Oracle® Health Insurance Components Security Guide

March 07, 2016

ORACLE

License Restrictions Warranty/Consequential Damages Disclaimer

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

Warranty Disclaimer

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Hazardous Applications Notice

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Trademark Notice

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third Party Content, Products, and Services Disclaimer

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Table of Contents

1 Introduction

Disclaimer:
This document is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

1.1 Overview

Security planning is a critical step to help protect your company's valuable data and ensure that information is not compromised. Established security policies and goals should guide the security plan your organization executes to secure its systems.

Oracle Health Insurance (OHI) Components applications store sensitive data and require security measures to be taken. Security policies should align with those already established at your organization, or new ones should be established if they are not already defined.

This document provides guidelines for securing an OHI installation, including the configuration and installation steps needed to meet security goals. Details on the types of security features and services that are available to detect and prevent a potential security breach are provided. This encompasses secure system deployment, protection of sensitive data, reliability and availability of the application, authentication and authorization mechanisms.

You may use this document to develop your organization's security policies and practices in the context of OHI. It is critical that an organization set security standards and properly implement them. The development and review of security documentation, an evaluation of business requirements, and the configuration and validation of available security measures and services should all be performed.

1.2 Document Ownership and Control

This document is maintained by Oracle Health Insurance Components Development. It is reviewed twice per year and adjusted as needed.

2 General Security Principles

The following principles are fundamental to using any application securely.

2.1 Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. Regularly check My Oracle Support for Critical Patch Updates (CPU) for the OHI execution platform (Oracle Database and Oracle WebLogic application server).

2.2 Restrict Network Access to Critical Services

Keep both the OHI application's middle-tier and database behind a firewall. In addition, configure a firewall between the middle-tier and the database. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary.

2.3 Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, grants, etc., often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

2.4 Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

2.5 Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check the Installation Guide and Release Notes before installing a new release. Regularly check this Security Guide for up-to-date security related information.

2.6 Minimize the Attack Surface

The "attack surface" of a system is the sum of the different entry points that an unauthorized user can exploit to gain access to system services or to the data is maintained in the system. Common strategies for reducing the attack surface or hardening the system include (but are not limited to):

- Minimize the number of services running, i.e. make sure to only run required services.
- Make sure that all entry points, like the system's user interface and its web services are secured.

Specifically for OHI Components applications make sure to:

- Do not install software on the machines that execute the OHI Components applications technology stack that is not required for running the OHI Components applications.
- Follow the Installation Guide to prevent installation of software that is not required to run the application. For example, for Oracle's WebLogic server installation it specifically mentions the services that need to be installed.
- Do not install additional applications in the WebLogic domains that run OHI Components applications.
- Make sure to track and trace use of the system, e.g. by logging which users access its services.
- Apply firewalls at the system's boundaries.
- Secure all entries, for example make sure that SSL/TLS is used between clients and load balancer / DMZ.

