Oracle Access Manager Suite

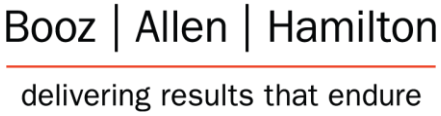
Version 11g Release 2

Security Target

ST Version: 1.0
July 13, 2017

Oracle Corporation
100 Oracle Parkway
Redwood City, CA 94065

Prepared By:



Cyber Assurance Testing Laboratory
304 Sentinel Drive
Annapolis Junction, MD 20701

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 Profiles (PPs):

- Standard Protection Profile for Enterprise Security Management Access Control, version 2.1
- Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1

1.1.1 ST Identification

ST Title:	Oracle Access Manager Suite 11g Release 2 Security Target
ST Version:	1.0
ST Publication Date:	July 13, 2017
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.

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

Table 1-1: Product 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
AC	Access Control
CC	Common Criteria
ESM	Enterprise Security Management
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IT	Information Technology
J2EE	Java 2 Enterprise Edition
JDBC	Java Database Connectivity
JDK	Java Development Kit
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OAM	Oracle Access Manager
OES	Oracle Entitlements Server
OID	Oracle Internet Directory
OUD	Oracle User Directory
PDP	Policy Decision Point
PEP	Policy Enforcement Point

PM	Policy Management
PP	Protection Profile
RBG	Random Bit Generation
RDBMS	Relational Database Management System
rDSA	RSA Digital Signature Algorithm
RFC	Request for Comment
RMI	Remote Management Interface
SAR	Security Assurance Requirements
SDK	Software Development Kit
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TLS	Transport Layer Security
TSF	TOE Security Function
TSFI	TOE Security Function Interface
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WLS IAP	WebLogic Server Identity Assertion Provider

Table 1-2: Acronym Definition

1.1.5 References

[1] or [AC] Standard Protection Profile for Enterprise Security Management Access Control, version 2.1 (AC PP)

[2] or [PM] Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1 (PM PP)

[3] 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

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

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

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

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

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

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

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

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

[12] Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[13] Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)
[14] Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server
[15] Administrator's Guide for Oracle Access Management for All Platforms

1.2 TOE Reference

The TOE is Oracle Access Manager Suite 11g Release 2, which contains the following components:

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

1.3 TOE Overview

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

The following figure depicts the TOE boundary:

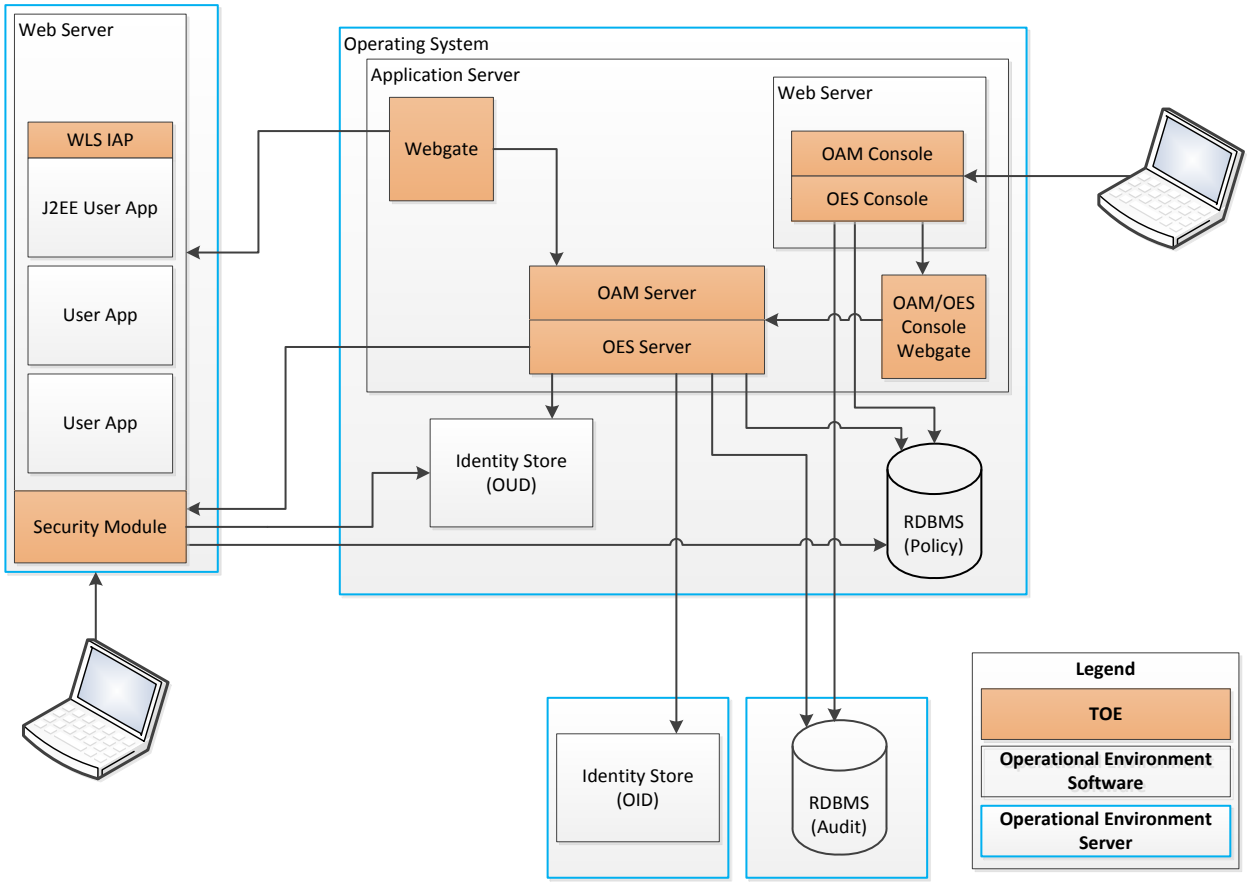


Figure 1-1: TOE Boundary

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

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

In the evaluated configuration, one or more Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) are connected to user space web applications in the Operational Environment. When users attempt to perform actions against these applications, the requests are either intercepted by a PEP or transmitted by the application to a PDP for further adjudication. The PDP compares the request to administratively-configured access control policies that are stored in the environmental RDBMS and determines whether

or not the requests should be authorized. The application then acts based on these decisions. The TOE provides two kinds of PDPs/PEPs:

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

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

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

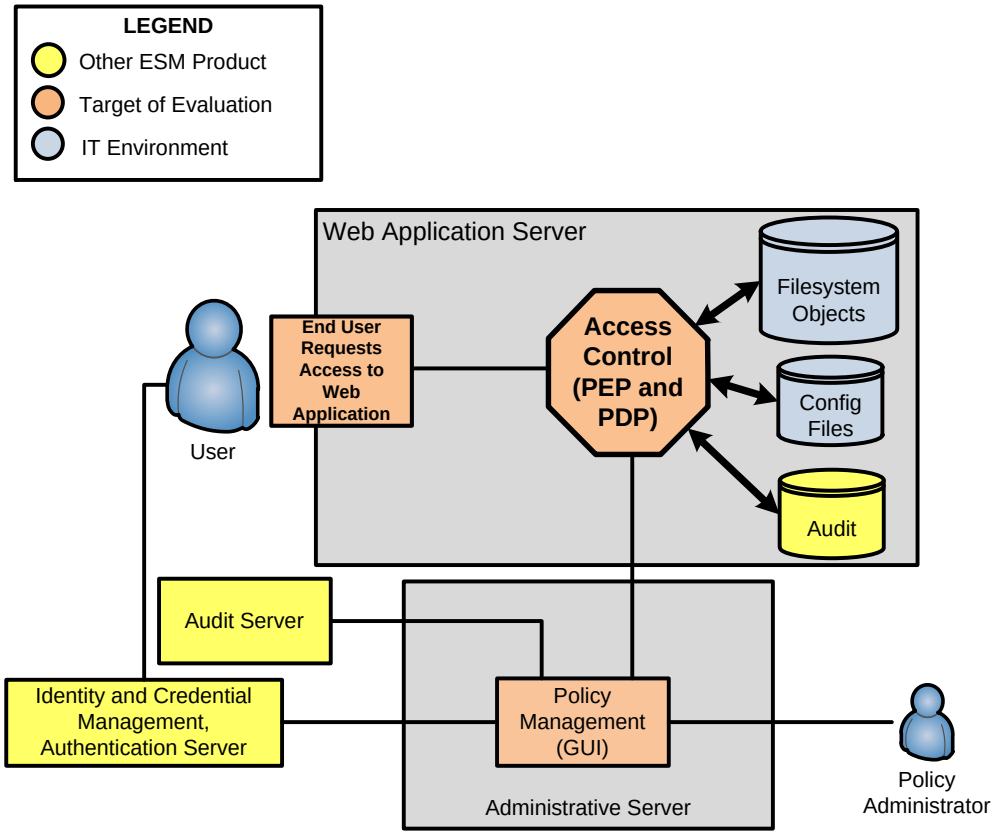


Figure 1-2: ESM PP context for the TOE

Figure 1-2 illustrates the TOE in the context of the Enterprise Security Management Protection Profile suite. The ability of the PDP and PEP to intercept activities on a web application can be seen as an Access Control product. The OAM and OES administrative interfaces can be seen as a Policy Management

capability. The Identity Store serves as Identity and Credential Management for administrators and users, and audit data can be logged to an external source.

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

- Because the TOE claims conformance to both the AC PP and PM PP, the Policy Management component was highlighted as part of the TOE.
- The TSF is not expected to interface with a Secure Configuration Management product.
- The other products with which the TOE interfaces have not currently been evaluated against Enterprise Security Management PPs.

