Oracle Identity Manager

Version 11g Release 2

Common Criteria Evaluation Security Target

ST Version: 1.0
July 29, 2015

Oracle Corporation
100 Oracle Parkway
Redwood City, CA 94065

Prepared By:

Booz | Allen | Hamilton

delivering results that endure

Cyber Assurance Testing Laboratory
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation. This ST targets exact conformance with the following Protection Profile (PP):

- Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1

1.1.1 ST Identification

ST Title: Oracle Identity Manager Security Target
ST Version: 1.0
ST Publication Date: July 29, 2015
ST Author: Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this document provides identifying information for the ST and TOE as well as a brief description of the TOE and its associated TOE type.

Chapter 2 describes the TOE in terms of its physical boundary, logical boundary, exclusions, and dependent Operational Environment components.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the threats, assumptions, objectives, and organizational security policies that apply to the TOE.

Chapter 5 defines extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 6 describes the SFRs that are to be implemented by the TSF.

Chapter 7 describes the SARs that will be used to evaluate the TOE.

Chapter 8 provides the TOE Summary Specification, which describes how the SFRs that are defined for the TOE are implemented by the TSF.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1-1 and 1-2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

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.
Self-Service	The process by which an end user can initiate a password reset or a request for elevated privileges.
User	In an OIM context, is synonymous with organizational user.

Table 1-1: Customer Specific Terminology

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

Table 1-2: CC Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-3. This table is to be used by the reader as a quick reference guide for acronym definitions.

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 1-3: Acronym Definition

1.1.5 References

[1] Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 (ICM PP)

[2] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003

[5] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004

[6] NIST Special Publication 800-56B Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009

[7] NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation, December 2001

[8] NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012

[9] FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001

[10] FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008

[11] Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008

[12] Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)

[13] Oracle Fusion Middleware Administering Oracle Identity Manager 11g Release 2 (11.1.2.3.0)

[14] Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager 11g Release 2 (11.1.2.3.0)

[15] Enterprise Deployment Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)
[16] Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite 11g Release 2 (11.1.2.3.0)
[17] Fusion Middleware Developer's Guide for Oracle Identity Manager 11g Release 2 (11.1.2)
[18] Oracle Fusion Middleware Administrator's Guide 11g Release 2 (11.1.2.3)
[19] Oracle Identity Manager Identity Connectors Documentation

1.2 TOE Reference

The TOE is Oracle Identity Manager (OIM) 11g Release 2.

1.3 TOE Overview

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

The TOE:

- 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.
- Allows for administrative configuration of identity and credential information as well as user-initiated self-service.
- Issues and maintain credentials associated with user identities.
- Publishes and changes credential status (such as active, suspended, or terminated).
- Establishes appropriate trusted channels between itself and the repositories it reads from and writes to.
- Generates an audit trail of configuration changes and subject identification and authentication activities.
- Writes audit trail data to a trusted repository.
- Securely transmits identity and credential attribute data via a trusted channel.

The following figure depicts the TOE boundary:

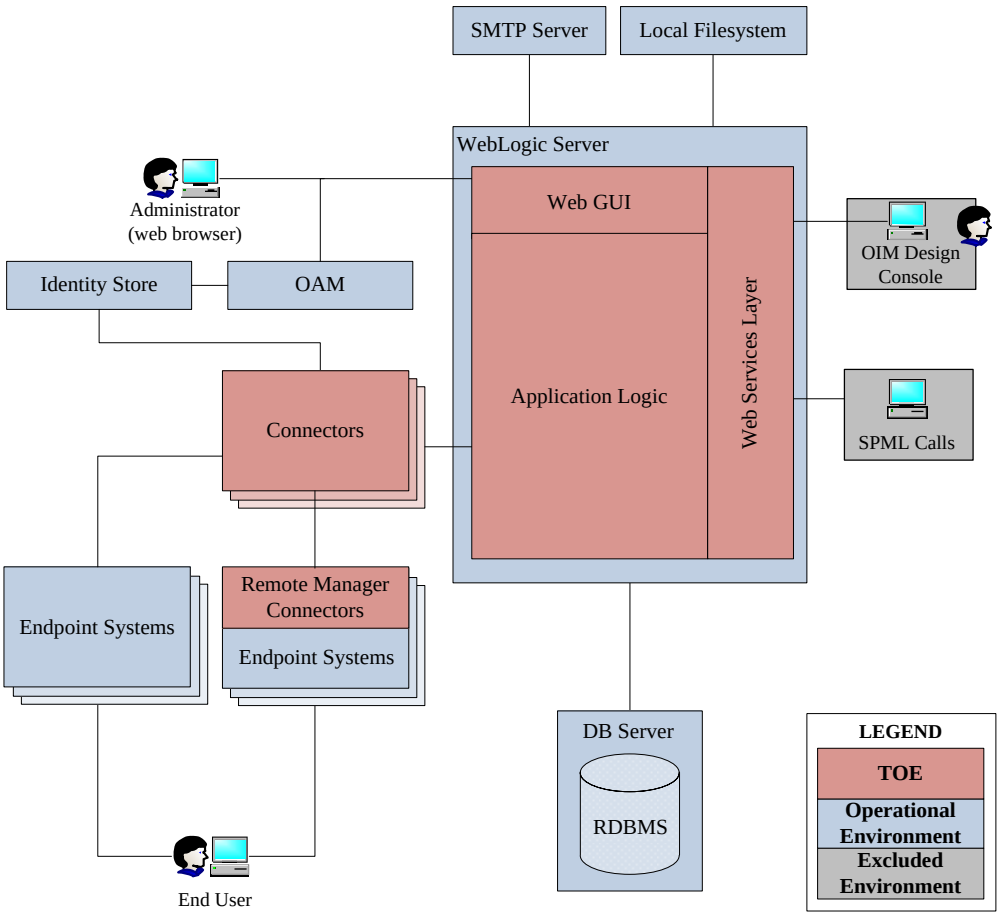

Figure 1-1: TOE Boundary

As illustrated in Figure 1-1, the TOE is comprised of two major components: a WebLogic server application that handles all of the administration and application logic, and one or more connectors that communicate with endpoint systems in the Operational Environment to make configuration changes based on identity associations that are processed by the server. Some applications on endpoint systems cannot be updated through a remote interface. For these applications, a remote manager connector will reside on the system in order to receive instructions remotely and translate them into the proper local operations.

The WebLogic server is not part of the TOE because the TOE has a prerequisite requirement for a Java Application Server to be present in the Operational Environment prior to installation. The product could alternatively be installed on WebSphere but that is not claimed as part of this evaluation.

The TOE is managed directly through a web browser. The TSF also provides an SPML interface but it has been excluded from the evaluated configuration because the exact same server-side methods are invoked for this interface compared to the Web GUI.

The TOE is intended to be deployed in an environment where an LDAP server (such as Active Directory) already exists and is used to maintain data about the organizational users. This LDAP store (referred to as the Identity Store) will also be used to authenticate administrators of the TOE. Oracle Access Manager (OAM) is an access control product offered by Oracle that is often deployed alongside OIM. This

component can be used to determine if administrator requests to access the TSF should be granted. The external RDBMS contains configuration data for the management GUI such as the definition of administrative roles and privileges as well as workflow approval processes. It also contains data that can be used by the TOE's application logic such as associating data from multiple LDAP attributes with a single type of identity and serves as the remote storage repository for TSF audit data. The Identity Store is managed using the same connector interface that is used to provision applications on endpoint systems. The local file system of the server on which the TOE resides is used to store various configuration and log files. The Operational Environment is also expected to have an SMTP server so that it can communicate password resets and workflow notifications to the appropriate administrators or users.

Finally, the Operational Environment is expected to contain endpoint systems that are used by end users to perform various organizational functions. The TOE defines identities for these end users and configures the endpoint systems in a way that gives these end users least privileges to perform their organizational responsibilities.