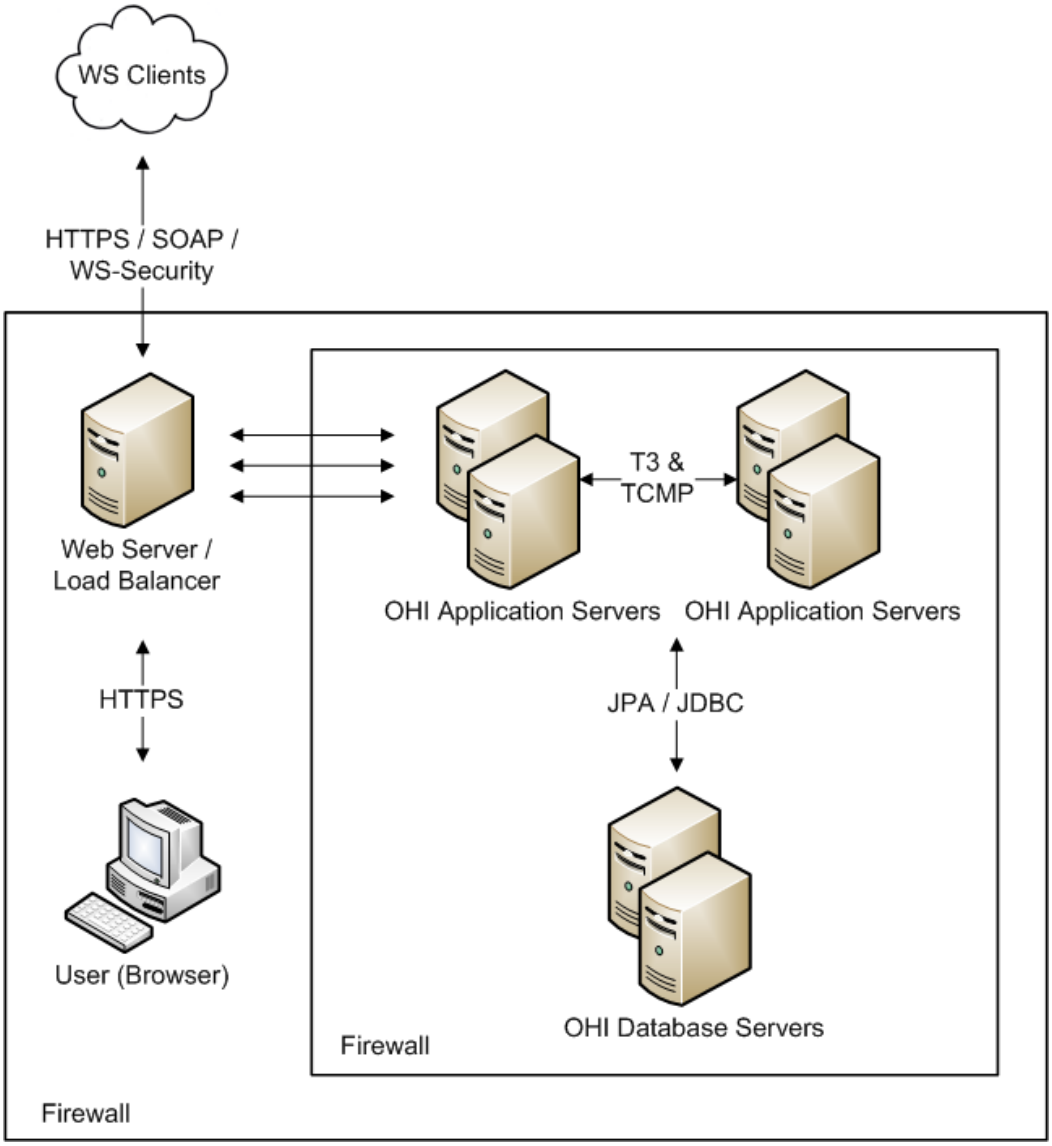
3 System Deployment

3.1 Network Security in an OHI Environment

When deploying OHI Components applications onto a network there are many security issues to take into consideration, especially the use of firewall and VPN technologies. A firewall will permit or deny network permissions based on configured rules, to protect the internal network from unauthorized access while permitting legitimate communications.

Firewalls perform the following functions in a typical OHI environment:

- Guard the company Intranet from unauthorized outside access.
- Separate Intranet users accessing the OHI system from internal subnetworks where critical corporate information and services reside.
- Protect from IP spoofing and routing threats.
- Prohibit unauthorized users from accessing protected networks and control access to restricted services.



A typical OHI Components environment usually has the following security zones:

- Internet - External web service clients may come from outside of the company network.
- Intranet - A company network separated by the external firewall that gives remote workers access to the OHI user interface. This is also where OHI web servers and / or load balancers may be placed. Alternatively, for additional protection, web and load balancing servers may be placed in a separate demilitarized zone (DMZ) where external and internal clients first interact with the OHI environment.
- OHI application server and database zone - OHI application servers, database servers and possibly authentication servers (for example, if a customer chooses to delegate authentication using LDAP servers) typically reside in this zone.

Ensure that the firewalls used to secure an OHI environment support the HTTP 1.1 protocol; it enables browser cookies and inline data compression for improved performance.

3.2 Accessing the User Interface outside the Firewall

OHI Components applications' user interfaces are browser-based and will allow remote workers to access the application services. It is recommended that these users access the application from within the company network, secured behind the outside firewall. Virtual Private Network (VPN)

technology should be used to allow employees working remotely to access an OHI application. A VPN tunnels outside traffic through the firewall, placing remote workers virtually inside the firewall.

3.3 Provide access to OHI Web Services for External Clients

It may be required to give external clients, that are not inside the company firewall, access to OHI web services. In that case, the following aspects have to be taken into account:

- Do not expose the OHI web services directly, always make sure that the web services are fronted by a separate web server / load balancer.
- Messages exchanged between a web service and an external client may contain protected health information; as a minimum security requirement, message traffic must be accessed only through HTTP secured with SSL.
- Apply proper web services security policies to enforce authentication and to guarantee integrity and confidentiality of messages.