1.4 TOE Type

The TOE type for OAM Suite is Enterprise Security Management, specifically Web-Based Access Control and Policy Management. The TOE includes Security Modules act as PDPs and PEPs for web applications, intercepting user requests on these applications and determining whether they should be authorized. The TOE provides administrative interfaces to configure the policies that the Security Modules use for decision-making and enforcement. This is considered to be an enterprise-level product because it can be used to control access to enterprise web applications that are deployed internally within an 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 TOE is limited to the OAM Suite (which contains OAM and OES), which at a general level provides both the means to enforce access controls against web-based resources and the interface to define the access control rules. The following table describes the TOE components in the evaluated configuration:

Component	Definition
Access Clients	See Webgates.
OAM Console	A web-based administrative GUI used to configure the behavior of Webgates.
OAM Server	A server-side application, installed on an environmental WebLogic Managed Server, which is responsible for handling the back-end of the OAM Console. Note that the OAM Server and OES Server may reside on the same underlying application server.
OES Administration Console	The web-based administrative GUI used to configure the behavior of Security Modules. Also referred to as OES Console in this ST.
OES Server	A server-side application, installed on an environmental WebLogic Managed Server, which is responsible for handling the back-end of the OES Console. Note that the OAM Server and OES Server may reside on the same underlying application server.
Security Modules	Agents provided as part of OES that are installed onto web servers (WebLogic) and can enforce access control on specific actions or functions provided by the web server.
Webgates	Agents provided as part of OAM that are used to control access to web servers by acting as filters for HTTP requests.
WLS IAP	An agent deployed on a J2EE WebLogic server as a mechanism that allows the server to communicate with a Webgate.

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	Provides the back-end functionality to support the hosting and execution of the applications used by administrators to manage the TSF.
Identity Store	An LDAP repository that defines identity and attribute data for organizational users as well as administrators of the TOE.
Keystore	A Java-based repository that is used to store certificate data for use with public-key cryptography.
Operating System	The underlying platform on which each component of the TOE is installed. Includes the local filesystem component for storage of audit data for TOE activity.
RDBMS	A relational database that stores access control policy data that is defined by the TOE and audit data for TOE activity.

User Application(s)	Web applications that are deployed internally to an organization and used to perform various internal functions. Example include applications related to finances, personnel management, and help desk.

Table 2-2: Evaluated 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

No components of the product 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

These components are installed with the OAM Suite but are not included in the TSF.

Separate products that are installed in tandem with Oracle Identity and Access Management, of which the OAM Suite is a part:

- Oracle Unified Directory
- Oracle Adaptive Access Manager
- Oracle Identity Manager
- Oracle Enterprise Single Sign-on Suite Plus
- Oracle Privileged Account Manager
- Oracle Mobile Security Suite

Separate components within the OAM Suite with non-interfering security functions:

- Oracle Security Token Service
- Oracle Identity Federation
- Oracle Access Management Mobile and Social
- Oracle Access Management Access Portal Service
- Oracle Access Management Adaptive Authentication

2.4 Physical Boundary

The physical boundary of the TOE includes the Oracle Access Manager and Oracle Entitlements Server software that is installed on the system. The TOE does not include the hardware or operating systems of the systems on which it is installed. It also does not include the third-party software which is required for the TOE to run. The following table lists the minimum software components that are required to use the TOE:

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

Table 2-3: Operational Environment System Requirements

2.5 Logical Boundary

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Enterprise Security Management
2. Security Audit
3. Communications
4. Cryptographic Support
5. User Data Protection
6. Identification and Authentication
7. Security Management
8. Protection of the TSF
9. Resource Utilization
10. TOE Access
11. Trusted Path/Channels

2.5.1 Enterprise Security Management

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

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

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

2.5.2 Security Audit

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

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

2.5.3 Communications

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

2.5.4 Cryptographic Support

The TOE provides cryptographic capabilities in support of TLS and HTTPS secure communications. Cryptographic capabilities are provided by the FIPS 140-2 validated RSA BSAFE Crypto-C Micro Edition version 4.1.2 software cryptographic module, CMVP certificate #2300. This means that the individual cryptographic algorithms used by the TOE are also FIPS-validated and that the cryptographic module takes appropriate action to zeroize cryptographic keys when no longer needed. This module is provided with OAM Suite and is therefore considered to be within the scope of the TOE. However, Oracle simply provides this component; it is not modified in any way. The module was validated at Overall Level 1, with Level 3 Cryptographic Module Specification.

2.5.5 User Data Protection

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

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

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

2.5.6 Identification and Authentication

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

2.5.7 Security Management

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

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

2.5.8 Protection of the TSF

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

2.5.9 Resource Utilization

If the connection between a PDP and the server is lost, that PDP will be able to continue enforcing the last policy received or act on cached enforcement decisions, depending on the PDP type. The PDPs will

periodically poll the server for new policy information, so in the event of communications being restored, the latest policy data will be retrieved without administrator intervention.

2.5.10 TOE Access

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

2.5.11 Trusted Path/Channels

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

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 July 13, 2017.

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 July 13, 2017.

3.4 PP Claims

This ST claims exact compliance to the following Protection Profiles:

- Standard Protection Profile for Enterprise Security Management Access Control, version 2.1
- Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1

The following is the list of NIAP Technical Decisions that are applicable to the ST/TOE:

- TD0042
- TD0055
- TD0066
- TD0079

3.5 Package Claims

The TOE claims exact conformance to Protection Profiles that are conformant with CC Part 3. The TOE claims the following architectural variations and/or optional SFRs that are defined in the appendices of the claimed PPs:

- AC PP
    - Web-Based Access Control (Appendix C.1.3)
    - Conditional Enforcement of Session Establishment (Appendix C.4)
    - Cryptographic Key Generation (Appendix C.5.1)
    - Cryptographic Key Zeroization (Appendix C.5.2)
    - Cryptographic Operation (Appendix C.5.3 through C.5.6 and Appendix C.5.9)
    - HTTPS (Appendix C.5.7)
    - TLS (Appendix C.5.11)
- PM PP
    - Object Attribute Definition (Appendix C.1.1)
    - Subject Attribute Definition (Appendix C.1.2)
    - Selectable Auditing (Appendix C.3)
    - Cryptographic Key Generation (Appendix C.8.1)
    - Cryptographic Key Zeroization (Appendix C.8.2)
    - Cryptographic Operation (Appendix C.8.3 through C.8.6 and Appendix C.8.9)
    - HTTPS (Appendix C.8.7)

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

Note in particular that the TOE claims the SFR FTA_TSE.1. This SFR is optional in both the ACPP and PMPP. The TOE only claims this for the access control component; the policy management component (Appendix C.7.2 in PMPP) is not claimed.

3.6 Package Name Conformant or Package Name Augmented

This ST claims exact conformance to two Protection Profiles. The ST is conformant to the claimed package.

3.7 Conformance Claim Rationale

The AC PP states the following: “The purpose of an Access Control product is to enforce access control policies.”

The PM PP states the following: “A TOE that conforms to this PP may be able to define policies that control access to any of a wide variety of resources.”

The TOE provides the ability to both define and enforce access control policies. These access control policies enforce access to the resources that are defined for Web-Based Access Control in the AC PP. The TOE protects objects that reside on a web server, which can be considered an enterprise-level resource. Therefore, the conformance claims to AC PP and PM PP are appropriate. The SFRs that were chosen from these PPs include all required SFRs and a subset of optional SFRs defined as such by the PPs. Therefore, the conformance claim of exact compliance is appropriate.

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE as well as the threats that the TOE is deployed into the Operational Environment to mitigate. These threats have been taken from the AC PP and PM PP. The following table combines the threats defined in these PPs and indicates the PP(s) from which they were taken:

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

Table 4-1: Threats

Note the following in the above table:

- In some cases, the same name is used to identify two threats with different wordings. When a threat whose definition is overloaded is referenced, it will be identified with its PP reference preceding its name (i.e. [AC]T.UNAUTH).
- If the threat's wording is identical in both claimed PPs, it will be referenced by its name only.
- All references to "Access Control product" and "Policy Management product" are considered to refer to the parts of the TOE that are responsible for these capabilities. Since the TOE claims both PPs, the references are to parts of itself rather than to two distinct products.

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 AC PP and PM PP. The following table combines the policies defined in these PPs and indicates the PP(s) from which they were taken:

PP	Policy Name	Policy Definition
[PM]	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.
[AC]	P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

Table 4-2: TOE Organizational Security Policies

4.3 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the AC PP and PM PP. The tables listed in the following subsections list the assumptions defined in these PPs and indicates the PP(s) from which they were taken.

For those assumptions that were defined in the PPs as optional and are claimed as part of the security problem definition for the TOE, the suffix "(optional)" has been added.

4.3.1 Personnel Assumptions

PP	Assumption	Assumption Definition
[AC]	A.INSTALL	There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.
[PM]	A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.

Table 4-3: Personnel Assumptions

4.3.2 Physical Assumptions

No physical assumptions have been defined for the TOE.

4.3.3 Connectivity Assumptions

PP	Assumption	Assumption Definition
[AC]	A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
[PM]		
[AC]	A.POLICY	The TOE will receive policy data from the Operational Environment.
[AC]	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.
[PM]		
[AC]	A.SYSTIME (optional)	The TOE will receive reliable time data from the Operational Environment.
[PM]		
[AC]	A.USERID	The TOE will receive identity data from the Operational Environment.
[PM]		

Table 4-4: Connectivity Assumptions

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 AC PP and PM PP. The following table combines the objectives defined in these PPs and indicates the PP(s) from which they were taken:

PP	TOE Objective	TOE Objective Definition
[PM]	O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
[PM]	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.
[PM]	O.AUTH	The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
[PM]	O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
[PM]	O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.
[AC]	O.CRYPTO	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
[PM]		
[AC]	O.DATAPROT	The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
[PM]	O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
[AC]	O.INTEGRITY	The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.
[PM]		The TOE will contain the ability to assert the integrity of policy data.
[AC]	O.MAINTAIN	The TOE will be capable of maintaining access control policy enforcement if it is unable to communicate with the Policy Management product which provided it the policy.
[PM]	O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
[AC]	O.MNGRID	The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.
[AC]	O.MONITOR	The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users).
[AC]	O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.
[PM]	O.POLICY	The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.
[AC]	O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
[PM]		
[PM]	O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
[AC]	O.SELFID	The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.

[PM]		The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

Table 4-5: TOE Objectives

Note the following in the above table:

- In some cases, the same name is used to identify two objectives with different wordings. When an objective whose definition is overloaded is referenced, it will be identified with its PP reference preceding its name (i.e. [AC]O.SELFID).
- All references to "Access Control product" and "Policy Management product" are considered to refer to the parts of the TOE that are responsible for these capabilities. Since the TOE claims both PPs, the references are to itself rather than to two distinct products.

