Oracle Access Management 12c

Security Target

Version 2.0

September 2023

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
1.0	2 Dec 2021	Addressed CB ORs.
1.1	7 Jan 2022	Addressed CB ORs.
1.2	31 Mar 2022	Corrections to the role of WebGates. Revise ECD.
1.3	2 May 2022	Additional clarifications and restructure of the TSS.
1.4	27 Sept 2022	Addressed evaluator ORs.
1.5	11 Jan 2023	Updated TOE version and identification.
1.6	5 June 2023	Addressed evaluator ORs.
1.7	19 June 2023	Updated interfaces.
1.8	27 June 2023	Addressed certifier comments.
1.9	27 July 2023	Corrected TOE version identifier. Addressed CBORs.
2.0	19 September 2023	Updated AGD version.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

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

2 Oracle Access Management (OAM) is an Enterprise Security Management (ESM) product that controls access to web resources. It enforces administrator-configurable rules ensuring that resources are protected from unauthorized access.

3 The TOE includes a policy management function that is used to configure the access control policies that are applied to these web resources. 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 resources based on user attributes that are organizationally defined.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Oracle Access Management 12.2.1.4 with patches 35371374 and 33974688
Security Target	Oracle Access Management 12c Security Target, v2.0

1.3 Conformance Claims

4 This ST supports the following conformance claims:

a) CC version 3.1 revision 5

i) CC Part 2 extended

ii) CC Part 3 conformant

b) Standard Protection Profile for Enterprise Security Management Policy Management (PP_ESM_PM), v2.1

c) Standard Protection Profile for Enterprise Security Management Access Control (PP_ESM_AC), v2.1

d) NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name
TD0042	Removal of Low-level Crypto Failure Audit from PPs
TD0055	Move FTA_TAB.1 to Selection-Based Requirement
TD0066	Clarification of FAU_STG_EXT.1 Requirement in ESM PPs
TD0079	RBG Cryptographic Transitions per NIST SP 800-131A Revision 1

TD #	Name
TD0573	Update to FCS_COP and FCS_CKM in ESM PPs
TD0574	Update to FCS_SSH in ESM PPs
TD0576	FTP_ITC and FTP_TRP Updated
TD0621	Corrections to FCS_TLS_EXT.1 in ESM PPs

1.4 Terminology

Table 3: Terminology

Term	Definition
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation. In this case, Oracle Solaris.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in a ST.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.

2 TOE Description

2.1 Type

5 The TOE is an enterprise web access control and policy management solution.

2.2 Usage

6 The TOE, shown in the green boxes below is deployed to allow administrators to define access control polices over user access to web resources.

