmitted to the Operational Environment

6.4.4 FMT_SMR.1

73 The TOE defines a number of administrative roles, each of which is given a fixed set of permissions to interact with the TSF. Administrators can be assigned to one or more roles in order to manage the functions and data that are associated with these permissions. Table 17 below lists the administrative roles that can be used to perform management activities that are within the scope of the TSF. Other roles are provided by OIG but their use is limited to functions that are not defined as part of the claimed Protection Profile, so they are not considered to be part of the TSF.

74 For most types of identity data, there are three different types of administrative roles that can interact with that data, as follows:

- Administrator – An administrator of the data type is able to define instances of that data.
- Authorizer – An authorizer of the data type is able to associate instances of that data with users.
- Viewer – A viewer of the data type is able to approve user self-service requests to be associated with an instance of that data.

Table 17: Administrative Roles & Privileges

Administrator Role	Privileges
Application Instance Administrator	Has the ability to create, modify, and delete application instances, which consist of accounts used to access resources in the Operational Environment.
Application Instance Authorizor	Has the ability to associate organizational users with environmental accounts via application instances.
Application Instance Viewer	Has the ability to approve self-service requests initiated by users to have their environmental account associations updated.
Entitlement Administrator	Has the ability to create, modify, and delete entitlements.
Entitlement Authorizor	Has the ability to associate organizational users with environmental entitlements.
Entitlement Viewer	Has the ability to approve self-service requests initiated by users to have their environmental entitlements updated.
Help Desk	Can manage user passwords, enable or disable users, and unlock the user if they have been locked out due to an excessive number of failed authentication attempts.

Administrator Role	Privileges
Organization Administrator	Can manage organizations and specify additional ones if the environment's organizational structure dictates it. Can also associate password policies with organizations to enforce on those organizational users.
Role Administrator	Can manage enterprise roles as well as identity conditions that determine their membership.
Role Authorizor	Can modify the enterprise role identity attribute by granting roles to and revoking rules from users.
Role Viewer	Has the ability to approve self-service requests initiated by users to have their role information updated.
Self-Service (implicit)	Can manage a subset of their own identity attributes, change their password, and request changes to their identity attributes, user role, accounts, or entitlements.
System Administrator	Has full privileges to manage all aspects of the TSF.
System Configurator	Has the ability to define and modify extended identity attributes, password policies, and general TSF system performance attributes such as lockout settings. Also can define policies governing the approval requests that can be granted by various roles.
User Administrator	Has the ability to create, delete, and manage users, including their identity attributes, user role, accounts, or entitlements, as well as whether the user is enabled at an organizational level.
User Viewer	Has the ability to approve self-service requests to change their identity attributes, user role, accounts, or entitlements.
AdminRole Administrator	Has the ability to create, delete, and modify Admin Roles, as well as modify Admin Role memberships.

75 An administrator role is distinct from an enterprise user role. An enterprise user role is an arbitrarily-defined role that represents a position within the organization such as "Finance Department" or "Northeast Region". Administrators can define Access Policies that associate these roles with account and/or configuration information on environmental assets. As users are assigned to different roles, the TOE automatically provisions these assets through the use of connectors. This process ensures that users are given an appropriate set of authorizations to fulfill their organizational responsibilities.

6.5 Protection of the TSF

6.5.1 FPT_APW_EXT.1

76 Password data and security questions/answers for organizational users are stored in the Identity Store and RDBMS in the Operational Environment. When password data is provided to the TSF by an administrator attempting to authenticate or a user requesting to change their password, the data is converted to a non-plaintext form prior to transmission to the Operational Environment. The password is hashed before being transmitted to the Identity Store and is also stored in reversible encryption in the RDBMS. The encryption key for this resides in a key store stored on the server's local file system as part of the environmental WebLogic server. This key store is protected with a password that is located in the WebLogic Credential Store Framework. Additionally, historical passwords are maintained as hashes in the RDBMS in order to prevent password reuse if this is governed by a password policy.

6.5.2 FPT_SKP_EXT.1

77 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 environmental 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.

6.6 Trusted Path/Channels

6.6.1 FTP_ITC.1

78 The TOE uses a third-party cryptographic module in the OE to implement trusted channels with remote data stores (Identity Store, RDBMS) using TLS.

6.6.2 FTP_TRP.1

79 The TOE uses a third-party cryptographic module in the OE to implement a trusted path between administrators and the OIG web GUI and REST API interfaces using TLS.

7 Rationale

7.1 Conformance Claim Rationale

80 The following rationale is presented with regard to the PP conformance claims:

a) **TOE Type.** As identified in section 2.1, the TOE is an enterprise identity and credential management solution consistent with the claimed PP.

b) **Security Problem Definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the claimed PP.

c) **Security Objectives.** As shown in section 4, the security objectives are reproduced directly from the claimed PP.

d) **Security Requirements.** As shown in section 5, the security requirements are reproduced directly from the claimed PP. No additional requirements have been specified.

7.2 Security Objectives Rationale

81 All security objectives are drawn directly from the claimed PPs which present the security objectives rationale.

7.3 Security Requirements Rationale

82 All security requirements are drawn directly from the claimed PPs which present the security requirements rationale.