4.4.2 Security Objectives for the Operational Environment

The TOE's operating environment must satisfy the following objectives:

PP	Environmental Objective	Environmental Objective Definition
[PM]	OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.
[AC]	OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
[PM]		
[AC]	OE.POLICY	The Operational Environment will provide a policy that the TOE will enforce.
[PM]	OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
[PM]	OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
[PM]	OE.ROBUST (optional)	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
[AC]	OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.
[PM]	OE.SYSTIME (optional)	
[AC]	OE.USERID	The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.
[PM]		The Operational Environment shall be able to identify a user requesting access to the TOE.

Table 4-6: TOE Operational Environment Objectives

Note the following in the above table:

- In some cases, the same name is used to identify two objectives with different wordings. When an objective whose definition is overloaded is referenced, it will be identified with its PP reference preceding its name (i.e. [AC]OE.USERID).
- If the objective's wording is identical in both claimed PPs, it will be referenced by its name only.
- All references to "Access Control product" and "Policy Management product" are considered to refer to the parts of the TOE that are responsible for these capabilities. Since the TOE claims both PPs, the references are to itself rather than to two distinct products.

4.4.3 Operational Environment Components Rationale

The following table summarizes how the Operational Environment components and applications are expected to satisfy the Operational Environment objectives in the evaluated configuration. Some Operational Environment objectives are in fact satisfied by the TSF. The reason for this is that the TOE claims conformance to multiple Protection Profiles and each Protection Profile assumes that anything covered by another Protection Profile is part of the Operational Environment.

PP	Environmental Objective	Satisfied by
[PM]	OE.ADMIN	N/A – this objective is satisfied by a personnel assumption
[AC]	OE.INSTALL	N/A – this objective is satisfied by a personnel assumption
[PM]		
[AC]	OE.POLICY	The TSF
[PM]	OE.PERSON	N/A – this objective is satisfied by a personnel assumption
[PM]	OE.PROTECT	The TSF
[AC]	OE.SYSTIME	System clock
[PM]	OE.SYSTIME (optional)	
[AC]	OE.USERID	Identity Store
[PM]		

Table 4-7: TOE Operational Environment Components Rationale

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives which are defined in this ST represent the combination of the assumptions, threats, OSPs, and objectives that are specified in the two Protection Profiles to which the ST and TOE claim exact 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 Profiles.

The set of assumptions and objectives have been defined based on the optional SFRs that have and have not been claimed. This definition was performed according to the instructions presented in the security problem definition rationale for the claimed PPs.

Because the TOE consists of both Access Control and Policy Management components, all references to these components in the security problem definition are understood to refer to the TSF and not the Operational Environment. Since the SFRs that provide the assumed capabilities are part of the TSF, the accuracy of these objectives will be verified by testing.

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 PPs to which the ST and TOE claim conformance. These extended components are formally defined in the PPs that require 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 four operations in a manner which is consistent with the claimed PP, specifically:

- 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.

The use of square brackets without any other text formatting is used to indicate a selection or assignment that was made in the PP that the ST author does not have discretion to modify.

In addition to this, the fact that the TOE claims conformance to multiple PPs means that there are numerous SFRs with non-unique names. Rather than altering the SFR names, the following conventions have been defined:

- For SFRs that are only defined in one of the claimed PPs: the SFR name is prefaced with a reference to the PP from which it was taken in square brackets; i.e. [AC]FCO_NRR.2.1.
- For SFRs that are identical in both of the claimed PPs: the SFR name is prefaced with the text "AC+PM" in bold square brackets; i.e. [AC+PM]FAU_GEN.1.1.
- For SFRs that have the same name but different definitions in each of the claimed PPs: in addition to having the SFR name prefaced with "AC+PM" in bold square brackets, markers are placed in bold square brackets that identify the parts of the SFR which belong to each PP. For example, the list of auditable events specified in [AC+PM]FAU_GEN.1.1 will have some entries prefaced with [AC], some entries prefaced with [PM], and still others prefaced with [AC+PM].

These conventions have been defined to unambiguously identify the SFRs that are from the claimed PPs so that the claim of exact conformance can be confirmed and so that duplicate functional claims are not re-iterated unnecessarily.

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	**[PM]**ESM_ACD.1	Access Control Policy Definition
	[PM]ESM_ACT.1	Access Control Policy Transmission
	[PM]ESM_ATD.1	Object Attribute Definition
	[PM]ESM_ATD.2	Subject Attribute Definition

Class Name	Component Identification	Component Name
	[PM]ESM_EAU.2	Reliance on Enterprise Authentication
	[AC+PM]ESM_EID.2	Reliance on Enterprise Identification
Security Audit	**[AC+PM]**FAU_GEN.1	Audit Data Generation
	[AC]FAU_SEL.1	Selective Audit
	[PM]FAU_SEL.1	Selective Audit
	[PM]FAU_SEL_EXT.1	External Selective Audit
	[AC]FAU_STG.1	Protected Audit Trail Storage (Local Storage)
	[AC+PM]FAU_STG_EXT.1	External Audit Trail Storage
Communications	**[AC]**FCO_NRR.2	Enforced Proof of Receipt
Cryptographic Support	**[AC+PM]**FCS_CKM.1	Cryptographic Key Generation (for Asymmetric Keys)
	[AC+PM]FCS_CKM_EXT.4	Cryptographic Key Zeroization
	[AC+PM]FCS_COP.1(1)	Cryptographic Operation (for Data Encryption/Decryption)
	[AC+PM]FCS_COP.1(2)	Cryptographic Operation (for Cryptographic Signature)
	[AC+PM]FCS_COP.1(3)	Cryptographic Operation (for Cryptographic Hashing)
	[AC+PM]FCS_COP.1(4)	Cryptographic Operation (for Keyed-Hash Message Authentication)
	[PM]FCS_HTTPS_EXT.1	HTTPS
	[AC+PM]FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
	[AC+PM]FCS_TLS_EXT.1	TLS
User Data Protection	**[AC]**FDP_ACC.1	Access Control Policy
	[AC]FDP_ACF.1	Access Control Functions
Identification and Authentication	**[PM]**FIA_USB.1	User-Subject Binding
Security Management	**[PM]**FMT_MOF.1	Management of Functions Behavior
	[AC]FMT_MOF.1(1)	
	[AC]FMT_MOF.1(2)	
	[PM]FMT_MOF_EXT.1	External Management of Functions Behavior
	[AC]FMT_MSA.1	Management of Security Attributes
	[AC]FMT_MSA.3	Static Attribute Initialization
	[PM]FMT_MSA_EXT.5	Consistent Security Attributes
	[AC+PM]FMT_SMF.1	Specification of Management Functions
	[AC+PM]FMT_SMR.1	Security Roles
Protection of the TSF	**[AC+PM]**FPT_APW_EXT.1	Protection of Stored Credentials
	[AC]FPT_FLS_EXT.1	Failure of Communications
	[AC]FPT_RPL.1	Replay Detection
	[AC+PM]FPT_SKP_EXT.1	Protection of Secret Key Parameters
Resource Utilization	**[AC]**FRU_FLT.1	Degraded Fault Tolerance
TOE Access	**[AC]**FTA_TSE.1	TSF-initiated Termination
Trusted Path /Channels	[**AC+PM]**FTP_ITC.1	Inter-TSF Trusted Channel
	[PM]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 [PM]ESM_ACD.1 Access Control Policy Definition

[PM]ESM_ACD.1.1 The TSF shall provide the ability to define access control policies for consumption by one or more compatible Access Control products.

[PM]ESM_ACD.1.2 Access control policies defined by the TSF shall be capable of containing the following:

- Subjects: [**organizational users defined in Identity Store**]; and
- Objects: [**URLs, files, executable scripts, forms**]; and
- Operations: [**access, open, download, execute, enable, disable, HTTP operations**]; and
- Attributes: [**attributes associated with organizational users defined in Identity Store]**

[PM]ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

6.3.1.2 [PM]ESM_ACT.1 Access Control Policy Transmission

[PM]ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: [immediately following creation of a new or updated policy, at a periodic interval].

6.3.1.3 [PM]ESM_ATD.1 Object Attribute Definition

[PM]ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: [**required authentication level, administrator-defined attributes**].

Application Note: *Administrator-defined attributes can be arbitrarily defined. An example of this would be using the TOE to define attribute values such as "required role" for a web application object that can be used to enforce different access control policies against different objects in the same repository.*

[PM]ESM_ATD.1.2 The TSF shall be able to associate security attributes with individual objects.

6.3.1.4 [PM]ESM_ATD.2 Subject Attribute Definition

[PM]ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: [**administrator-defined attributes**].

Application Note: *Administrator-defined attributes can be arbitrarily defined.*

[PM]ESM_ATD.2.2 The TSF shall be able to associate security attributes with individual subjects.

6.3.1.5 [PM]ESM_EAU.2 Reliance on Enterprise Authentication

[PM]ESM_EAU.2.1 The TSF shall rely on [[**LDAP (OID, OUD) in the Operational Environment**]] for subject authentication.

[PM]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.

6.3.1.6 [AC+PM]ESM_EID.2 Reliance on Enterprise Identification

[AC+PM]ESM_EID.2.1 The TSF shall rely on [[**LDAP (OID, OUD) in the Operational Environment, calling application identity store**]] for subject identification.

[AC+PM]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.

6.3.2 Class FAU: Security Audit

6.3.2.1 [AC+PM]FAU_GEN.1 Audit Data Generation

[AC+PM]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**].

