

Lightship Security 12c Oracle Access Management User Guide

[Home](#) » [Lightship Security](#) » Lightship Security 12c Oracle Access Management User Guide 



Oracle Access Management 12c
Common Criteria Guide
Version 1.6
September 2023
Document prepared by
www.lightshipsec.com

Contents

- [1 About this Guide](#)
- [2 Secure Acceptance](#)
- [3 Configuration Guidance](#)
- [4 Secure Communications Configuration](#)
- [5 Documents / Resources](#)

About this Guide

1.1 Overview

1. This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of Oracle Access Management 12c and related informat

1.2 Audience

2. This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use thguide in conjunction with the related documents listed in Table

3.

1.3 About the Common Criteria Evaluation

3. The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at <https://www.commoncriteriaportal.org/>

1.3.1 Protection Profile Conformance

4. The Common Criteria evaluation was performed against the requirements of the following Protection Profiles available at <https://www.niap-ccevs.org/Profile/PP.c>
- a) Standard Protection Profile for Enterprise Security Management Policy Management, v2.1
 - b) Standard Protection Profile for Enterprise Security Management Access Control, v2.1

1.3.2 Evaluated Software

5. The Target of Evaluation (TOE) is Oracle Access Management 12c.
6. The evaluation testing was performed using the following components in the environment.

Table 1: Non-TOE Components

Component	Details
OAM Server & Console – Platform Requirements	<ul style="list-style-type: none">• Oracle Linux 7.6 UEK 5• Oracle WebLogic Server 12c• Oracle JRE 8
OAM WebGate – Platform Requirements	<ul style="list-style-type: none">• 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	

1.3.3 Evaluated Functions

7. The following functions have been evaluated under Common Criteria:
- a) **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 (URLs).
When a policy is created or modified, the TSF applies this policy to the Policy Store. 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 and stored in the OUD. Administrators of the TOE are also defined using the System Identity Store. Administrators of the TOE are authenticated by the System Identity Store using LDAP with username/password.

b) **Security Audit.** 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. 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. Once generated, audit data is stored in a manner that prevents unauthorized modification or deletion.

c) **Communications.** The TOE provides feedback to administrators when changes to policy rules are applied. Each individual WebGate is identified by a unique name. Policies are uniquely identified by name as well. Policy changes implemented by an Administrator are recorded in the Policy Store and are retrieved from the server and applied by the WebGates for which they are intended. In addition to providing a notification when the policy data is retrieved, an administrator is capable of querying a WebGate to determine the specific policy that it has implemented.

d) **Cryptographic Support.** The TOE's cryptographic capabilities are provided by RSA BSAFE cryptographic modules in the TOE's operational environment.

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

f) **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 TOE, 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.

g) **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 TOE also provides super administrator roles with global authority over all applications and all domains. By default, the TOE enforces a restrictive deny-by-default policy on any resources that are defined to be protected. The TOE 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 instruct the TOE to process rules in an administratively-defined order.

h) **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. WebGates 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. WebGates 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 TOE to enforce an incorrect policy.

i) Resource Utilization. If the connection between a WebGate and the OAM Server is lost, that WebGate will be able to continue enforcing the cached enforcement decisions. The WebGates 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.

j) 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.

k) Trusted Path/Channels. Remote administrative communications with the OAM Console are secured using HTTPS. All interactions between the OAM Server and other components are secured using TLS.

8. **NOTE:** No claims are made regarding any other security functionality.

1.3.4 Evaluation Assumptions

9. The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 2: Evaluation Assumptions

Assumption	Guidance
There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.	Assign one or more administrators to be responsible for managing OAM.
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.	RSA BSAFE provides the cryptographic primitives. See configuration steps in Section 4.1 below.
Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.	Follow the verification procedures in 2.2 below. Server hardware should be physically secured from unauthorized access. Configure and operate OAM in accordance with this document and referenced guidance.
Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	Implement processes to ensure that OAM administrators are trustworthy (e.g., background checks / clearances) and trained to operate OAM.
One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.	OAM Servers and OAM WebGates perform this function – no additional actions required.
The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	Identity services for OAM are provided by Oracle Unified Directory or Oracle Internet Directory. Identity services are assumed to be trusted.
The Operational Environment will provide reliable time data to the TOE.	Multiple NTP sources should be configured.
The Operational Environment shall be able to identify a user requesting access to the TOE.	Identity services for OAM are provided by Oracle Unified Directory or Oracle Internet Directory. Identity services are assumed to be trusted.
The Operational Environment will provide a policy that the TOE will enforce.	The Policy Store is provided by Oracle Database 12c.
The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.	All components listed in Table 1 should be managed and deployed in accordance with organizational security policies.