The following figure, taken from the ICM PP, shows the reference architecture for an identity and credential management product:

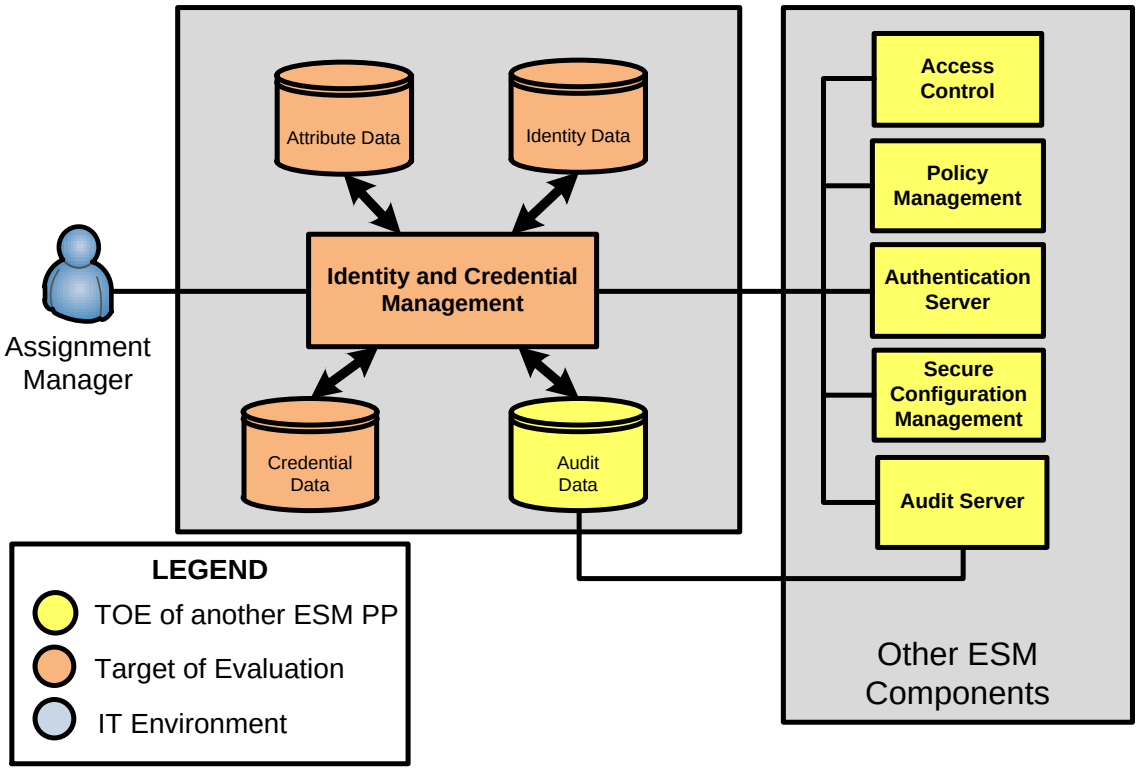

Figure 1-2: ESM PP context for the TOE

In general, the following correspondence can be seen between Figure 1-2 above and the TOE diagram shown in Figure 1-1

- Identity and Credential Management – the TOE
- Attribute Data, Credential Data, Identity Data – RDBMS and LDAP store
- Audit Data – local file system and RDBMS

- Other ESM Components – endpoint systems

Figure 1-2 was derived from the conceptual diagram presented in the ICM PP with some minor differences. These differences do not impact the ability of the TOE to claim exact conformance with the ICM PP. They are as follows:

- The TOE does not interface with an ESM Audit Server, ESM Authentication Server, or ESM Secure Configuration Management product since these Protection Profiles have not been published as of the publication of this ST.
- In the evaluated configuration, the TOE is expected to interface with existing organizational data stores rather than introducing its own so these are part of the Operational Environment and not the TSF.
- The environmental components that the TSF is expected to provision are general organizational assets and not explicitly ESM products. For example, the TSF can assign an individual a certain set of privileges on an operating system or manage some attributes of the individual that are defined in an organizational data store. However, if another ESM product uses data from this organizational data store to enforce its own TSF (e.g. another product derives its administrator login and privileges from Active Directory attributes), the TSF may implicitly manage the behavior of this product by managing the organizational user attributes that govern its behavior.