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.*

Component	Event	Additional Information
[PM]ESM_ACD.1	Creation or modification of policy	Unique policy identifier
[PM]ESM_ACT.1	Transmission of policy to Access Control products	Destination of policy
[PM]ESM_ATD.1	Association of attributes with objects	None
[PM]ESM_ATD.2	Association of attributes with subjects	None
[PM]ESM_EAU.2	All use of the authentication mechanism	None
[AC]FAU_SEL.1	All modifications to audit configuration	None

[PM]FAU_SEL_EXT.1	All modifications to audit configuration	None
[AC+PM]FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
[AC]FCO_NRR.2	The invocation of the non-repudiation service	Identification of the information, the destination, and a copy of the evidence provided
[AC]FDP_ACC.1	Any changes to the enforced policy or policies	Identification of Policy Management product making the change
[AC]FDP_ACF.1	All requests to perform an operation on an object covered by the SFP	Subject identity, object identity, requested operation
[PM]FIA_USB.1	Successful and unsuccessful binding of user attributes to a subject	None
[AC]FMT_MOF.1	All modifications to TSF behavior	None
[PM]FMT_MSA.1	All modifications of security attributes	None
[AC]FMT_MSA.3	All modifications of the initial values of security attributes	Attribute modified, modified value
[AC+PM]FMT_SMF.1	Use of the management functions	Management function performed
[AC+PM]FMT_SMR.1	Modifications of the members of the management roles	None
[AC]FPT_FLS_EXT.1	Failure of communication between the TOE and Policy Management product	Identity of the Policy Management product, reason for the failure
[AC]FPT_RPL.1	Detection of replay	Action to be taken based on the specific actions
[AC+PM]FTA_TSE.1	Denial of session establishment	None
[AC+PM]FTP_ITC.1	All use of the trusted channel functions	Identity of the initiator and target of the trusted channel
[PM]FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with trusted path functions, if available

Table 6-2: Auditable Events

[AC+PM]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, [**the information in Table 6-2, other audit relevant information**].

6.3.2.2 [AC]FAU_SEL.1 Selective Audit

[AC]FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [event type]; and

b) [**no other attributes**]

6.3.2.3 [PM]FAU_SEL.1 Selective Audit

[PM]FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events *from [local definition]* based on the following attributes:

a) [event type]; and

b) [**no other attributes**]

6.3.2.4 [PM]FAU_SEL_EXT.1 External Selective Audit

[PM]FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by [an ESM Access Control product] from the set of all auditable events based on the following attributes:

a) [event type]; and

b) [**no other attributes**]

6.3.2.5 [AC]FAU_STG.1 Protected Audit Trail Storage (Local Storage)

[AC]FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

[AC]FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

6.3.2.6 [AC+PM]FAU_STG_EXT.1 External Audit Trail Storage

[AC+PM]FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [**database, local file system**].

[AC+PM]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.

[AC+PM]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. All audit data is stored in the Operational Environment.*

6.3.3 Class FCO: Communications

6.3.3.1 [AC]FCO_NRR.2 Enforced Proof of Receipt	
[AC]FCO_NRR.2.1	The TSF shall enforce the generation of evidence of receipt for received policies at all times.
[AC]FCO_NRR.2.2	The TSF shall be able to relate the [**PDP instance name or Webgate unique identifier**] of the recipient of the information, and the [**policy name and version, policy UID**] of the information to which the evidence applies.
[AC]FCO_NRR.2.3	The TSF shall provide a capability to verify the evidence of receipt of information to originator given [**new or updated policy received within elapsed amount of time equal to polling interval**].

6.3.4 Class FCS: Cryptographic Support

6.3.4.1 [AC+PM]FCS_CKM.1	***Cryptographic Key Generation (for Asymmetric Keys)***
[AC+PM]FCS_CKM.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: [standards defined in first selection].

6.3.4.2 [AC+PM]FCS_CKM_EXT.4	***Cryptographic Key Zeroization***
[AC+PM]FCS_CKM_EXT.4.1	The TSF shall zeroize all plaintext secret and private cryptographic keys and cryptographic security parameters when no longer required.

6.3.4.3 [AC+PM]FCS_COP.1(1)	***Cryptographic Operation (for Data Encryption/Decryption)***
[AC+PM]FCS_COP.1.1(1)	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in [**CBC mode**] and cryptographic key sizes 128-bits, 256-bits and [no other key sizes] that meets the following:

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

6.3.4.4 [AC+PM]FCS_COP.1(2)	***Cryptographic Operation (for Cryptographic Signature)***
[AC+PM]FCS_COP.1.1(2)	The TSF shall perform cryptographic signature services in accordance with: • [RSA Digital Signature Algorithm (rDSA) with a key size (modulus) 2048 bits or greater] That meets the following: • *RSA Digital Signature Algorithm FIPS PUB 186-3, "Digital Signature Standard"*

6.3.4.5 [AC+PM]FCS_COP.1(3)	***Cryptographic Operation (for Cryptographic Hashing)***
[AC+PM]FCS_COP.1.1(3)	The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-1] and message digest sizes [160] bits that meet the following: FIPS Pub 180-3, "Secure Hash Standard".

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

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

6.3.4.8 [AC+PM]FCS_RBG_EXT.1	***Cryptographic Operation (Random Bit Generation)***
[AC+PM]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 [one or more independent software-based noise sources].

[AC+PM]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.

6.3.4.9 [AC+PM]FCS_TLS_EXT.1 TLS

[AC+PM]FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[TLS_RSA_WITH_AES_256_CBC_SHA].

6.3.5 Class FDP: User Data Protection

6.3.5.1 [AC]FDP_ACC.1 Access Control Policy

[AC]FDP_ACC.1.1 The TSF shall enforce the [access control Security Function Policy (SFP)] on [

- Subjects: subset of users from an organizational data store; and
- Objects: URLs, files, executable scripts, forms; and
- Operations: access, open, download, execute, enable, disable, HTTP operations]

6.3.5.2 [AC]FDP_ACF.1 Access Control Functions

[AC]FDP_ACF.1.1 The TSF shall enforce the [access control SFP] to objects based on the following: [all operations between subjects and objects defined in Table 6-3 below based upon some set of organizational attributes].

Subject	Object	Operation
User	URLs	Access via HTTP operation
	Files	Open
		Download
	Executable Scripts	Execute
		Enable
		Disable
	Forms	HTTP GET
		HTTP POST

Table 6-3: Access Control Subjects, Objects, and Operations

[AC]FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- **Webgate rules:**
  - **Webgates are applied to web applications in the Operational Environment**
  - **Within a Webgate, authorization policies are applied to URIs that are contained with a protected web application**
  - **Authorization policies can be enforced on identity, IP address, temporal, and attribute conditions**
  - **Rules can be used to define one or more conditions that result in the requested access being allowed or denied using Boolean logic**
  - **Rules can result in additional authentication factors being requested**
  - **Responses can be used to transmit data back to the operational environment so that the calling application can take additional action beyond redirecting a subject**
  - **If an object is protected by an authorization policy, access to it is controlled on a deny-by-default basis**
- **Security Module rules:**
  - **Security Modules can control access to the following types of applications: Java, J2EE, WebLogic**
  - **Authorization policies are associated with Security Modules and define the subject-object-operation pairings that will result in access being allowed or denied**
  - **Subjects are identified by username, group membership, or role**
  - **Objects are identified by resource name and type**
  - **An authorization policy is configured either to grant**

access or deny access if the conditions of the access request apply to it

- **By default, an authorization policy evaluates all actions against a resource that is defined as protected, but specific actions may optionally be excluded from this**
- **Authorization policies may optionally contain multiple conditions that relate to one another using Boolean logic so that combinations of conditions can be used to make an access control decision**
- **Responses can be used to transmit data back to the operational environment so that the calling application can take additional action beyond redirecting a subject**
- **If multiple authorization policies apply to the same action, a deny result takes precedence over any number of permit results**].

[AC]FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based of the following additional rules: [**Webgates can be configured to enforce policies in the order in which they are listed rather than operate on a deny-by-default basis**].

[AC]FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

6.3.6 Class FIA: Identification and Authentication

6.3.6.1 [PM]FIA_USB.1	*User-Subject Binding*

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

[PM]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: [**administrators are assigned a session at login time**].

[PM]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: [**user permission change terminates their active session with changes taking effect on next login**].

6.3.7 Class FMT: Security Management

6.3.7.1 [PM]FMT_MOF.1	*Management of Functions Behavior*

[PM]FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behavior of, modify the behavior of] the functions: [**specified in Table 6-4**] to [**authorized roles**

with the following conditions:

- **System administrators can perform all management functions without restriction**
- **Domain administrators can only perform management functions within their domain].**

Application Note: *Domain administrators are able to manage the configuration of Webgates and/or Security Modules if a system administrator or other domain administrator assigns them to the same domain. A domain administrator can also define new domains that are subsets of the domain that they are authorized to administer and assign administrators for any of these domains.*

SFR	Management Activity
[PM]ESM_ACD.1	Creation of policies
[PM]ESM_ACT.1	Transmission of policies
[PM]ESM_ATD.1	Association of attributes with objects
[PM]ESM_ATD.2	Association of attributes with subjects
[PM]ESM_EAU.2	N/A – authentication data is managed by the environmental Identity Store and not the TSF
[PM]ESM_EID.2	N/A – authentication data is managed by the environmental Identity Store and not the TSF
[PM]FAU_SEL.1	Configuration of auditable events
[PM]FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
[PM]FAU_STG_EXT.1	Configuration of external audit storage location
[PM]FIA_USB.1	Definition of subject security attributes, modification of subject security attributes
[PM]FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
[PM]FMT_MSA.1	Management of sets of subjects that can interact with security attributes
	Management of rules by which security attributes inherit specified values
[PM]FMT_MSA_EXT.5	N/A – the TSF automatically behaves in the secure manner defined by this SFR and this behavior is not configurable
[PM]FMT_SMR.1	Management of the users that belong to a particular role
[PM]FTA_TAB.1	N/A – this SFR was moved to selection-based as per NIAP TD0055 and has not been included within the scope of the TOE
[PM]FTP_ITC.1	N/A – the actions requiring the use of a trusted channel are not configurable once the TOE is in an operational state
[PM]FTP_TRP.1	N/A – the actions requiring the use of a trusted path are not configurable once the TOE is in an operational state

Table 6-4: Management Functions

6.3.7.2 [AC]FMT_MOF.1(1) Management of Functions Behavior

[AC]FMT_MOF.1.1(1) The TSF shall restrict the ability to [determine the behavior of, modify the behavior of] the functions: audited events, repository

for trusted audit storage, Access Control SFP, policy being implemented by the TSF, Access Control SFP behavior to enforce in the event of communications outage, [**no other functions**] to [an authorized and compatible Policy Management product].

6.3.7.3 [AC]FMT_MOF.1(2) Management of Functions Behavior

[AC]FMT_MOF.1.1(2) The TSF shall restrict the ability to query the behavior of the functions: policy being implemented by the TSF, [**no other functions**] to [an authorized and compatible Enterprise Security Management product].