1.4 Conventions

10. The following conventions are used in this guide:

- a) CLI Command <replaceable> – This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within <> is replaceable. For example: Use the cat <filename> command to view the contents of a file
- b) [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example: The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.
- c) **GUI > Reference** – denotes a sequence of GUI screen interactions. For example: Select **File > Save** to save the file.
- d) [REFERENCE] Section – denotes a document and section reference from Table 3. For example: Follow [ADMIN] Configuring Users to add a new user.

1.5 Related Resources

11. This guide supplements the below Oracle guidance resources.

Table 3: Related Resources

Reference	Resource
[ADMIN]	https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.4/aiaag/introducing-oracle-access-management.html

12. **NOTE:** The information in this guide supersedes related information in other resources.

Secure Acceptance

2.1 Obtaining the TOE

13. The TOE is downloaded by users from the Oracle Identity & Access Management Downloads page at <https://www.oracle.com/middleware/technologies/identitymanagement/downloads.html>
14. To obtain the TOE:
- Download the following:
 - Oracle Identity and Access Management 12cPS4 (Version 12.2.1.4.0)
 - Oracle Identity and Access Management 12cPS4 Infrastructure (Version 12.2.1.4.0)
 - Oracle Unified Directory 12cPS4 (Version 12.2.1.4.0)
 - The OAM WebGate is a feature/plugin installed with the Oracle HTTP Server 12.2.1.4 at <https://www.oracle.com/caen/middleware/technologies/webtier-downloads.html>.
Locate the “Oracle HTTP Server 12.2.1.4” download section of the page and click the Linux 64-bit download link.
 - Download patches 35371374 (OAM Server) and 33974688 (OAM WebGate) from My Oracle Support at <https://support.oracle.com>.
15. **Note:** The Oracle Unified Directory is not a TOE component but is used in the evaluated configuration.

2.2 Verifying the TOE

16. To verify the correct version of the TOE is installed, administrators must run the opatch lsinventory command on both the OAM Server and OAM WebGate.

Configuration Guidance

3.1 Installation & Configuration

17. The TOE is installed and configured at the customer site by Oracle Support personnel. To install the TOE in the evaluated configuration, it is recommended that customers contact Oracle.
18. It is also recommended that customers configure the underlying OS in accordance with the instructions provided by the Oracle Linux v7.6 Common Criteria Guidance Document (<https://www.oracle.com/a/ocom/docs/oracle-linux-v7.6-common-criteria-guidance-v1.7.pdf>). Particular attention should be given to SSH and system firewall configuration. Using the system firewall (iptables), customers must block any unnecessary ports from external access. The TOE uses ports 5575, 7002, 14101, and 14151 by default.
19. Note: After installation of any package (initial, patch, update, etc.), administrators must execute the `$ORACLE_HOME/OPatch/patchutil cleanup` command to ensure the TOE runs in the evaluated configuration.
20. The following option should be added under the `JAVA_OPTIONS` in `$DOMAIN_HOME/bin/setDomainEnv.sh`: `-Doracle.oam.handshake.check=true`.

3.2 Logging In

21. Administrators of the TOE can access all management functionality through the Web GUI. Once configured, the TOE protects communications between remote administrators and the TOE using TLSv1.2.
22. To access the web GUI, administrators must point a web browser to the URL defined during installation.

3.3 Data Source / Stores

23. OAM supports a wider variety of data sources as described in **Managing Data Sources**. The evaluated configuration uses the following data sources:
 - a) Database (Policy Store and Audit Store). Oracle Database 19c.
 - b) User Identity Store. Oracle Unified Directory 12c (or any LDAPv3 directory server including Oracle Internet Directory 12c).
 - c) Keystore. Java keystore located on the local file system providing secure storage of certificates and keys.