1.4 TOE Type

The TOE type for OIM is Enterprise Security Management, and more specifically identity and credential management. The TOE is a software application that is used to associate an organization's computer system users with role and privilege information based on their position within the organization. This concept of correlating the attributes of an individual with permissions assigned to their account(s) on IT resources can be understood as identity management. Additionally, the TSF provides measures to govern a user's authentication credential (password), including the ability to change this credential and the ability to effectively revoke it by changing the status of the associated account. These capabilities can collectively be understood as identity and credential management. This facilitates Enterprise Security Management by providing more effective and centralized control over what kinds of users have what access to what kinds of resources within the organization.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

2.1 Evaluated Components of the TOE

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

Component	Definition
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. • Remote manager connectors – a specific type of legacy connector that must reside on the endpoint system and execute instructions directly on that system because no API exists to interface with it remotely.
Web GUI	A component that runs on the environmental WebLogic server and is responsible for providing a visual administrative interface to the application logic.

Table 2-1: Evaluated Components of the TOE

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

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

Server	Physical system on which the OIM software is installed. Contains local file system, SMTP server, and application server.
SMTP Server	Email server used to send notifications and self-service data to administrators and end users.

Table 2-2: Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

There are no optional components that are omitted from the installation process.

2.3.2 Installed but Requires a Separate License

No components are installed that require a separate license.

2.3.3 Installed But Not Part of the TSF

This section contains functionality or components that are part of the purchased product but are not part of the TSF relevant functionality that is being evaluated as the TOE.

- SPML interface – OIM can be administered via SPML calls that are invoked by a web application other than the Web GUI. This is not in the evaluated configuration because the SPML calls interface with the exact same server-side methods that the Web GUI uses so it is redundant functionality.

2.4 Physical Boundary

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

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

Table 2-3: Operational Environment System Requirements

2.5 Logical Boundary

The TSF is comprised of several security features. Each of the security features identified above belongs to one of several general categories, as identified below.

1. Enterprise Security Management
2. Security Audit
3. Cryptographic Support
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

2.5.1 Enterprise Security Management

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

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

2.5.2 Security Audit

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

2.5.3 Cryptographic Support

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

2.5.4 Identification and Authentication

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

2.5.5 Security Management

The TOE is managed by authorized administrators using a web GUI. Administrative privileges are defined by the TSF using identity data that is defined in the Operational Environment. The TOE can also define workflow steps such that administrative activities can be subjected to an approval process. The TOE provides a set of out-of-the-box administrative roles with fixed privileges to manage different aspects of the TSF. In addition to direct administration, an organizational user can perform self-service by updating their organizational password or updating some of their personal attributes. These users can also initiate requests to be assigned privileges that can be subjected to a workflow approvals process to ensure that users can quickly be given appropriate privileges to perform their organizational responsibilities.

2.5.6 Protection of the TSF

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

2.5.7 Trusted Path/Channels

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

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 September 2012.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended to include all applicable NIAP and International interpretations through 30 July 2015.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is conformant to Part 3 to include all applicable NIAP and International interpretations through 30 July 2015.

Note that this evaluation also includes evaluation assurance activities that are defined in the claimed Protection Profile that has augmented the CEM and are not considered to be alterations to Part 3.

3.4 PP Claims

This ST claims exact compliance to the following Protection Profile:

- Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1 [ICM PP]

3.5 Package Claims

The TOE claims exact compliance to a Protection Profile that is conformant with CC Part 3. The TOE claims following "architectural variations" SFRs that are defined in the appendices of the claimed PP:

- FCS_CKM.1
- FCS_CKM_EXT.4
- FCS_COP.1(1)
- FCS_COP.1(2)
- FCS_COP.1(3)
- FCS_COP.1(4)
- FCS_HTTPS_EXT.1
- FCS_RBG_EXT.1
- FCS_TLS_EXT.1
- FMT_MTD.1

This does not violate the notion of exact compliance because the PP specifically indicates these as allowable options and provides both the ST author and evaluation laboratory with instructions on how these claims are to be documented and evaluated.