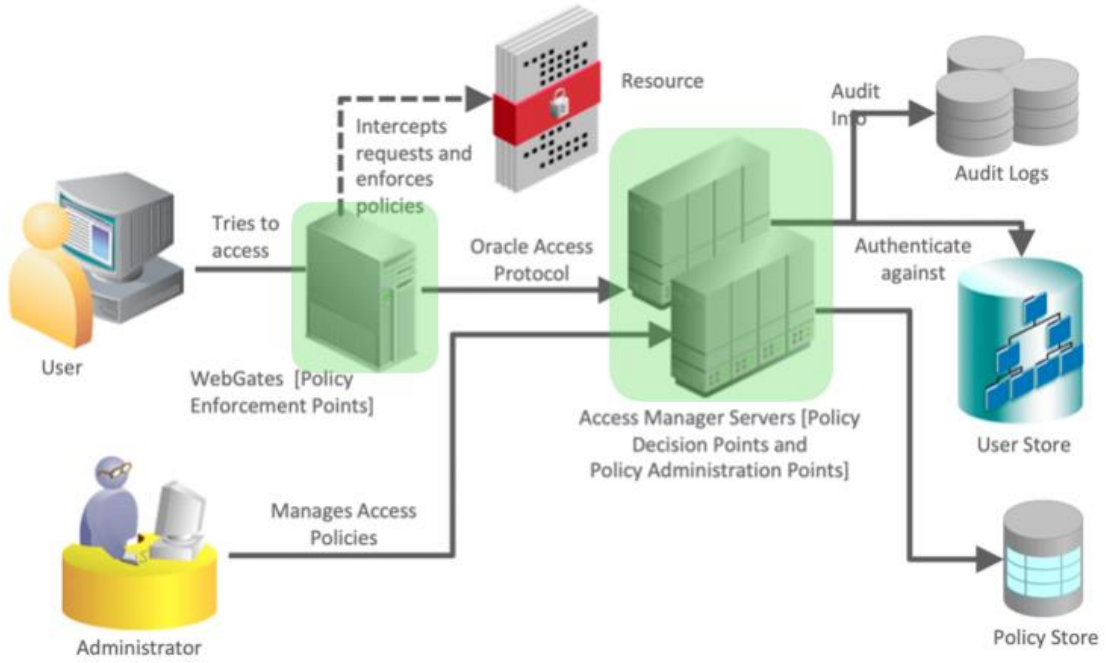

Figure 1: TOE Usage Example

7 To come under access control, a web server, application server, or third-party application must be protected by an OAM WebGate that is registered as an agent with the OAM Server. Administrators define authentication and authorization policies via the OAM Console to protect the resource. To enforce these policies, the WebGate acts as a filter for HTTP requests.

8 Communication with remote administrators and between components is protected by TLS.

2.3 Architecture

9 Key architectural components of the TOE (refer to section 2.5.3 for underlying system requirements):

a) **OAM Server.** The Policy Decision Point. The OAM Server is deployed on an instance of Oracle WebLogic Server. The OAM Server retrieves policy data from the Policy Store, evaluates access requests from WebGates and responds with policy decisions for enforcement.

b) **OAM Console.** The Policy Administration Point - a management Web GUI for configuration and policy definition. Deployed on a WebLogic Administration Server. The OAM Console is itself protected by a dedicated OAM WebGate. The OAM Console transmits policy data to the Policy Store.

c) **OAM WebGate.** The Policy Enforcement Point(s) that intercept HTTP requests to enforce access decisions. OAM WebGate(s) are deployed on Oracle HTTP Servers (web server).

10 Key architectural components in the TOE environment (refer to section 2.5.3 for underlying system requirements):

a) **Audit Store.** Database for audit records.

b) **Policy Store.** Database for policies.

c) **Identity Store.** Directory for enterprise identities.

2.4 Logical Scope

2.4.1 Access Control Policy Definition

11 The OAM Console allows the TOE administrator to define policies to enforce access control over web resources (URLs).

12 The OAM Console transmits policies to the OAM Server via the Policy Store.

13 The OAM Console protects against inconclusive policy evaluations by providing the ability to prevent or reconcile potentially conflicting rules.

14 The OAM Console uniquely identifies the policies it creates.

2.4.2 Access Control Policy Enforcement

15 The OAM Server and OAM WebGate components work together to enforce the policies defined via the OAM Console.

16 The OAM Server retrieves policy data from the Policy Store, evaluates access requests from the OAM WebGates and responds with policy decisions for enforcement.

17 OAM WebGates are deployed on web servers that contain the URL defined resources under access control. OAM WebGates intercept requests to access protected resources, asks the OAM Server for a policy decision and subsequently enforces the decision.

2.4.3 Policy Security

18 The TOE protects the integrity and confidentiality of policy data transmitted between components. Policy data flow is as follows:

a) Administrator (web browser) to OAM Console via the OAM Console's dedicated WebGate:

   i) Communications with remote administrators are protected via HTTPS

   ii) Communications between the OAM Console and OAM Console WebGate are protected via TLS

b) OAM Console to OAM Server via Policy Store – communications with the Policy Store are protected via TLS

c) OAM Server to WebGate (policy decisions) – communications are protected via TLS

19 By using HTTPS/TLS, the TOE is immunized against replay attacks.

20 The TOE generates an audit record when policies are created or changed, providing evidence of receipt of policies.

2.4.4 Security Audit

21 The TOE generates records of auditable events which are logged to the environmental Audit Store and also stored on the local filesystem of the component that generated the event. Any audit data that is transmitted remotely from the TOE to the Operational Environment is secured using TLS.

22 An administrator can configure the types of events for which logs are generated for both administrator and end user activities for OAM Console, OAM Server and WebGate activities. Once generated, audit data is stored in a manner that prevents unauthorized modification or deletion.