6.3.7.4 [PM]FMT_MOF_EXT.1 External Management of Functions Behavior

[PM]FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the behavior of the functions of Access Control products: audited events, repository for remote audit storage, Access Control SFP, policy being implemented by the TSF, Access Control SFP behavior to enforce in the event of communications outage, [**no other functions**] to [

- **An OAM system administrator can configure the behavior of Webgates without limitation**
- **An OES system administrator can configure the behavior of Security Modules without limitation**
- **A domain administrator on either OAM or OES can only configure Webgates or Security Modules in the same domain that they are authorized to manage**].

6.3.7.5 [AC]FMT_MSA.1 Management of Security Attributes

[AC]FMT_MSA.1.1 The TSF shall enforce the access control SFP to restrict the ability to [change_default, query, modify, delete, [**create**]] the security attributes: access control policies, access control policy attributes, implementation status of access control policies to [an authorized and compatible Policy management Product].

6.3.7.6 [AC]FMT_MSA.3 Static Attribute Initialization

[AC]FMT_MSA.3.1 The TSF shall enforce the [access control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

[AC]FMT_MSA.3.2 The TSF shall allow the [authorized and compatible Policy Management product] to specify alternative initial values to override the default values when an object or information is

created.

6.3.7.7	*[PM]FMT_MSA_EXT.5*	*Consistent Security Attributes*
	[PM]FMT_MSA_EXT.5.1	The TSF shall [identify the following internal inconsistencies within a policy prior to distribution: [**different rules applying to the same subject/object pairing**]].
	[PM]FMT_MSA_EXT.5.2	The TSF shall take the following action when an inconsistency is detected: [issue a prompt for an administrator to manually resolve the inconsistency, [**no other action**]].

6.3.7.8	*[AC+PM]FMT_SMF.1*	*Security Management Functions*
	[AC+PM]FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [configuration of audited events, configuration of repository for trusted audit storage, configuration of Access Control SFP, querying of policy being implemented by the TSF, management of Access Control SFP behavior to enforce in the event of communications outage, [**management functions defined in Table 6-4**]].

6.3.7.9	*[AC+PM]FMT_SMR.1*	*Security Management Roles*
	[AC+PM]FMT_SMR.1.1	The TSF shall maintain the roles [**OAM Console system administrator, OAM Console domain administrator, OES Console system administrator, OES Console domain administrator**]**.**
	[AC+PM]FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.3.8 Class FPT: Protection of the TSF

6.3.8.1	*[AC+PM]FPT_APW_EXT.1*	*Protection of Stored Credentials*
	[AC+PM]FPT_APW_EXT.1.1	The TSF shall store credentials in non-plaintext form.
	[AC+PM]FPT_APW_EXT.1.2	The TSF shall prevent the reading of plaintext credentials.

6.3.8.2	*[AC]FPT_FLS_EXT.1*	*Failure of Communications*
	[AC]FPT_FLS_EXT.1.1	The TSF shall maintain policy enforcement in the following manner when the communication between the TSF and the Policy Management product encounters a failure state: [enforce the last policy received].

6.3.8.3	*[AC]FPT_RPL.1*	*Replay Detection*
	[AC]FPT_RPL.1.1	The TSF shall detect replay for the following entities: [**database**].

[AC]FPT_RPL.1.2 The TSF shall perform [**rejection of the information**] when replay is detected.

6.3.8.4 [AC+PM]FPT_SKP_EXT.1 Protection of Secret Key Parameters

[AC+PM]FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.3.9 Class FRU: Resource Utilization

6.3.9.1 [AC]FRU_FLT.1 Degraded Fault Tolerance

[AC]FRU_FLT.1.1 The TSF shall ensure the operation of [enforcing the most recent policy] when the following failures occur: [restoration of communications with the Policy Management product after an outage].

6.3.10 Class FTA: TOE Access

6.3.10.1 [AC]FTA_TSE.1 TOE Session Establishment

[AC]FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [day, time].

6.3.11 Class FTP: Trusted Path/Channels

6.3.11.1 [AC+PM]FTP_ITC.1 Inter-TSF Trusted Channel

[AC+PM]FTP_ITC.1.1 The TSF shall use [TLS] 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.

[AC+PM]FTP_ITC.1.2 The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

[AC+PM]FTP_ITC.1.3 Refinement: The TSF shall initiate communication via the trusted channel for *transfer of policy data*, [**remote storage of audit data, remote storage of configuration settings, communications from user applications to PEP/PDP, retrieval of identity data used to evaluate policy decisions**].

6.3.11.2 [PM]FTP_TRP.1 Trusted Path

[PM]FTP_TRP.1.1 The TSF shall *use* [HTTPS] to provide a *trusted* 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].
[PM]FTP_TRP.1.2	The TSF shall permit [remote users] to initiate communication via the trusted path.
[PM]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 PPs against which exact conformance 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 PPs.

Any references to "Access Control product" or "Policy Management product" that appear in the SFRs are considered to apply to the TSF since the TOE claims conformance to both PPs. The TSF implements both capabilities in a single product.

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 Profiles.

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 [PM]ESM_ACD.1:

Administrators of OAM Suite are able to define access control policies by using the graphical user interfaces (GUIs) provided by the OAM Server and OES Server. These interfaces are known as the OAM Console and OES Console. The OAM Suite is an integrated product that provides both Policy Management and Access Control capabilities, so there are no compatibility considerations for the ability to define policies. Every single operation that the Access Control component is capable of controlling is something that can be defined in a policy by the Policy Management component. Therefore, the subjects, objects, and operations against which a Webgate or Security Module is capable of controlling access is the same set of subjects, objects, and operations that can be defined in a policy by the OAM Console and OES Console. Information about the subjects, objects, and operations that the TSF can control access to is provided in section 8.5.

Each policy created by the TOE is uniquely identified. Webgate policies are identified by a unique name and each policy artifact is identified by a unique UID. This allows individual versions of the same policy to be differentiated from one another. Security Module policies are identified both by unique name and by sequential version number.

The TOE can apply different access policies to different web servers and applications. Multiple Webgates and Security Modules can be deployed to control access to the operational environment. Each of these PDPs can be associated with its own policy. The same web server/application can have both a Webgate and a Security Module protecting it so that the full range of access control functions can be enforced against a given resource in the operational environment.

8.1.2 [PM]ESM_ACT.1:

When an administrator on the OAM Console creates or modifies an access control policy, the policy data is immediately transmitted to the environmental RDBMS for future retrieval by the server. The relevant Webgates are notified that a policy change has occurred. The updated policy data is then queried by the Webgate when a user attempts to access a protected resource. The PDPs will also poll the server on a regular interval in the event that the notification was not received, or that the server was not available at the time the notification was received.

Access control policies are transmitted to Security Modules in a ‘push’ configuration, in which the OES Server will send updated policy data directly to the Security Module when the administrator presses the “Distribute” button on the OES Console.

All remote communications involved with this process (OAM/OES Server to PDP and OAM/OES Server to RDBMS) are secured using TLS.

8.1.3 [PM]ESM_ATD.1:

OAM Suite gives administrators the ability to associate TOE-defined attribute data with environmental objects in order to apply fine-grained access control policies to the operational environment.

For web servers that are protected by Webgates, an administrator can associate URL and file objects with a required authentication level. This allows the Webgate to enforce rules that check how a subject has authenticated to the operational environment and require them to provide additional authentication if their current authentication level does not match the level that is associated with a requested object.

Web applications that are protected by Security Modules have even more fine-grained attributes that can be applied to them. The TSF is able to define arbitrary attributes that can be applied to objects that exist within the protected web application. For example, an administrator that is using OAM Suite to protect resources on a WebLogic application can define an attribute called 'role' and associate objects defined by the application with various role attribute values to determine the sets of users that can interact with them.

8.1.4 [PM]ESM_ATD.2:

OAM Suite gives administrators the ability to associate TOE-defined attributes with subjects in order to apply fine-grained access control policies to the operational environment. Specifically, the OES Server is able to associate subjects that represent end users (defined in an Identity Store) with arbitrary administrator-defined attributes similar to what is described in **[PM]**ESM_ATD.1. Continuing the above example, an administrator could associate certain users with a role attribute so that when they attempt to access WebLogic resources that have the same attribute, the values of each object can be compared as part of evaluating whether or not the access attempt is allowed.

8.1.5 [PM]ESM_EAU.2:

Administrators who wish to access the OAM Server or OES Server in order to manage the TSF must be authenticated by the operational environment prior to being granted access to the TOE. The OAM and OES Server components define individual users who exist in the environmental Identity Store as administrators for the TOE. In the evaluated configuration, the Identity Store is an LDAP repository, either of Oracle Internet Directory (OID) or Oracle User Directory (OUD). The Identity Stores used for the OAM Server and OES Server are separately configurable; however, the same Identity Store is used for both interfaces in the evaluated configuration. Administrators will supply authentication credentials (username/password) to the TOE which then relays the authentication request to the Identity Store. The TOE then determines whether or not to allow administrative access to the TSF based on the LDAP response it receives. The TOE does not allow any ability for an administrator to perform management functions until they are authenticated.

8.1.6 [AC+PM]ESM_EID.2:

Both administrators who manage the TOE and end users who access objects that are protected by the TSF are identified by username data that is defined in the environmental Identity Store prior to any TSF-mediated actions being allowed. Administrators supply credentials to the OAM Server or OES Server for validation against the Identity Store. End users are also identified and authenticated by the Identity Store so that the TSF can identify subjects that are requesting access to protected objects. The environmental web servers or web applications are responsible for identifying and authenticating their users so that the TSF is able to enforce access controls against the proper subjects.

8.2 Security Audit

8.2.1 [AC+PM]FAU_GEN.1:

Audit data is generated by the TOE for both administrative activity and for access attempts made against environmental resources that are mediated by the TOE. The startup and shutdown of the TOE is logged as part of the function of the application servers on which the TOE components reside. Actions performed by administrators on the OAM Server and OES Server are logged to the RDBMS, as are records of Security Modules retrieving policy data from the RDBMS. Since Webgates query policy data from the RDBMS when user requests are performed, OAM auditing is all performed by the server component. Additional audit data is written to log files that reside on the environmental operating system where the TOE component is located. Audit log data includes, but is not limited to, date, time, and subject information (initiator), event type, event status, message text related to the event. The full list of auditable events is provided in Table 6-2.