3.6 Package Name Conformant or Package Name Augmented

This ST claims exact compliance to a Protection Profile. The ST is conformant to the claimed package.

3.7 Conformance Claim Rationale

The ICM PP states the following: "This protection profile focuses on the aspect of ESM that is responsible for enforcing identity and credential management. Identity and Credential Management products will generate and issue credentials for subjects that reside within the enterprise. They will also maintain the organizational attributes that are associated with these subjects. By providing a means for subjects to validate their identities and determining the relationship these subjects have to the enterprise, an Identity and Credential Management product is able to support enterprise accountability and access control."

The TOE is a software application that allows for the centralized enrollment of users which includes the issuing and maintenance of credentials, association of user accounts with identity attributes, and definition of privileges based on these associated attributes. As such, it is consistent with the definition of an identity and credential management product as stated in the ICM PP. Therefore, the conformance claim is appropriate.

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE. These threats have been taken from the ICM PP.

Threat	Threat Definition
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.

Table 4-1: TOE Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the ICM PP. Note as per NIAP TD0055, this objective is expected to be satisfied by the OAM component in the TOE's Operational Environment because 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.

Policy	Policy Definition
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.

Table 4-2: TOE Organization Security Policies

4.3 Assumptions

The specific conditions listed in this section are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the ICM PP.

Assumption	Assumption Definition
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.SYSTIME	The TOE will receive reliable time data from the Operational Environment.

Table 4-3: TOE Assumptions

Note that 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.

4.4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.4.1 TOE Security Objectives

This section identifies the security objectives of the TOE. These objectives have been taken from the ICM PP. A subset of the optional security objectives has been included based on the set of optional SFRs that are claimed by the TSF.

Objective	Objective Definition
O.ACCESSID	The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.CRYPTO	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
O.EXPORT	The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.
O.IDENT	The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.

O.INTEGRITY	The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.
O.MANAGE	The TOE will provide Assignment Managers with the capability to manage the TSF.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTCRED	The TOE will be able to protect stored credentials.
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.

Table 4-4: TOE Objectives

4.4.2 Security Objectives for the Operational Environment

This section identifies the security objectives of the environment into which the TOE is expected to be deployed. These objectives have been taken from the ICM PP. A subset of the optional environmental objectives has been included based on the set of optional SFRs that are not claimed by the TSF.

Objective	Objective Definition
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.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.SYSTIME (optional)	The Operational Environment will provide reliable time data to the TOE.

Table 4-5: Operational Environment Objectives

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives that are defined in this ST represent the assumptions, threats, OSPs, and objectives that are specified in the Protection Profile to which the TOE claims conformance. The associated mappings of assumptions to environmental objectives, SFRs to TOE objectives, and OSPs and objectives to threats are therefore identical to the mappings that are specified in the claimed Protection Profile.

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PP to which the ST and TOE claim conformance. These extended components are formally defined in the PP that requires their usage.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This ST will highlight the operations in the following manner:

- **Assignment:** allows the specification of an identified parameter. Indicated with bold text.
- **Refinement:** allows the addition of details. Indicated with italicized text.
- **Selection:** allows the specification of one or more elements from a list. Indicated with underlined text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR.

When multiple operations are combined, such as an assignment that is provided as an option within a selection or refinement, a combination of the text formatting is used.

If SFR text is reproduced verbatim from text that was formatted in a claimed PP (such as if the PP's instantiation of the SFR has a refinement or a completed assignment), the formatting is not preserved. This is so that the reader can identify the operations that are performed by the ST author as opposed to the PP author.

Finally, when multiple cases are specified for the handling of TSF behavior based on the contents of a selection (e.g. when conformance to different standards is required based on the type of digital signature algorithm used by the TSF), only the applicable case or cases have been retained. This unambiguously defines the TSF by excluding non-applicable conditional statements. Application notes have been included in all instances of this so that all omissions are clearly identified. If an entire SFR component is non-applicable (e.g. FAU_GEN_EXT.1.3 only applies to TOE-internal audit data storage, which the TSF does not provide), the component has been retained.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

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
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic

Class Name	Component Identification	Component Name
		signature)
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1	HTTPS
	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1	TLS
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 Management 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

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class ESM: Enterprise Security Management

6.3.1.1 ESM_EAU.2 Reliance on Enterprise Authentication

ESM_EAU.2.1	The TSF shall rely on [[**OAM authentication against external LDAP store, external OAM authentication, security questions**]] 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.