2.4.5 Secure Administration

23 Administrators manage the TOE security functions via the OAM Console. The TOE has the following secure administration capabilities:

a) The TOE enforces role-based access control to restrict access to management functions

b) Administrators are authenticated against an external LDAP server

c) Administrator sessions are uniquely identified and securely managed

d) It is not possible to view secret keys via the OAM Console

e) Remote administrator communications are protected via HTTPS

2.4.6 Continuity of Enforcement

24 The TOE will deny all access requests in the event of a communication outage between components.

25 The TOE will retrieve the latest policy from the Policy Store following the restoration of communications in the event of an outage.

2.4.7 Cryptographic Support

26 The TOE's cryptographic capabilities are provided by RSA BSAFE cryptographic modules in the TOE's operational environment.

2.5 Physical Scope

2.5.1 Software

27 The TOE is the following software, and may be downloaded by users from the identified links:

a) Oracle Access Management 12.2.1.4.0 with patch 35371374

https://www.oracle.com/security/identity-management/technologies/downloads/

b) Oracle WebGate 12.2.1.4.0 with patch 33974688

https://support.oracle.com

2.5.2 Guidance Documents

28 The TOE includes the following guidance documents:

a) [CC Guide] - Oracle Access Management 12c Common Criteria Guide, v1.6 (PDF) - https://www.oracle.com/corporate/security-practices/assurance/development/external-security-evaluations/common-criteria/certifications.html

b) [Info] - Oracle Access Management 12c Information Library - https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.4/aiaag/introducing-oracle-access-management.html

29 **Note**: Oracle support personnel should be consulted for the provisioning of the TOE.

2.5.3 Non-TOE Components

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

Table 4: Non-TOE Components

Component	Details
OAM Server & Console – Platform Requirements	• Oracle Linux 7.6 UEK 5 • Oracle WebLogic Server 12c • Oracle JRE 8
OAM WebGate – Platform Requirements	• Oracle HTTP Server 12c • Oracle Linux 7.6 UEK 5
Audit Store	Oracle Database 19c
Policy Store	Oracle Database 19c
Identity Store	Oracle Unified Directory / Oracle Internet Directory 12c
OAM Console Identity Store	LDAPv3 directory server
Administrator System	Web Browser
User System	Web Browser

31 The minimum system requirements for the components identified in Table 4 can be found online at: https://www.oracle.com/middleware/technologies/internet-application-server/fusion-requirements-and-specifications.html.

2.6 Excluded Functionality

32 This CC evaluation only covers the functionality identified in section 2.4 when the TOE is configured in accordance with [CC Guide]. Although OAM can be deployed in a Cloud, Docker and Kubernetes environments, only an on-premise environment was tested.

3 Security Problem Definition

33 The Security Problem Definition is reproduced from the claimed PPs.

3.1 Threats

Table 5: PP_ESM_PM Threats

Identifier	Description
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.CONTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FORGE	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.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
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 6: PP_ESM_AC Threats

Identifier	Description
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.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
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.

Identifier	Description
T.FORGE	A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
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.
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.
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.

3.2 Assumptions

Table 7: PP_ESM_PM Assumptions

Identifier	Description
A.CRYPTO (optional)	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.
A.POLICY	The TOE will receive policy data from the Operational Environment.
A.ROBUST (optional)	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME (optional)	The TOE will receive reliable time data from the Operational Environment.
A.USERID	The TOE will receive identity data from the Operational Environment.

Table 8: PP_ESM_AC Assumptions

Identifier	Description
A.CRYPTO (optional)	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.

Identifier	Description
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.POLICY	The TOE will receive policy data from the Operational Environment.
A.ROBUST (optional)	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME (optional)	The TOE will receive reliable time data from the Operational Environment.
A.USERID	The TOE will receive identity data from the Operational Environment.
A.INSTALL	There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.

3.3 Organizational Security Policies

Table 9: PP_ESM_PM OSPs

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

Table 10: PP_ESM_AC OSPs

Identifier	Description
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

4 Security Objectives

34 The security objectives are reproduced from the claimed PPs.

4.1 Security Objectives for the TOE

Table 11: PP_ESM_PM Security Objectives for the TOE

Identifier	Description
O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.