3.4 Audit Logging

24. The TOE generates audit logs by default as described at Logging, Auditing, Reporting and Monitoring Performance. Audit records that are generated by the TSF are simultaneously transmitted to the underlying local file systems in the Operational Environment and are not stored within the TSF. The TOE provides logging in multiple locations, as follows:

OAM Console Audit Logs

- `/u01/app/oracle/admin/domains/oam_domain/servers/oam_policy_mgr1/logs/oam_policy_mgr1.log`
- `/u01/app/oracle/admin/domains/oam_domain/servers/oam_policy_mgr1/logs/oam_policy_mgr1-diagnostic.log`
- `/u01/app/oracle/admin/domains/oam_domain/servers/oam_policy_mgr1/logs/auditlogs/OAM/audit.log`
- `/u01/app/oracle/admin/domains/oam_domain/servers/AdminServer/logs/AdminServer.log`
- `/u01/app/oracle/admin/domains/oam_domain/servers/AdminServer/logs/auditlogs/OAM/audit.log`
- `/home/oracle/oam_policy.out`
- `/home/oracle/wls.out`
- `/home/oracle/nm.out`

AM Server Audit Logs

- `/u01/app/oracle/admin/domains/oam_domain/servers/oam_server1/logs/auditlogs/OAM/audit.log`
- `/u01/app/oracle/admin/domains/oam_domain/servers/oam_server1/logs/oam_server1.log`

- /u01/app/oracle/admin/domains/oam_domain/servers/oam_server1/logs/oam_server1-diagnostic.log
- /home/oracle/oam_server.out

WebGate Audit Logs

- /u01/app/oracle/admin/domains/ohs_domain/servers/ohs1/logs/weblogic.log
- /u01/app/oracle/admin/domains/ohs_domain/servers/ohs1/logs/ohs1.log
- /u01/app/oracle/admin/domains/ohs_domain/servers/ohs1/logs/admin_log

25. **Note:** The OAM Console Audit Logs meet the requirements for the policy management portion of the TOE. The OAM Server Audit Logs and WebGate Audit Logs provide the audit events for the Access Control portion of the TOE.
26. A reference of audit event types and format is provided below.

3.4.1 Troubleshooting TLS Connections

27. When troubleshooting TLS connections additional audit events can be generated by using the java option “-Djavax.net.debug=ssl,handshake” in the startWebLogic.sh startup script. Additional information about Debugging SSL/TLS Connections can be found here: <https://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/ReadDebug.html>.
28. Note: Care should be taken when using debug interfaces and minimal debug information should be output.

3.4.2 Audit Datastore

29. During installation and configuration as described in section 3.1, the TOE is also configured to utilize an external database as an audit store by default. This includes the configuration to the audit store using the trusted channel as described in section 1.3.3. Additional customization of audit behaviour is described in Securing Applications with Oracle Platform Security Services – <https://docs.oracle.com/en/middleware/fusion-middleware/platformsecurity/12.2.1.4/jsec/audpolicy.html#GUID-B042E456-BC36-482D-B7A3A4425267B960>.
30. During a database outage or other event that prevents connectivity between the TOE and the Audit Datastore, audit records will continue to be written to the local audit storage location, as per the section above, and will be pushed to the external database when it comes back online.

3.5 Defining Access Control Policies

31. The TOE provides policy management and access control capabilities as described at Managing Policies to Protect Resources and Enable SSO.
32. In summary, the process for defining an access control policy using OAM consists of the following activities performed at the OAM Console:
- Register and set up an OAM Webgate
 - Define one or more Application Domains
 - Define Resources to be protected within the Application Domain
 - Define Authentication Policies and Authorization Policies for accessing these Resources
33. The following diagrams depict how the TOE implements policy definition between objects and object attributes, policy distribution, and data source communications:

Figure 1: OAM Policy Definition

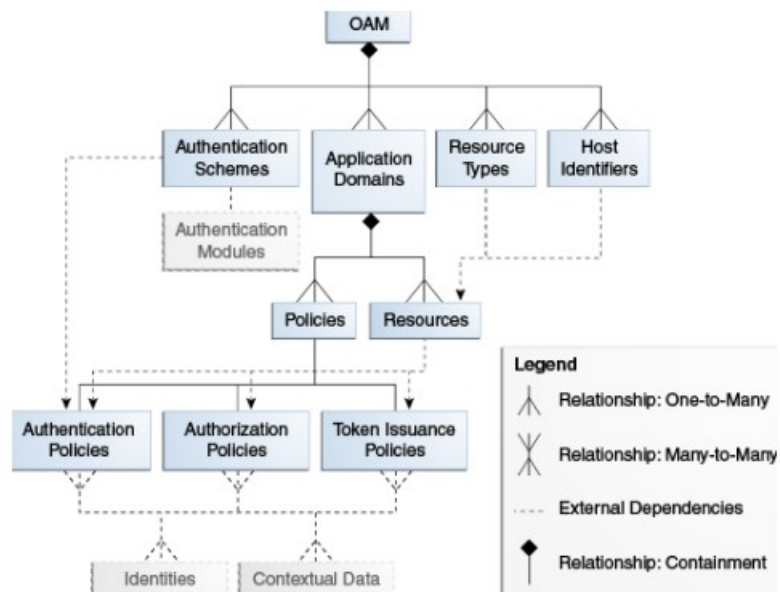


Figure 2: OAM Policy Distribution