6.3.1.2 ESM_EID.2 Reliance on Enterprise Identification

ESM_EID.2.1	The TSF shall rely on [[**OAM authentication against external LDAP store, external OAM authentication, environmental email server**]] 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.

6.3.1.3 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, [**basic identity attributes, extended identity attributes, enterprise permissions, credential expiration date, credential history (stored as one-way hashes), credential change on next login flag, security questions/answers, user status, credential status**].
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.

Application Note: *The case of non-password-based credentials is not applicable to the TOE; the TOE uses passwords as its only form of credential.*

6.3.1.4 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].

6.3.2 Class FAU: Security Audit

6.3.2.1 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 *6-2* for the not specified level of audit; and

c) [**no other 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	Enrollment 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
FCS_HTTPS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_TLS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed
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

Table 6-2: Auditable Events

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, [**no other audit relevant information**].

6.3.2.2 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.

Application Note: *This is not applicable to audit data that is stored on the filesystem of the underlying OS that is local to the TOE because it does not transit a network interface.*

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.*

6.3.3 Class FCS: Cryptographic Support

6.3.3.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1 The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with:

[

- NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]

and specified cryptographic key sizes equivalent to, or greater than, 112 bits of security that meet the following: [**NIST SP 800-56B**].

6.3.3.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and cryptographic security parameters when no longer required.

6.3.3.3 FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1(1) The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in [**one or more of ECB, CBC, CFB128, OFB, CTR modes**] and cryptographic key sizes 128-bits, 256-bits, and [192 bits] that meets the following:

- FIPS PUB 197, "Advanced Encryption Standard (AES)"
- [NIST SP 800-38A]

6.3.3.4 FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services in accordance with a:

[RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater that meets FIPS PUB 186-3, "Digital Signature Standard"].

6.3.3.5 *FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)*

FCS_COP.1.1(3) The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384] and message digest sizes [160, 256, 384] bits that meet the following: FIPS Pub 180-3, "Secure Hash Standard."

6.3.3.6 FCS_COP.1(4)	*Cryptographic Operation (for keyed-hash message authentication)*
FCS_COP.1.1(4)	The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[SHA-1, SHA-256, SHA-384], key size [**160, 256, 384 bits**], and message digest sizes [160, 256, 384] bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."

6.3.3.7 FCS_HTTPS_EXT.1	*HTTPS*
FCS_HTTPS_EXT.1.1	The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2	The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

6.3.3.8 FCS_RBG_EXT.1	*Cryptographic Operation (Random Bit Generation)*
FCS_RBG_EXT.1.1	The TSF shall perform all random bit generation (RBG) services in accordance with [NIST Special Publication 800-90 using [HMAC_DRBG (any)]] seeded by an entropy source that accumulates entropy from [(3) a combination of hardware-based and software-based noise sources.].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

6.3.3.9 FCS_TLS_EXT.1	*TLS*
FCS_TLS_EXT.1.1	The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: Mandatory Ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA Optional Ciphersuites: [TLS_RSA_WITH_AES_256_CBC_SHA].

6.3.4 Class FIA: Identification and Authentication

6.3.4.1 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: [**administrative 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**].

6.3.5 Class FMT: Security Management

6.3.5.1 FMT_MOF.1 Management of Functions Behavior

FMT_MOF.1 The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions: [**functions specified in Table 6-3**] to **[authorized roles for each function specified in Table 6-3]**.

Management Activity	OIM 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 Enable/Disable Account	Application Instance Authorizer
	Grant/Revoke Account Modify Account Enable/Disable Account	Application Instance 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
	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	Add/Delete Admin Roles	User Viewer

security attributes		
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	User Viewer
Management of the users that belong to a particular role	Modify Admin Role Membership	User Viewer

Table 6-3: Management Functions by Role

6.3.5.2 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**].