Identifier	Description
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.
O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
O.INTEGRITY	The TOE will contain the ability to assert the integrity of policy data.
O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
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.
O.PROTCOMMS	The TOE will provide protected communication channels or administrators, other parts of a distributed TOE, and authorized IT entities.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

Table 12: PP_ESM_AC Security Objectives for the TOE

Identifier	Description
O.DATAPROT	The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
O.INTEGRITY	The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.
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.
O.MNGRID	The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.

Identifier	Description
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).
O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.SELFID	The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.

4.2 Security Objectives for the Operational Environment

Table 13: PP_ESM_PM Security Objectives for the Operational Environment

Identifier	Description
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.
OE.CRYPTO (optional)	The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
OE.ROBUST (optional)	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME (optional)	The Operational Environment will provide reliable time data to the TOE.
OE.USERID	The Operational Environment shall be able to identify a user requesting access to the TOE.

Table 14: PP_ESM_AC Security Objectives for the Operational Environment

Identifier	Description
OE.CRYPTO (optional)	The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.POLICY	The Operational Environment will provide a policy that the TOE will enforce.
OE.PROTECT (optional)	The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.
OE.USERID	The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.

5 Security Requirements

5.1 Conventions

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

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

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

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

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

e) **Iteration.** Indicated by adding a string starting with “/” (e.g. “FCS_COP.1/Hash”).

36 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:

a) 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.

b) 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.

c) 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].

5.2 Extended Components Definition

37 Table 15 identifies the Extended Components used in this ST, their source PP and any related Technical Decisions.

Table 15: Extended Components

Extended SFR	Source PP	Technical Decisions
ESM_ACD.1	PP_ESM_PM	
ESM_ACT.1	PP_ESM_PM	
ESM_ATD.1	PP_ESM_PM	
ESM_EAU.2	PP_ESM_PM	
ESM_EID.2	PP_ESM_PM PP_ESM_AC	
FAU_SEL_EXT.1	PP_ESM_PM	

Extended SFR	Source PP	Technical Decisions
FAU_STG_EXT.1	PP_ESM_PM PP_ESM_AC	TD0066
FCS_HTTPS_EXT.1	PP_ESM_PM	TD0621
FCS_TLS_EXT.1	PP_ESM_PM PP_ESM_AC	TD0621
FMT_MOF_EXT.1	PP_ESM_PM	
FMT_MSA_EXT.5	PP_ESM_PM	
FPT_APW_EXT.1	PP_ESM_PM PP_ESM_AC	
FPT_FLS_EXT.1	PP_ESM_AC	
FPT_SKP_EXT.1	PP_ESM_PM PP_ESM_AC	

5.3 Functional Requirements

Table 16: Summary of SFRs

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_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	[PM]FCS_HTTPS_EXT.1	HTTPS
	[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

Class Name	Component Identification	Component Name
	[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	TOE Session Establishment
Trusted Path /Channels	[AC+PM]FTP_ITC.1	Inter-TSF Trusted Channel
	[PM]FTP_TRP.1	Trusted Path

5.3.1 Class ESM: Enterprise Security Management

[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*]; and
- Operations: [*allow or deny access*]; 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.

[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].

[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.

Application Note: As per Appendix C in [PP_ESM_PM], Section C.1 – Attribute Definition, the source of authoritative subject attribute data is maintained by the LDAP (OUD) in the Operational Environment. The TOE does not maintain any subject attributes, therefore ESM_ATD.2 is not claimed.

[PM]ESM_EAU.2 Reliance on Enterprise Authentication

[PM]ESM_EAU.2.1 The TSF shall rely on [*[LDAP 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.

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

[AC+PM]ESM_EID.2.1 The TSF shall rely on [[*LDAP (OID) 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.

5.3.2 Class FAU: Security Audit

[AC+PM]FAU_GEN.1Audit 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 17 for the not specified level of audit; and

c) [*no other auditable events*].

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

Table 17: Auditable Events

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	Definition of object attributes	Identification of the attribute defined
	Association of attributes with objects	Identification of the object and the attribute
[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
[PM]FCS_HTTPS_EXT.1	Failure to establish a session, Establishment/termination of a session	Non-TOE endpoint of connection (IP address), Reason for failure (if applicable)
[AC+PM]FCS_TLS_EXT.1	Failure to establish a session, Establishment/termination of a session	Non-TOE endpoint of connection (IP address), Reason for failure (if applicable)
[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
[AC]FMT_MOF.1	All modifications to TSF behavior	None
[AC+PM]FMT_SMF.1	Use of the management functions	Management function performed

Component	Event	Additional Information
[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

[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, [*additional information in Table 17*].