8.2.2 [AC]FAU_SEL.1:

The events that are audited by OAM Suite's access control functionality are dependent on its configuration. The TSF has a configurable audit level with four settings: NONE, LOW, MEDIUM, and ALL. All user activity that is mediated by Webgates is audited when the TSF is configured at a log level of MEDIUM or ALL. Logging of cryptographic functionality on these components is configured on the system where they reside during installation and is not configurable from the GUI. In the evaluated configuration, auditing of cryptographic functionality is enabled when these components are configured.

By default, the Security Modules generate audit records for auditable events. While this can be configured by manually editing configuration files on the underlying OS platform, the default setting of generating all security-relevant audit data is defined by the evaluated configuration.

8.2.3 [PM]FAU_SEL.1:

All administrative activity on the OAM Server including administrator login, configuration changes, and policy changes are logged when the audit level is configured to be LOW, MEDIUM, or ALL.

By default, the OES Server generates audit records for auditable events. While this can be configured by manually editing configuration files on the underlying OS platform, the default setting of generating all security-relevant audit data is defined by the evaluated configuration.

8.2.4 [PM]FAU_SEL_EXT.1:

Administrators use the OAM Console to define the events that are logged by the Webgates. Because the TOE includes both Access Control and Policy Management components, the auditable events configuration that the OAM Console is are capable of is the same as what can be configured for the Webgate and Security Modules as described in **[AC+PM]**FAU_SEL.1.

8.2.5 [AC]FAU_STG.1:

Audit records that are generated by the TSF are transmitted to the underlying local file systems in the Operational Environment and are not stored within the TSF. Therefore, there is no TSF interface to modify or delete audit data that is stored there. This data is also transmitted to the RDBMS in the

evaluated configuration but the OAM Console and OES Console do not provide the ability to modify or delete audit data stored in this manner.

8.2.6 [AC+PM]FAU_STG_EXT.1:

All audit data that is recorded by the TSF gets written securely to the operational environment. Audit data that is generated by the Security Modules is recorded to the local file systems on which those components reside. This communications channel is local so there is no encryption for this. This data can be transmitted remotely from the local file system to the RDBMS but the security of this channel is the responsibility of the operational environment. All audit data that the OAM Console and OES Console generate is logged either to the local file system of their respective servers or to the RDBMS. Any audit data in the RDBMS is protected against unauthorized modification and deletion as there is no administrative method to manipulate this data once it has been stored. All communications between the TOE and the RDBMS use JDBC protected by TLS.

8.3 Communications

8.3.1 [AC]FCO_NRR.2:

When policies are defined and updated for consumption by Webgates and Security Modules (i.e. the PDPs that rely on this policy data to determine if requested access should be permitted), the TOE provides a mechanism to verify that they have been distributed and for an administrator to determine what policies are being implemented and to ensure that distribution of a new or updated policy was successful.

As part of setting up a Webgate, a unique ID and credentials are defined for it. Webgate policies are identifiable by a unique name and every policy is further given a unique UID so that different versions of the same policy can be differentiated from one another. An administrator is able to view the status of all of the Webgates that are deployed as part of the TOE. Each Webgate identifies the name and UID of the policy that is being implemented. Within a policy, rules are applied on a resource level, identified by a relative path. The Webgate's application domain includes a unique host identifier which identifies the absolute root path of the URL that the policy is applicable to. The combination of the host identifier and resource level of a given rule allows for unambiguous identification of the object the rule applies to.

During the initial installation and configuration of the Security Module, the administrator creates a new security module in the OES Console GUI with a unique name. The administrator then enrolls the installed Security Module with the unique name that was created in the OES Console as well as the specific server information (i.e. hostname and port number). Once the enrollment is complete, the SM is enrolled/attached to that specific OES Console.

In the evaluated configuration of the TOE, Security Modules are configured to receive updated policy data through a 'push' mechanism. In this configuration, policy changes are transmitted directly from the OES Console to the Security Module, which will return a receipt of the transaction. The Security Module sends notification back to the OES Console when new policy data is applied.

An administrator can also query a Security Module to determine the policy that it is currently enforcing. Policies are also identified by version number so if changes are being made to a policy, the administrator is able to determine which specific instance of the policy is currently applied.

8.4 Cryptographic Support

8.4.1 [AC+PM]FCS_CKM.1:

The TOE includes the RSA BSAFE Crypto-C Micro Edition version 4.1.2 cryptographic module, which is validated by FIPS 140-2 (CMVP certificate #2300). This cryptographic module implements FIPS-validated RSA key generation in accordance with FIPS 186-4 (CAVP RSA certificate #1850). This meets the key pair generation requirements of NIST SP 800-56B.

The TOE is conformant to Sections 5.9, 6.3.1, and 8 of NIST SP 800-56B. The TOE satisfies all operations marked as "Shall" and "Should". Additionally, all operations marked as "Shall Not" or "Should Not" are omitted from the implementation's functionality and the implementation does not contain any TOE-specific extensions.

8.4.2 [AC+PM]FCS_CKM_EXT.4:

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

8.4.3 [AC+PM]FCS_COP.1(1):

The RSA BSAFE cryptographic module that is included with the TOE implements FIPS-validated AES cryptography in accordance with NIST SP 800-38 (CAVP AES certificate #3596). In support of the TLS and HTTPS cryptographic functions used by the TSF to secure remote trusted channels and paths, the cryptographic module provides AES-CBC with 128-bit and 256-bit keys.

8.4.4 [AC+PM]FCS_COP.1(2):

The RSA BSAFE cryptographic module that is included with the TOE implements FIPS-validated RSA cryptography (CAVP RSA certificate #1850). In support of the TLS and HTTPS cryptographic functions used by the TSF to secure remote trusted channels and paths, the cryptographic module provides a FIPS 186-4 compliant implementation of RSA (which also meets FIPS 186-3) using a minimum modulus size of 2048 bits.

8.4.5 [AC+PM]FCS_COP.1(3):

The RSA BSAFE cryptographic module that is included with the TOE implements FIPS-validated hash functions in accordance with FIPS PUB 180-4 (CAVP SHS certificate #2958). In support of the TLS and HTTPS cryptographic functions used by the TSF to secure remote trusted channels and paths, the cryptographic module provides SHA-1 services.

8.4.6 [AC+PM]FCS_COP.1(4):

The RSA BSAFE cryptographic module that is included with the TOE implements FIPS-validated HMAC functions in accordance with FIPS PUB 198-1 (CAVP HMAC certificate #2293). In support of the TLS and HTTPS cryptographic functions used by the TSF to secure remote trusted channels and paths, the cryptographic module provides HMAC-SHA-1 services. The HMAC implementation supports all of (key size > block size, key size = block size, key size < block size) for all HMAC services.

8.4.7 [PM]FCS_HTTPS_EXT.1:

The TOE provides the ability for remote administrators to connect to the OAM Console and OES Console using HTTPS as specified in RFC 2818. This HTTPS implementation uses TLS as described in **[AC+PM]**FCS_TLS_EXT.1. When an administrator accesses the TOE using a web browser, the HTTPS connection is established through the web server (using RSA BSAFE) that is used by the TSF to serve web content remotely. Only after the HTTPS connection is established can the administrator supply authentication credentials to the TOE.

8.4.8 [AC+PM]FCS_RBG_EXT.1:

The RSA BSAFE Crypto CME v4.1.2 cryptographic module that is included with the TOE implements FIPS-validated DRBG functions (CAVP DRBG certificate #931). In support of the TLS and HTTPS cryptographic functions used by the TSF to secure remote trusted channels and paths, the cryptographic module provides a NIST SP 800-90A compliant HMAC-based DRBG. The DRBG is seeded by a third-party entropy source in the operational environment. In the evaluated configuration, the cryptographic module collects sufficient entropy to ensure at least 256 bits of strength for key generation.

8.4.9 [AC+PM]FCS_TLS_EXT.1:

The TOE provides the ability to encrypt remote communications using TLS 1.0 in conformance with RFC 2246 and TLS 1.1 in conformance with RFC 4346 by invoking the RSA BSAFE cryptographic module that is provided without modification as part of the TOE. TLS 1.1 is used for Identity Store communications; all other applications of TLS use TLS 1.0. The trusted channels and paths the TOE can use and the cryptographic modules that facilitate them are described in section 8.11. The TLS implementation provided by the TOE uses the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

8.5 User Data Protection

8.5.1 [AC]FDP_ACC.1:

Webgates and Security Modules are deployed to control access to a variety of objects on one or more web servers in the operational environment. The access control policies that are enforced by the TSF are made up of a collection of access control rules. These rules define the subject-object-operation combinations that are mediated by the TOE. Subjects as defined by the TOE's access control security function policy (SFP) are any organizationally-defined users that can be identified by a web server, objects are anything that is hosted on a web server (URLs, files, scripts, forms), and operations are any activities that a user would perform against these objects in the course of interacting with the web server (accessing a URL with an HTTP GET or POST request, downloading a file, executing a script, submitting a form, etc.).

A Webgate is a software agent that is installed on a web server, such as Oracle HTTP Server, where a web application resides. The Webgate is registered on the OAM Server and associated with the target application. The Webgate then intercepts HTTP requests bound for the application and evaluates the request against access control policies that it queries from the environmental RDBMS in order to determine if the access should be permitted.

A Security Module is an agent used to control access to an application, similar to a Webgate. The difference is that while Webgates are used to determine whether or not a resource identified by a URI can be identified, Security Modules operate at the application level and can therefore control the functions that a subject can perform within a given resource. Security Modules are configured by an administrator on the OES Console.

From a deployment standpoint, a Security Module can be responsible for intercepting access requests made against a web application or the web application can be written to directly request authorization checks from the Security Module using an API. In either case, the Security Module is acting as a policy decision point (PDP), but the decision can either be enforced directly by the Security Module or the calling application is assumed to be written in a way that it will take appropriate action based on the result returned to it by the Security Module.

8.5.2 [AC]FDP_ACF.1:

Webgates are deployed against web applications and used to control access to web page URLs and files that are stored on web servers. Webgates enforce access control rules known as authorization policies. Each authorization policy includes the following:

- Unique name
- Success and failure URLs (where the subject's browser is redirected based on the access control decision)
- List of objects to which the authorization policy applies

Additionally, an administrator can define specific conditions that must be fulfilled for a successful authorization result (such as supplying additional authentication data) and responses to be applied following a successful authorization.