6.3.5.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 The TSF shall be capable of performing the following management functions: **[management functions listed in Table 6-4].**

Requirement	Management Activity
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
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

Table 6-4: Management Functions by SFR

6.3.5.4 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, User Viewer, Help Desk**].

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

6.3.6 Class FPT: Protection of the TSF

6.3.6.1 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.

6.3.6.2 FPT_SKP_EXT.1	*Protection of TSF Data (for reading of all symmetric keys)*
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.3.7 Class FTP: Trusted Path/Channels

6.3.7.1 FTP_ITC.1	*Inter-TSF Trusted Channel*
FTP_ITC.1.1	The TSF shall use [[**TLS implemented via FCS-specified service**]] to provide a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.
FTP_ITC.1.2	The TSF shall permit [the TSF, another trusted IT product**]** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for transfer of identity and credential data, [**transfer of authentication data, transfer of audit data, provisioning of user privileges**].

6.3.7.2 FTP_TRP.1	*Trusted Path*
FTP_TRP.1.1	Refinement: The TSF shall use **[[HTTPS implemented via FCS-specified service, TLS implemented via FCS-specified service**]] to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification, disclosure.
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, execution of management functions.

6.4 Statement of Security Functional Requirements Consistency

The Security Functional Requirements included in the ST represent all required SFRs specified in the PP against which exact compliance is claimed and a subset of the optional SFRs. All hierarchical relationships, dependencies, and unfulfilled dependency rationales in the ST are considered to be identical to those that are defined in the claimed PP, with the exception of a corrected wording in FTP_ITC.1.3 to reflect the intent of the SFR.

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are consistent with the SARs that are defined in the claimed Protection Profile.

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 Developer action elements:

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

7.1.1.2 Content and presentation elements:

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

7.1.1.3 Evaluator action elements:

ADV_ FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_ FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

7.2 Class AGD: Guidance Documentation

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 Developer action elements:

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 Content and presentation elements:

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 Evaluator action elements:

AGD_OPE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 Developer action elements:

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 Content and presentation elements:

AGD_ PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

7.2.2.3 Evaluator action elements:

AGD_ PRE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

7.3 Class ALC: Life Cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 Developer action elements:

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

7.3.1.2 Content and presentation elements:

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 Evaluator action elements:

ALC_CMC.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.3.2 TOE CM Coverage (ALC_CMS.1)

7.3.2.1 Developer action elements:

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 Content and presentation elements:

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 Evaluator action elements:

ALC_CMS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.4 Class ATE: Tests

7.4.1 Independent Testing - Conformance (ATE_IND.1)

7.4.1.1 Developer action elements:

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 Content and presentation elements:

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 Evaluator action elements:

ATE_IND.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 Developer action elements:

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 Content and presentation elements:

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 Evaluator action elements:

AVA_VAN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

8 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR.

8.1 Enterprise Security Management

8.1.1 ESM_EAU.2

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. The TSF receives the result of this request and abides by that result. This same authentication method is used for user self-service.

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:

- 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.
- 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.

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.

8.1.2 ESM_EID.2

See ESM_EAU.2 above.

8.1.3 ESM_ICD.1

The TOE is responsible for configuring and maintaining identity and credential attributes for organizational users. These attributes define 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 Active Directory, OID, or OUD as the organizational user store, or 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.

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.

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.

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.

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
    - Active Directory
    - Exchange
    - Windows
- Novell
    - eDirectory
    - GroupWise
- Oracle
    - 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
- UNIX

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.

In the evaluated configuration, the organizational identity store is an Active Directory, 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.

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. !, $, #, ^)

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.

8.1.4 ESM_ICT.1

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.

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.

8.2 Security Audit

8.2.1 FAU_GEN.1:

The TSF generates audit records when auditable events occur. The auditable events that are logged are described in Table 6-2. 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

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

8.2.2 FAU_STG_EXT.1:

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. All communications between the TOE and the RDBMS use JDBC and are encrypted using TLS. No audit data is stored directly within the TOE boundary so the Operational Environment is expected to protect the stored audit data.