[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:

- [event type]; and
- [*no other attributes*]

[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:

- [event type]; and
- [*no other attributes*]

[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:

- [event type]; and
- [no other attributes].

[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.

[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 [*Audit Store*].

[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 (Audit Store and platform file system).

5.3.3 Class FCO: Communications

[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 [*Hostname, IP address*] of the recipient of the information, and the [*policy ID*] 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 [*60 seconds*].

5.3.4 Class FCS: Cryptographic Support

[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.

[AC+PM]FCS_TLS_EXT.1 TLS

[AC+PM]FCS_TLS_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and [no earlier TLS versions] that supports the cipher suites: [

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289].

Application Note: This SFR is updated in accordance with TD0621.

5.3.5 Class FDP: User Data Protection

[AC]FDP_ACC.1 Access Control Policy

[AC]FDP_ACC.1.1 The TSF shall enforce the [*access control SFP*] on [

- *Subjects: subset of users from an organizational data store; and*
- *Objects: URLs; and*
- *Operations: allow or deny access*]

[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 below table based upon administrator defined set of organizational attributes*].

Subject	Object	Operation
User	URL File Executable Script	Allow Access Deny Access

[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: [

- *WebGates are applied to web applications in the Operational Environment*
- *Authorization policies are applied to URIs that are contained within 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*

].

[AC]FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based of the following additional rules: [*none*].

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

5.3.6 Class FIA: Identification and Authentication

[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: [*changes take effect on next login*].

5.3.7 Class FMT: Security Management

[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 18*] to [*authorized roles with the following conditions:*

- *Super 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 if a super 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.

Table 18: Management Activities

SFR	Management Activity
[PM]ESM_ACD.1	Creation of policies
[PM]ESM_ACT.1	Transmission of policies
[PM]ESM_ATD.1	Definition of object attributes
	Association of attributes with objects
[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

SFR	Management Activity
[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
[AC]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

[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*].

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

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

[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 super administrator can configure the behavior of the OAM Server and WebGates without limitation*
- *A domain administrator can only configure policies in the same domain that they are authorized to manage]*.

[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].*

[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.

[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: [*[prevent the policy from being saved, deny subject access to the object, allow subject access to the object based on rule precedence]*].

[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 18]*.

[AC+PM]FMT_SMR.1 Security Management Roles

[AC+PM]FMT_SMR.1.1 The TSF shall maintain the roles *[super administrator, domain administrator]*.

[AC+PM]FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.3.8 Class FPT: Protection of the TSF

[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.

[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: [deny all requests].

[AC]FPT_RPL.1 Replay Detection

[AC]FPT_RPL.1.1 The TSF shall detect replay for the following entities: *[OAM Server].*

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

[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.

5.3.9 Class FRU: Resource Utilization

[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].*

5.3.10 Class FTA: TOE Access

[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]*.

5.3.11 Class FTP: Trusted Path/Channels

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

[AC+PM]FTP_ITC.1.1 The TSF shall be capable of using [TLS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [audit server, authentication server, [*OAM server, OAM console, OAM WebGates, OAM Authentication Protocol, policy store, user endpoints*]] that is logically distinct from other

communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

Application Note: OAM server, OAM console, OAM WebGates, and OAM Authentication Protocol are included in this SFR in accordance with PP application notes stating: *If the TOE claims conformance to multiple PPs, remote interfaces to distributed components of the TOE must be claimed here and evaluated as if they were interfaces to the Operational Environment.*

[AC+PM]FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

[AC+PM]FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for transfer of policy data, [*transfer of audit data, authentication, retrieval of identity data used to evaluate policy decisions*].

Application Note: This SFR is altered by TD0576.

[PM]FTP_TRP.1 Trusted Path

[PM]FTP_TRP.1 The TSF shall be capable of using [HTTPS] to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identifications of its end points and protection of the communicated data from modification, disclosure, and [no other types of integrity or confidentiality violations].

[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 and execution of management functions.

Application Note: This SFR is altered by TD0576.