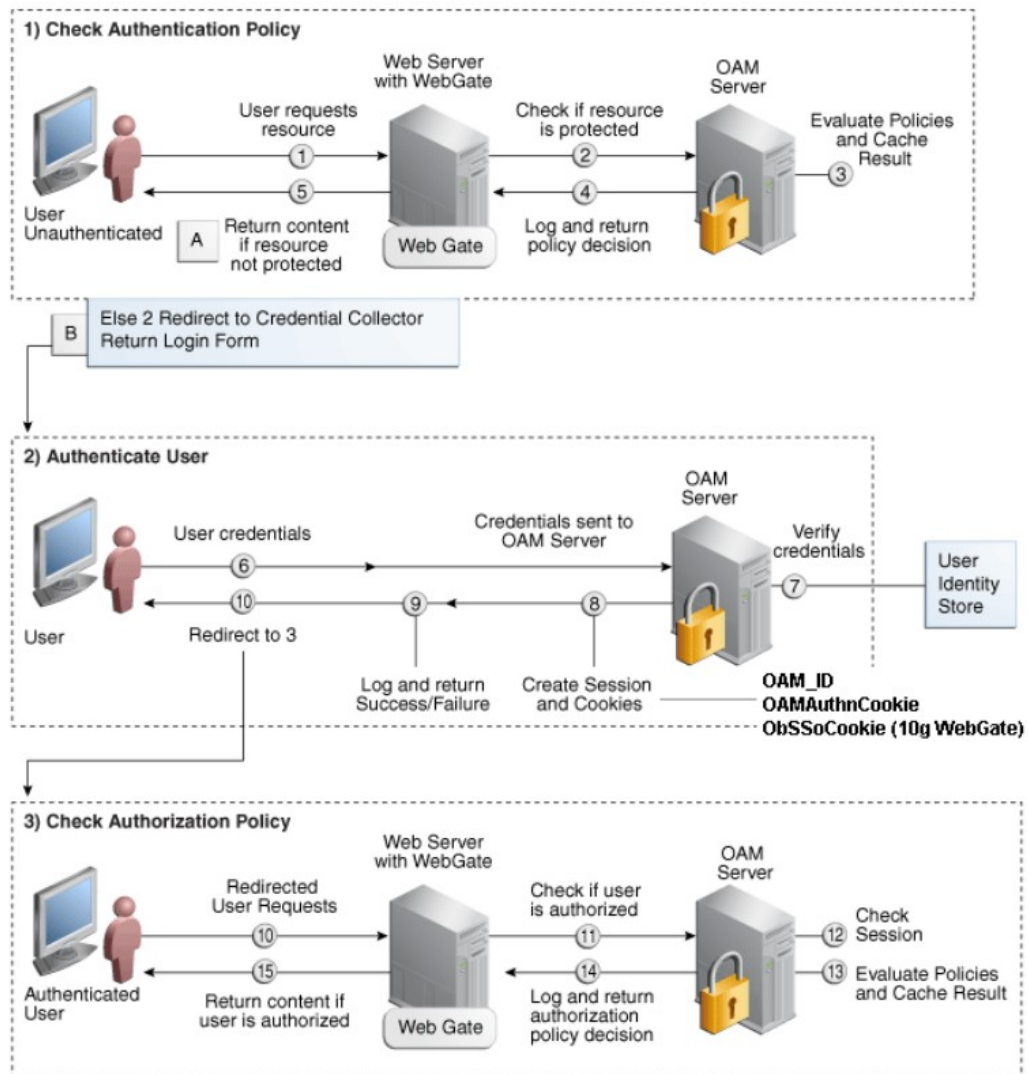
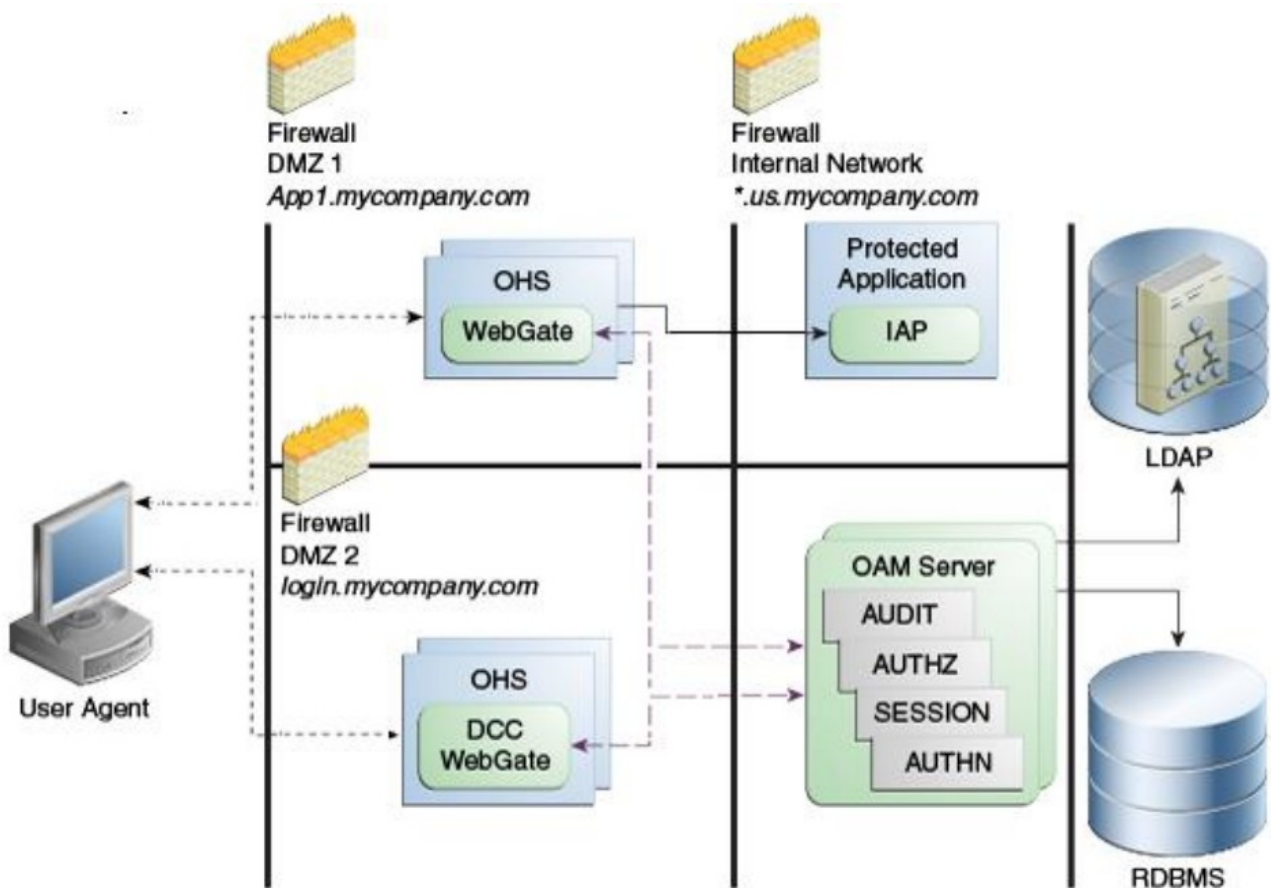