When an administrator creates a Webgate, they specify a friendly name and password for it along with the base URL of the application that is to be protected. If the application to be protected is a J2EE WebLogic application, the creation of a Webgate also includes the deployment of a WebLogic Server Identity Assertion Provider (WLS IAP) component on the application. This is used by the TSF as an interface to a WebLogic application, which cannot communicate with a Webgate natively. The Webgate creation also allows protected resources and public resources to be specified. Protected resources are those that operate in a deny-by-default protection scheme and must be explicitly authorized by the TSF in order for a subject to be able to access them. Public resources are those that can be accessed by anyone without authorization. Both resource types are identifiable by one or more default URL prefixes. These can either be explicit URLs or groups of URLs that are identified by using wildcards ('…' for wildcards within a directory structure, '*' for all children of a given prefix).

When the Webgate is created, it automatically creates a Public Resource Policy and Protected Resource Policy. These are examples of authorization policies; additional authorization policies can be defined for

the Webgate if desired. Each authorization policy can consist of resources, conditions, rules, and responses, described as follows:

Resources: Identifies the URI(s) on the application that the authorization policy will apply to.

Conditions: Identifies the conditions of the access attempt that determine whether or not the policy applies. Conditions include the following:

- Identity – denotes that the authorization policy will apply to a user or group of users defined by the Identity Store and identified by the operational environment.
- IPv4 Range – denotes that the authorization policy will apply to a subject requesting access from one of a given set of IPv4 addresses.
- Temporal – denotes that the authorization policy will only apply on certain days and/or times.
- Attribute – denotes specific attributes that can be used to determine when the authorization policy will apply. This includes Identity Store attributes (such as an arbitrarily defined 'department' field), session attributes (has the subject been authenticated to the web application at a certain level), and attributes about the requested resource.

Rules: Rules determine whether or not access is allowed based on the conditions that are associated with the request. Each authorization policy has an allow rule and a deny rule. For each rule, an administrator can define the conditions that cause the access request to be governed by each rule. This can be defined in terms of an AND relationship or an OR relationship. For example, an authorization policy can be written such that a subject may access a web page only if they belong to a certain group AND they are accessing it from a certain time of day. Additionally, rules can be combined into logical expressions such that the final policy decision is based on a Boolean evaluation of each individual rule. For example, an expression (Rule1 AND Rule2) OR (Rule3 AND Rule4) could be written for four separate rules so that different combinations of observed conditions could result in access being granted.

OAM also provides a notion of step up authentication, where a user is attempting to access resources that are more sensitive than ones that they are currently authorized to access. Rather than being outright denied from accessing the resource, the TSF will provide an additional authentication challenge to determine whether the resource can be accessed. For example, a user may be authorized to access a particular resource using only username and password but another resource requires username, password, and correct answers to security questions. In this instance, the TSF would require the user to answer their security questions as a form of step up authentication to access the more sensitive resource.

Responses: Responses allow the Webgate to transmit specific information about an access attempt back to the web application that it intercepted the request from. For example, if the access request is authorized, the user's common name could be included in a response so that the application can present customized information to them. If the access request is not authorized, other user information could be returned for security purposes. The following responses are supported:

- Session count value
- User's ID
- User's IP address
- User's group memberships
- User's identity domain

- Attribute values belonging to user (defined in Identity Store)
- Attribute values belonging to session
- Current authentication level for the session
- Name of authentication scheme executed to achieve the current authentication level
- Session creation time
- Session expiration time
- Literal string

By default, if access is not explicitly allowed to an object that is protected by a Webgate, the access is denied. This is also true if the only applicable authorization policy rules are inconclusive because they evaluate to a contradictory result.

In general, rules will be evaluated such that more specific rules take priority over less specific ones. When rules with the same level of specificity have different results, the rule expression evaluates to inconclusive and the deny result takes precedence. The one exception to this is that authorization policies can be configured to process rules within a given policy in sequential order so that their precedence can be defined by administrators.

Security Modules are similar to Webgates in that they are deployed to determine what activities can be performed against resources in a web application. However, Security Modules provide a more fine-grained level of control by allowing an administrator to define authorizations for individual functions within an application. In other words, while a Webgate can be used to control access to a file or URL, Security Modules can be used to control access to runtime elements (such as executable scripts and forms) that belong to a given web application in order to control what a user can and cannot do once they have been authorized access to the application via the Webgate.

In order to have a Security Module enforce an access control policy against a web application, a Security Module of the correct type is first installed on the application's web server. The TSF includes a WebLogic Security Module, which can control access to Java, J2EE, and WebLogic applications.

Once a Security Module has been installed, an administrator uses the OES Console to configure its behavior. This involves the following steps:

- **Create an application:** A new application is defined within the OES console that identifies the application to be protected by a Security Module.
- **Create a resource type:** Depending on the application type, different types of resources can be defined as templates to be protected by authorization policies. The 'resource type' construct defines a generic type of resource (file, URL, etc.) and the actions that can be performed against it (such as GET and POST for a URL and read, write, copy, edit, and delete for a file). Administrators can also define arbitrary business objects and sequences of behaviors that constitute actions on these objects so that controlling access to objects can be done at an abstract level. For example, it is possible to define business logic activities for a financial application such as deposit, withdrawal, view account balance, and transfer to savings based on the underlying interactions with the application.
- **Create a resource:** Once a generic resource type has been defined, specific examples of that resource that are implemented in the application can be protected by authorization policies.

- **Create an authorization policy:** An authorization policy, just like for Webgates, is a rule or collection of rules that determines whether certain subjects can access a protected resource.
- **Create a Security Module definition and bind it to the application:** The administrator creates a logical association between the installed Security Module software, its abstract representation in the OES Console, and the abstract definition of the application it protects in the OES Console. This tells the Security Module what application it is protecting and what access control policies it will enforce to provide this protection.
- **Distribute the authorization policy to the security module:** The policy is written to the RDMBS and identifies the Security Module that it applies to and the correct Security Module will retrieve and apply it as part of the regular policy distribution process.

Authorization policies are the specific engine that a Security Module uses to determine if a requested operation is allowed. Each authorization policy will include the following components:

- **Principals:** the subject(s) that the authorization policy will apply to, identified by user, group (as defined by the Identity Store), or role (as defined by the application protected by the Security Module). The principal data is supplied by the calling application because this application will use the same Identity Store as the TOE and the subject will be identified by the operational environment as part of using the protected application.
- **Resources:** the object(s) that the authorization policy will apply to. These are defined with OES and map to components of the same name and type in the protected application.
- **Effect:** specifies whether a subject-object pairing that meets the conditions specified by the authorization policy will rely on access being granted or denied.

Optionally, an authorization policy may also contain the following elements:

- **Entitlements:** Rather than applying globally to all operations performed against a specific resource, specific entitlements can be defined if the authorization policy is only intended to control the ability of a subset of these entitlements. For example, an administrator may wish to prevent certain users from deleting WebLogic application objects while allowing the same users to create objects without restriction.
- **Conditions:** Similar to Webgates, Security Modules are able to apply Boolean logic to a set of rules to determine whether or not an access control request is valid.
- **Obligations:** Similar to Webgates, Security Modules are capable of specifying additional actions to be performed alongside returning the policy effect. This provides flexibility to protected applications by providing functions such as generating notifications if specific types of suspicious activity are observed.

As part of its policy evaluation process, a Security Module will evaluate all applicable authorization policies for a given request and will allow the requested access if and only if there is at least one authorization policy that results in access being granted and no authorization policies that result in access being denied.

8.6 Identification and Authentication

8.6.1 [PM]FIA_USB.1:

Once an administrator is authenticated to the TOE, they are provided with a session cookie that associates their web browser with the authenticated session. This session is uniquely identified so that the authenticated administrator is associated with only the data that applies to their own session. The administrator is defined in terms of username, role, and administrative scope so that only authorized actions can be performed against the TSF. The session then persists until it is timed out or manually terminated. If an administrator's attributes or the conditions that define these attributes are modified while that administrator is authenticated, their session will be terminated and they will be forced to re-authenticate in order for the updated permissions to take effect. This is true for both the OAM Console and OES Console interfaces.

8.7 Security Management

8.7.1 [PM]FMT_MOF.1:

The TSF provides the ability for administrators to configure Webgates and Security Modules as well as the ability to configure the OAM and OES Consoles. All administration is performed using the OAM and OES Consoles. The privilege model used by the TSF is straightforward: there exists one system administrator account for each of the OAM and OES Consoles that each have full authority to create and configure Webgates/Security Modules, define and assign privileges to new administrators, and to configure global characteristics of the administrative interfaces' behavior. Within each administrative interface, the system administrator has the ability to define domains and assign Webgates/Security Modules to these domains. They can then define domain administrators that are only able to administer policies within those domains. Domains can be further broken up into sub-domains, which can then have administrators assigned to them by either the system administrator or by a domain administrator with equal or greater scope.

8.7.2 [AC]FMT_MOF.1(1):

Through the OAM and OES Consoles, the TSF has the ability to configure and monitor the behavior of Webgates and Security Modules. Specifically, the TSF can configure the events that are audited by the Webgates and the access control policies that both they and the Security Modules enforce. The OAM and OES interfaces each define their own system administrator role. A system administrator for an interface can perform all security-relevant functionality on that particular interface. Each interface also provides the ability to define domain administrators, which are given only the ability to manage policies for resources associated to one or more domains assigned to that administrator. Since Webgates and Security Modules always enforce the last policy received in the event of a communications outage, the ability to manage the policies that they enforce also implicitly controls how they will behave when communications channels cannot be established. By default, the Webgates and Security Modules will log applicable audit data to the local file systems on which they are located and it is the responsibility of the operational environment to transmit this data beyond that.

8.7.3 [AC]FMT_MOF.1(2):

The TOE uses assurance of endpoints in order to ensure that communications between the OAM Server and Webgates and between the OES Server and Security Modules only occurs when they are authorized as part of the same deployment. Specifically, Webgates can define a credential during their registration.

When communications occur between the components, the credential will be validated so that an unauthorized management server or endpoint cannot be introduced into the deployment. Similarly, all components of the TOE all communicate with the same RDBMS. It is not possible for a second instance of an OAM Server or OES Server to communicate with this database, so the Webgates and Security Modules have assurance that any changes made to the database are genuine.