5.4 Assurance Requirements

5.4.1 Summary of Requirements

38 The TOE security assurance requirements are summarized in Table 19.

Table 19: Assurance Requirements

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

6 TOE Summary Specification

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

6.1 Access Control Policy Definition

6.1.1 [PM]ESM_ACD.1

40 Administrators define access control policies via the OAM Console. The TOE 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 is capable of controlling access to is the same set of subjects, objects, and operations that can be defined in a policy by the OAM Console.

41 Each policy created by the TOE is uniquely identified. Policies are identified by a unique name and each policy artifact is identified by a unique Policy ID.

42 The TOE can apply different access policies to different web servers and applications. Multiple WebGates can be deployed to control access to the operational environment. Policies can be applied to one or more WebGates.

6.1.2 [PM]ESM_ATD.1

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

44 An administrator can associate URL and file objects with a required authentication level. The URL is configured in two parts: the host identifier which provides the domain name, and the resource identifier which provides the path to a specific resource. This allows the TOE 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.

6.1.3 [PM]FMT_MOF.1 & [PM]FMT_MOF_EXT.1

45 All TOE administration is performed using the OAM Console. The privilege model used by the TSF is straightforward: there exists one super administrator account which has authority to create/register and configure WebGates, define and assign privileges to new administrators, and to configure global characteristics of the administrative interfaces' behavior.

46 Within the administrative interface, the super administrator has the ability to define domains and assign WebGates 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 super administrator or by a domain administrator with equal or greater scope.

6.1.4 [PM]FMT_MSA_EXT.5

47 The OAM Console protects against inconclusive policy evaluations by providing the ability to prevent or reconcile potentially conflicting rule results.

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

a) 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.

b) 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.

c) 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.

d) 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.

6.2 Access Control Policy Enforcement

6.2.1 [AC]FDP_ACC.1

49 The OAM Server, working with deployed WebGates controls 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), and operations are allow or deny access to activities that a user would perform against these objects in the course of interacting with the web server.

50 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 asks the OAM Server for a policy decision which the WebGate will then enforce.

6.2.2 [AC]FDP_ACF.1

51 WebGates are deployed against web applications to enforce access control decisions for web page URLs and files that are stored on web servers. The OAM Server and WebGates work together to enforce access control rules known as authorization policies. Each authorization policy includes the following:

a) Unique name

b) Success and failure URLs (where the subject's browser is redirected based on the access control decision)

c) List of objects to which the authorization policy applies

52 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.

53 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.

54 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 all children of a given prefix).

55 When the WebGate is registered as an agent with the OAM Server, the TOE 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:

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

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

c) 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.

d) IPv4 Range - denotes that the authorization policy will apply to a subject requesting access from one of a given set of IPv4 addresses.

e) Temporal - denotes that the authorization policy will only apply on certain days and/or times.

f) 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.

g) 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.

h) 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:

   i) Session count value

   ii) User's ID

   iii) User's IP address

   iv) User's group memberships

   v) User's identity domain

   vi) Attribute values belonging to user (defined in Identity Store)

   vii) Attribute values belonging to session

   viii) Current authentication level for the session

   ix) Name of authentication scheme executed to achieve the current authentication level

   x) Session creation time

   xi) Session expiration time

   xii) Literal string

56 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.

57 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.

6.2.3 [AC+PM]ESM_EID.2

58 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.

59 End users are 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.

6.2.4 [AC]FTA_TSE.1

60 The TOE 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).

6.2.5 [AC]FMT_MOF.1(1), [AC]FMT_MOF.1(2) & [AC]FMT_MSA.1

61 The trust relationship between the OAM Server and OAM Console is established during TOE installation (since they are deployed as part of the same installation), along with the Policy Store which is unique for each TOE instance. During installation, the TOE administrator specifies the Policy Store database credential.

62 The TOE administrator manages the following management functions related to access control enforcement via the OAM Console:

a) audited events

b) repository for trusted audit storage

c) policy being implemented

d) behavior to enforce in the event of communications outage

63 The TOE administrator manages the following security attributes related to access control enforcement via the OAM Console:

a) Access Control Policies

b) Access Control Policy Attributes

c) Implementation status of access control policies.

64 For a complete list of policy attributes, see section 6.2.2.

6.2.6 [AC]FMT_MSA.3

65 The OAM Server will by default deny access to any WebGate protected resources unless the TOE administrator has defined a policy that allows access to the resource.