Figure 3: OAM Data Source Communications



34. Multiple Application Domains may be defined since multiple distinct applications may be running on the same logical server. Within an Application Domain, individual Resources (files or URLs) can be defined as being protected by OAM. When a user requests to access one of these resources, the Webgate will intercept the request and determine, based on the user requesting access, how to respond based on the Authentication Policies and Authorization Policies defined for this resource.
35. Authorization Policies rely on conditions that must be satisfied by the access request. When writing conditions, the user identity, IP address (or range), or user attributes may be specified. The user attributes available will be determined by the connected identity store and can be arbitrarily-defined. There are also includes temporal conditions, which stipulate days and/or times when the condition will apply. Multiple conditions can be combined so that, for example, a user who attempts to access a resource may be permitted to at a given time or from a given location, but is forbidden from making the same attempt at a different time or location.
36. Within a given Application Domain, the Authorization Policies are uniquely identified by a Policy ID that is logged by the OAM Console. The policy ID is associated with the policy at policy creation and modification in the TOE logs. The policy is written to the policy store and the OAM server retrieves the policy from the policy store. The OAM Server pushes a list of all active policy IDs to the shared policy database, each time a change in policies is made. The policy data is written to the policy store in an Oracle proprietary format. Any additions or changes to an Authorization Policy will take immediate effect without administrative intervention.

3.5.1 Processing Contradictory Rules in OAM

37. Contradictory rules are resolved in the following manner by OAM Console/Webgates:
 - a) When an administrator defines an authorization policy, the presence of explicitly contradictory rules will

prevent the policy from being saved. Contradictory rules occur when the same subject-object operation combination at the same level of detail results in both a permit and a deny result

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.

3.5.2 Default Values

38. 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.

3.6 Communication Failures

39. 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. 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. Action taken on a communication failure and subsequent recovery is not configurable.

3.7 Log Types and Format

40. Logs that are generated by the TOE follow the type and format identified in the following link:
<https://docs.oracle.com/en/middleware/idm/accessmanager/12.2.1.4/aiaag/auditing-administrative-and-run-time-events.html#GUIDC5488480-D15F-4CFC-9A12-59205F9CDBCB>.
41. In addition to the above, the following audit logs are generated for the establishment and disestablishment of communications with the audit server: <Info> <JDBC> <oam.example.com> <oam_server1> <[ACTIVE] ExecuteThread: '0' for queue: weblogic.kernel.Default (selftuning)'\> <weblogic> <> <dacdd14d-1d39-44dc-b9d6-0b9952a6ce70000039bb> <1663183955505> <[severity-value: 64] [rid: 0] [partition-id: 0] [partition-name: DOMAIN] > <BEA-001128> <Connection for pool "opss-audit-DBDS" has been closed.> <Info> <JDBC> <oam.example.com> <oam_server1> <[ACTIVE] ExecuteThread: '4' for queue: 'weblogic.kernel.Default (selftuning)'\> <weblogic> <> <dacdd14d-1d39-44dc-b9d6-0b9952a6ce70000039c0> <1663184006352> <[severity-value: 64] [rid: 0] [partition-id: 0] [partition-name: DOMAIN] > <BEA-001516> <Data source connection pool "opss-audit-DBDS" connected to Database: "Oracle", Version: "Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 – Production

Secure Communications Configuration

4.1 FIPS & TLS Setup and Configuration

42. Follow the instructions in Appendix B – Securing Communication of [ADMIN] for FIPS and TLS configuration (<https://docs.oracle.com/en/middleware/idm/accessmanager/12.2.1.4/aiaag/securing-communication.html#GUID-2E7AAA62-28204D9F-B3BA-C37FFDD55D6E>).

43. TLS is supported for communications with the following entities:

- Audit Server
- Authentication Server
- OAM Server
- OAM Console
- OAM WebGates
- Policy Store
- User Endpoints

44. **Note:** This setup and configuration is to be performed with direct assistance from an Oracle Support representative.

4.2 Disabling Plaintext Ports

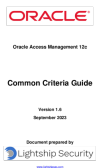
45. In the evaluated configuration, TOE administrators must disable the plaintext ports once the WLST CLI interface changes are complete.

46. To disable the plaintext ports:

47. From the WebLogic Console, navigate to Environment > Servers > “Service Name” > Configuration > General. Select Lock and Edit and then uncheck Plaintext Port. Click Save to save the configuration and exit.



Documents / Resources

	<p>Lightship Security 12c Oracle Access Management [pdf] User Guide 12c Oracle Access Management, Oracle Access Management, Access Management, Management</p>
---	---