8.7.4 [PM]FMT_MOF_EXT.1:

The functions a Policy Management component is required to modify for an Access Control component are identical to the set of functions defined in [AC]FMT_MOF.1(1) and [AC]FMT_MOF.1(2). Refer to sections 8.7.2 and 8.7.3 above for the administration functions the TSF is capable of performing against its access control enforcement capability and the roles that are privileged to administer those functions.

8.7.5 [AC]FMT_MSA.1:

The RDBMS used by the TOE is unique for each instance of the product. Therefore, an administrator using the OAM Console or OES Console to query or modify a Webgate or Security Module is interacting with a database that cannot be accessed by any components other than those that belong to the TOE. This ensures that any configuration of Webgates and Security Modules is done by an authorized instance of the TOE. Since the TOE is provided as a single product that implements both access control and policy management functions, there are no compatibility concerns.

8.7.6 [AC]FMT_MSA.3:

By default, the TOE implements a restrictive access control policy against objects that are defined to be protected. If no policy exists for an object, it is out of scope of the TOE as the TSF is not aware that the object exists. Administrators can opt to define access control rules for these objects that are more permissive in nature, either by explicitly allowing access to certain subjects based on certain conditions, or by excluding some operations from enforcement.

8.7.7 [PM]FMT_MSA_EXT.5:

The OAM Console and OES Console interfaces both protect against inconclusive policy evaluations by providing the ability to prevent or reconcile potentially conflicting rule results.

Contradictory rules are resolved in the following manner by OAM Console/Webgates:

- When an administrator defines an authorization policy, the presence of explicitly contradictory rules (e.g. the same subject-object-operation combination at the same level of detail results in both a permit and a deny result) will prevent the policy from being saved.
- If an authorization policy contains implicitly contradictory rules at the same level of detail (e.g. a subject belongs to one group that is allowed access to an object but also belongs to a second group that is not allowed access to the same object), the authorization policy will evaluate to ‘inconclusive’, which is treated as a deny.
- If an authorization policy contains implicitly contradictory rules at differing levels of detail (e.g. a subject is allowed access to an object individually but also belongs to a group that is not allowed access to the same object), the more specific rule will take precedence.

- If OAM is configured to process authorization policy rules in order, then it is not possible for there to be contradictory rules because the higher rule will always take precedence.

Contradictory rules are resolved in the following manner by OES Console/Security Modules:

- In the event of contradictory rules, the deny rule will always take precedence.
- If an authorization policy does not have sufficient information to be evaluated, the deny rule will be enforced

In addition to this, the OES Console provides a policy simulator option where a user-resource-action combination can be specified and the authorization decision of that hypothetical behavior is returned so that the administrator can see the impacts of a policy before it is implemented.

8.7.8 [AC+PM]FMT_SMF.1:

The OAM Suite TOE includes both the OAM Console and OES Console as Policy Management interfaces and Webgates and Security Modules as Access Control interfaces. The OAM Console and OES Console are not general-purpose policy management products; they are used specifically to administer Webgates and Security Modules. Likewise, in the evaluated configuration, Webgates and Security Modules are only managed by the OAM Console and OES Console components, respectively.

As described in section 8.7.1, the TSF provides administrators with the ability to manage the behavior of Webgates and Security Modules (which from the perspective of the PM PP are synonymous with 'Access Control product') as well as the behavior of the administrative interfaces. Some management functions are not applicable because the TSF enforces the behavior required by the SFR without the need for configuration. The following management functions are defined by the PP and accompanied with a description of how either the TSF implements the function or its management is not applicable to the TOE:

- **Configuration of audited events:** administrators can configure what is logged by Webgates and Security Modules
- **Configuration of repository for trusted audit storage:** administrators can configure whether administrative activity is logged to the RDBMS
- **Configuration of Access Control SFP:** administrators can define access control policies and apply them to Webgates/Security Modules
- **Querying of policy being implemented by the TSF:** administrators can check the status of Webgates/Security modules to see what policies are applied and what rules are contained within those policies
- **Management of Access Control SFP behavior to enforce in the event of a communications outage:** N/A – the TSF implements a secure behavior by default and this is not configurable
- **Creation of policies:** see "configuration of Access Control SFP"
- **Transmission of policies:** see "configuration of Access Control SFP"
- **Association of attributes with objects:** as part of policy configuration, the TSF can associate TOE-defined attribute values with individual objects so that fine-grained access control policies can be defined based on these attributes

- **Association of attributes with subjects:** the TSF can supplement organizational user definitions with TOE-defined attribute values so that fine-grained access control policies can be defined based on these attributes
- **Configuration of auditable events for defined external entities:** see "configuration of audited events"
- **Configuration of external audit storage location:** see "configuration of repository for trusted audit storage"
- **Definition of subject security attributes, modification of subject security attributes:** the TSF can be used to assign privileges to administrative accounts
- **Configuration of the behavior of other ESM products:** see "configuration of Access Control SFP"
- **Management of sets of subjects that can interact with security attributes:** see "definition of subject security attributes, modification of subject security attributes"
- **Management of rules by which security attributes inherit specified values:** see "definition of subject security attributes, modification of subject security attributes"
- **Management of the users that belong to a particular role:** see "definition of subject security attributes, modification of subject security attributes"

8.7.9 [AC+PM]FMT_SMR.1:

The OAM Console and OES Console each define their own sets of administrators. Both interfaces to the TOE use the same Identity Store for administrator identification and authentication so it is possible to replicate permissions for each interface to the same sets of administrators. Each interface defines its own system administrator that has full control over the TSF. Additionally, the ability to interact with Webgates/Security Modules can be granted to domain administrators by associating those components with specific domains. These administrators then have authority over all Webgates or Security Modules within their domain. Additionally, domain administrators can create sub-domains and assign domain administrators to them.

8.8 Protection of the TSF

8.8.1 [AC+PM]FPT_APW_EXT.1:

The TOE uses identity and credential data that is defined in the operational environment in order to authenticate administrators and to identify end users. This data is not persistently stored by the TOE or retained by the TSF after an authentication attempt has been made, so there is no dedicated interface to the TOE that can be used to disclose administrator credential data.

8.8.2 [AC]FPT_FLS_EXT.1:

Once a Webgate has made a decision based on a policy defined by the OAM Server, it will continue to enforce that decision for subsequent requests until a new policy is made available for its use that would override this. If the Webgate has not made a decision on a particular type of request and the server cannot be reached to retrieve relevant policy data, the request will be denied by default. Once a Security Module has received a policy from the OES Server, it will continue to enforce that policy until the OES Server has pushed a new or updated policy to it. Therefore, any disruption in communications between a Webgate or

Security Module and the rest of the TOE will not have an effect on the enforcement of the access control SFP.

8.8.3 [AC]FPT_RPL.1:

The TSF provides several mechanisms for preventing the consumption of malicious or otherwise unintended policies. First, the only mechanism that can be used to update policy data on the Webgates and Security Modules is the OAM/OES Server. Simply transmitting spoofed policy data to the PDP without any authorized trigger from the server will cause the data to be rejected. Direct manipulation of the policy data at rest in the RDBMS is not possible due to the fact that it is locked down from unauthorized interactive access. Finally, any legitimate policy data in transit between the server components and the PDPs is secured using TLS so it is not possible for an attacker to spoof the transfer of legitimate data using an existing connection between the server and the PDP.

8.8.4 [AC+PM]FPT_SKP_EXT.1:

The TOE provides no interface to view secret key data. The cryptographic data used by the TOE is protected against unauthorized disclosure by the FIPS-compliant cryptographic module that is used by the TOE to secure remote communications. The Security Policy documentation for this module identifies the keys and cryptographic parameters that are protected by the cryptographic module. Additionally, key data that is stored alongside Webgates that is used to establish trusted communications back to the OAM Server are encrypted with 256-bit AES.

8.9 Resource Utilization

8.9.1 [AC]FRU_FLT.1:

A Webgate or Security Module will enforce decisions it has previously made or whatever policy it currently has regardless of whether or not it is able to communicate with the server components of the TOE. If communications between the Webgate or Security Module and their respective server components fail, the Webgate or Security Module will periodically attempt to query the server in order to determine whether or not updated policy information is available. This allows the most recent policy to be enforced within a reasonable period of time once a communications outage is resolved.

8.10 TOE Access

8.10.1 [AC]FTA_TSE.1:

As part of its access control policy enforcement, a Webgate can enforce denial of session establishment by limiting a subject's access to a protected resource based on day or time. If a rule exists to prevent access to a web page during a given time window, a subject's attempt to access the resource will be rejected even if the TOE is able to validate their identity (due to them having provided correct authentication credentials and being authenticated by the Identity Store).

8.11 Trusted Path/Channels

8.11.1 [AC+PM]FTP_ITC.1:

The TOE uses a third-party cryptographic module, RSA BSAFE Crypto-C Micro Edition version 4.1.2, to implement trusted channels between distributed systems using TLS. The cryptographic module is FIPS 140-2 validated (certificate #2097) and included in OAM Suite by Oracle without modification. The following trusted channels are established by the TOE:

- **OAM Server/OES Server to RDBMS** – used to transmit and store TSF management data, policy data, and audit data for administrator activities.
- **OAM Server/OES Server to Identity Stor**e – used to validate administrator authentication attempts and to collect administrative identity data when needed by the administrative consoles.
- **Security Module (PEP/PDP) to RDBMS** – used to transmit audit data generated by the Security Module for persistent storage.
- **Webgate/Security Module (PEP/PDP) to Identity Store** – used to retrieve additional identity data about a subject if it is needed to perform an access control decision.
- **OAM Server to Webgate (PEP/PDP) –** used to notify Webgates when updated policy or configuration information is available for retrieval from the RDBMS. For cases where the WLS IAP is required for compatibility purposes, this same interface is used but the OAM Server connects to the WLS IAP as an intermediary.

8.11.2 [PM]FTP_TRP.1:

The TOE uses a third-party cryptographic module, RSA BSAFE Crypto-C Micro Edition version 4.1.2, to implement trusted paths from a remote administrator to the OAM Console and OES Console using HTTPS. The cryptographic module is FIPS 140-2 validated (certificate #2097) and included in OAM Suite by Oracle without modification.