6.3 Policy Security

6.3.1 [PM]ESM_ACT.1

66 When an administrator on the OAM Console creates or modifies an access control policy, the policy data is immediately transmitted to the environmental Policy Store for use by the OAM Server.

6.3.2 [AC]FCO_NRR.2

67 When policies are defined and updated, the TOE provides a mechanism to verify that they have been successfully distributed and for an administrator to determine what policies are being implemented.

68 The TOE generates an audit record when a policy is created, providing proof of receipt. All subsequent changes to a policy are also audited. Information in policy related audit records include:

a) Recipient Hostname (Policy Store)

b) Recipient IP Address (Policy Store)

c) Policy ID

69 The audit record / receipt will be available within 60 seconds of the policy being created / edited.

6.3.3 [AC]FPT_RPL.1

70 The TOE is immunized against replay attacks by using TLS between all components (as in accordance with the [AC]FPT_RPL.1 Assurance Activity which states "*Alternatively, the TOE may use a protocol such as SSL for transmitting data that immunizes it from replay threats.*").

6.3.4 [AC+PM]FTP_ITC.1

71 The TOE uses third-party cryptographic modules (see section 6.7) to implement trusted channels between distributed components using TLS as described in section 6.7.2.

6.4 Security Audit

6.4.1 [AC+PM]FAU_GEN.1

72 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.

73 Actions performed by administrators on the OAM Console are logged to the Audit Store. Additional audit data is written to log files that reside on the environmental operating system where the TOE component is located.

74 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 17.

6.4.2 [AC]FAU_SEL.1

75 The events that are audited by OAM 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.

6.4.3 [PM]FAU_SEL.1 & [PM]FAU_SEL_EXT.1

76 Administrators use the OAM Console to define the event types that are logged.

6.4.4 [AC]FAU_STG.1

77 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 Audit Store in the evaluated configuration but the OAM Console does not provide the ability to modify or delete audit data stored in this manner.

6.4.5 [AC+PM]FAU_STG_EXT.1

78 All audit data that is recorded by the TSF gets written securely to the operational environment. All audit data that the OAM Console generates is logged either to the local file system or to the Audit Store. Any audit data in the Audit Store is protected against unauthorized modification and deletion as there is no administrative method to manipulate this data once it has been stored.

79 All communications between the TOE and the Audit Store use JDBC protected by TLS.

6.5 Secure Administration

6.5.1 [AC+PM]FMT_SMF.1

80 The OAM Console is the TOE management interface. Some management functions are not applicable because the TSF enforces the behavior required by the SFR without the need for configuration.

81 The following management functions are defined by the PP(s) and accompanied with a description of how either the TSF implements the function or its management is not applicable to the TOE:

a) Configuration of audited events: administrators can configure what is logged by WebGates.

b) Configuration of repository for trusted audit storage: administrators can configure whether administrative activity is logged to the Audit Store.

c) Configuration of Access Control SFP: administrators can define access control policies and apply them to WebGates.

d) Querying of policy being implemented by the TSF: administrators can check the status of WebGates to see what policies are applied and what rules are contained within those policies.

e) 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.

f) Creation of policies: see "configuration of Access Control SFP".

g) Transmission of policies: see "configuration of Access Control SFP".

h) 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.

i) 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.

j) Configuration of auditable events for defined external entities: see "configuration of audited events".

k) Configuration of external audit storage location: see "configuration of repository for trusted audit storage".

l) Execution of restoration to normal state following threshold action (if applicable): the TSF can be used to manually unlock an administrative account that is locked out due to exceeding the maximum amount of failed login attempts.

m) Definition of subject security attributes, modification of subject security attributes: the TSF can be used to create administrative accounts and assign privileges to them.

n) Configuration of the behavior of other ESM products: see "configuration of Access Control SFP".

o) Management of sets of subjects that can interact with security attributes: see "definition of subject security attributes, modification of subject security attributes".

p) Management of rules by which security attributes inherit specified values: see "definition of subject security attributes, modification of subject security attributes".

q) Management of the users that belong to a particular role: see "definition of subject security attributes, modification of subject security attributes".

6.5.2 [PM]ESM_EAU.2

82 The OAM Console component defines individual users who exist in the environmental OAM Console Identity Store as administrators for the TOE. In the evaluated configuration, the Identity Store is an LDAP repository.