8.3 Cryptographic Support

8.3.1 FCS_CKM.1:

The TSF uses RSA Crypto-J version 5.0 running in a FIPS-compliant mode of operation to perform its cryptographic operations. The TSF complies with the key establishment specifications as stated in NIST SP 800-56B for the generation of asymmetric keys.

8.3.2 FCS_CKM_EXT.4:

The TOE zeroizes all secret cryptographic data when no longer in use. All cryptographic data is stored in volatile memory only and is overwritten with all zeroes by invoking the sensitiveData.clear() method in the underlying cryptographic module. The following table lists the cryptographic key and parameter data that is maintained by the cryptographic module that is used by the TOE:

Service	Cryptographic Data
Encryption and decryption	AES secret keys
Digital signature and verification	RSA private keys
MAC	HMAC keys
Random number generation	HMAC DRBG entropy, strength, and seed
Key establishment primitives	RSA private keys

Table 8-1: Cryptographic Data

8.3.3 FCS_COP.1(1):

The TOE uses the RSA Crypto-J version 5.0 cryptographic module to perform encryption and decryption using AES (CAVP certificate #1465).

8.3.4 FCS_COP.1(2):

The TOE uses the RSA Crypto-J version 5.0 cryptographic module to perform digital signature services using RSA (CAVP certificate #717).

8.3.5 FCS_COP.1(3):

The TOE uses the RSA Crypto-J version 5.0 cryptographic module to perform cryptographic hashing using SHA-1, SHA-256, or SHA-384 (CAVP certificate #1328).

8.3.6 FCS_COP.1(4):

The TOE uses the RSA Crypto-J version 5.0 cryptographic module to perform cryptographic hashing using HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 (CAVP certificate #863).

8.3.7 FCS_HTTPS_EXT.1:

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.

8.3.8 FCS_RBG_EXT.1:

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.

8.3.9 FCS_TLS_EXT.1:

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 TLS 1.0 or TLS 1.2. 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.

8.4 Identification and Authentication

8.4.1 FIA_USB.1:

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.

8.5 Security Management

8.5.1 FMT_MOF.1:

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.

Table 6-3 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 OIM 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 6-3, 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.

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.

8.5.2 FMT_MTD.1:

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.

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.

8.5.3 FMT_SMF.1:

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 6-4 defines the set of management activities that are prescribed by the claimed PP. Note that each of these functions are performed using the OIM 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.

8.5.4 FMT_SMR.1:

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 8-2 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 OIM 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.

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.

Administrator Role	Privileges Summary
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 Authorizer	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 Authorizer	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.
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 Authorizer	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. Can also assign users to admin roles to give them the ability to manage the TSF.

Table 8-2: Administrative Roles

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.

8.6 Protection of the TSF

8.6.1 FPT_APW_EXT.1:

Password data for organizational users is 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.

8.6.2 FPT_SKP_EXT.1:

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.

8.7 Trusted Path/Channels

8.7.1 FTP_ITC.1:

The TSF provides trusted channels that secure remote communications between the TOE and entities within the Operational Environment that handle TSF data. The trusted channels that are established are between the TOE and the organizational identity store, between the TOE and the environmental RDBMS, and between the TOE and any distributed connectors. Trusted channel data transmission is initiated by the TSF in all cases except for the Peoplesoft connector, which is initiated by the Operational Environment components that use it. All secure remote communications provided by the TSF are protected using TLS 1.0. The TOE uses RSA Crypto-J version 5.0 (CMVP certificate #1503) to implement this communications protocol. 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 OIM, this is not considered to be part of the TSF.

8.7.2 FTP_TRP.1:

The TSF provides a trusted path that secures administrator communications with the TOE. This trusted path is established using HTTPS/TLS 1.2 for the web GUI. The TOE uses RSA Crypto-J version 5.0 (CMVP certificate #1503) to implement the secure communications protocols used to establish the trusted path.