83 Administrators will supply authentication credentials (username/password) to the TOE which then relays the authentication request to the OAM 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.

6.5.3 [AC+PM]FMT_SMR.1

84 The OAM Console has a super administrator role that has full control over the TSF. Additionally, the ability to interact with policies can be granted to domain administrators. These administrators then have authority over all polices within their domain. Additionally, domain administrators can create sub-domains and assign domain administrators to them.

6.5.4 [AC+PM]FPT_APW_EXT.1

85 The TOE uses identity and credential data that is defined in the operational environment Identity Store 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.

6.5.5 [AC+PM]FPT_SKP_EXT.1

86 The TOE provides no interface to view secret key data. The cryptographic data used by the TOE is protected against unauthorized disclosure by the cryptographic modules in the environment that are used by the TOE to secure remote communications.

6.5.6 [PM]FTP_TRP.1

87 The TOE uses a third-party cryptographic module (RSA BSAFE Crypto J per section 6.7) to implement a trusted path between WebGates and administrators/users (web browsers) using TLS as described in section 6.7.2.

6.5.7 [PM]FIA_USB.1

88 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.

89 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.

6.6 Continuity of Enforcement

6.6.1 [AC]FRU_FLT.1

90 The OAM Server (Policy Decision Point) will retrieve the latest policy from the Policy Store following the restoration of communications in the event of an outage.

6.6.2 [AC]FPT_FLS_EXT.1

91 Any disruption in communication between the WebGate(s) and OAM Server, or between the OAM Server and Policy Store will result in access requests being denied during the outage.

6.7 Cryptographic Support

92 In accordance with PP_ESM_PM section 6.1.4 and PP_ESM_AC section 6.1.5, "*The cryptographic requirements for the TOE can either be implemented by the TSF or by reliance on non-ESM Operational Environment components*" and "*The ST must clearly indicate what cryptographic capabilities are used by the TSF*".

93 Table 20 identifies the cryptographic functions that are provided by the environment in support of TLS communications. The following non-ESM Operational Environment components provide this functionality:

a) **RSA BSAFE Crypto-C Micro Edition (CCME) v4.1.2.** Provides WebGate cryptographic functions.

b) **RSA BSAFE Crypto-J v6.2.5.** Provides OAM Server and OAM Console cryptographic functions.

Table 20: Environmental Cryptographic Functions

Algorithm Capabilities	CAVP
AES-CBC AES-GCM	C810 C652
RSA KeyGen (186-4) RSA SigGen (186-4) RSA SigVer (186-4) ECDSA KeyGen (186-4)	

Algorithm Capabilities	CAVP
ECDSA SigGen (186-4) ECDSA SigVer (186-4)	
SHA-256/384/512	
HMAC-SHA-256/384/512	
Counter DRBG	

6.7.1 [PM]FCS_HTTPS_EXT.1

94 The TOE provides the ability for remote administrators to connect to the OAM 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.

6.7.2 [AC+PM]FCS_TLS_EXT.1

95 The TOE implements TLS 1.2 in accordance with RFC5246. The TOE supports the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

96 Table 21 below identifies the TLS channels, showing both server and client components.

Table 21: TLS Channels

TLS Server	TLS Client
WebGate for Protected Resource(s) (TOE)	Browser (environment)
OAM Console – WebLogic Interface (TOE)	Browser (environment)
OAM Console – Dedicated Interface (TOE)	Browser (environment)
OAM Server (TOE)	WebGate (TOE)
OAM Oracle Authentication Protocol (TOE)	WebGate Oracle Authentication Protocol (TOE)
Policy Store (environment)	OAM Console (TOE) OAM Server (TOE)
Audit Store (environment)	OAM Console (TOE) OAM Server (TOE)
Identity Store (environment)	OAM Console (TOE) OAM Server (TOE)

97 **Note**: Assured identification of each endpoint identified in Table 21 is through the use of X.509 certificates.

7 Rationale

7.1 Conformance Claim Rationale

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

a) **TOE type.** As identified in section 2.1, the TOE is an enterprise web access control and policy management solution consistent with the claimed PPs.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the claimed PPs.

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

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

7.2 Security Objectives Rationale

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

7.3 Security Requirements Rationale

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