3.4 Configuring SSL

The Secure Sockets Layer (SSL) protocol provides communication security by encrypting traffic across a network in a way designed to prevent eavesdropping and tampering. It uses asymmetric cryptography for privacy and a keyed message authentication code for message reliability. Setting up an SSL-secured connection requires a digital certificate issued by a trusted certificate authority. Self-signed digital certificates should only be used for internal testing.

Oracle recommends that all OHI Components applications related data communication, whether it is browser or web services based and whether it is within the organization's firewall or accessed through VPN, is at least secured using SSL.

Configuring SSL in WebLogic

WebLogic Application Server supports SSL 3.0 and Transport Layer Security (TLS) 1.0 specifications. WebLogic does not support SSL version 2.0 and below.
For information on how to configure SSL in WebLogic please visit the following URLs:

- http://download.oracle.com/docs/cd/E17904_01/web.1111/e13707/ssl.htm#SECMG384
- http://download.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html[1]
- http://download.oracle.com/docs/cd/E17904_01/apirefs.1111/e13952/taskhelp/security/ConfigureKeystoresAndSSL.html[2]

Configuring SSL for Authentication: using LDAPS

OHI Components applications delegate authentication requests using configurable WebLogic authentication providers. Typically, authentication requests are delegated to an LDAP server. WebLogic authentication providers can authenticate using SSL-secured traffic by configuring the LDAP connect string to use LDAPS, e.g. ldaps://<machine>.<domain>:<ssl_port>. The SSL port for the LDAP protocol is usually 636.

This paragraph describes the configuration for enabling SSL encrypted traffic between OHI Components applications and Oracle Internet Directory (OID). OID supports three SSL Modes that are listed in the following table.

SSL Authentication Methods	Description	Supported by OHI Components?

Mode 1: No SSL Authentication	Neither the client nor the server authenticates itself to the other. No certificates are sent or exchanged. Only SSL encryption and decryption is used.	No
Mode 2: SSL Server Authentication	The directory server authenticates itself to the client. The directory server sends the client a certificate verifying that the server is authentic.	Yes
Mode 3: SSL Client and Server Authentication	The client and server authenticate themselves to each other and send certificates to each other.	Yes

To use the LDAPS feature, an SSL certificate needs to be obtained and installed on the Directory Server. Recommended steps for configuring Oracle Internet Directory 11g (OID) SSL Server Authentication (mode 2) are listed in this paragraph. The listed process is applicable for OID releases 11.1.1.2 to 11.1.1.4 and is based on Support Article 1203271.1 that is published on the Oracle Support website (and takes precedence over the product documentation). Article 1203271.1 covers steps 1 to 4 in the following list:

1. Support Article 1203271.1 suggests to create an additional OID Instance / Configset. Rationale as given in the article: "By default, the SSL authentication mode is set to authentication mode 1 (encryption only, no authentication). Be sure at least one Oracle Internet Directory server instance has this default authentication mode. Otherwise, you break Oracle Delegated Administration Services and other applications that expect to communicate with Oracle Internet Directory on the encrypted SSL port.". Create an additional OID instance (requires migrating the data of the original instance) or make sure that a configuration set is configured to also support authentication mode 1.
2. Use the Fusion Middleware Enterprise Manager to create a Wallet. For test systems Self-Signed Wallets are sufficient. For production systems Self-Signed Certificates are not recommended: Self-Signed Certificates typically lead to Certificate Trust messages. Users could react to these messages but in OHI Components applications the user authentication process will fail as a result of an error in the SSL handshake. Create a proper Wallet for production systems.
   For a production setup, generate a certificate request and send that to a Certificate Authority (CA). Import the SSL certificate that was issued by the CA before continuing with the following step.
3. Enable SSL for the OID server using the Wallet that was created in the previous step.
4. Restart the OID instance.
5. Stop the WebLogic (managed) servers that execute the OHI Components application.
6. If a Self-Signed certificate was used, prevent Certificate Trust warnings that will break the authentication process by importing the self-signed root certificate in the cacerts certificates store of the JVM that executes the OHI Components application.
   1. Export the Self-Signed root certificate from the Self-Signed Wallet using the Fusion Middleware Enterprise Manager.
   2. Make a backup of the JVM's cacerts file.
   3. Import the root certificate into the cacerts certificate store using the keytool. In the following example alias is a self-chosen, meaningful name for the root certificate (note: the alias has to be unique within the cacerts file!)
      keytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt -alias <alias> -file <path_to_exported_root_certificate_file>
7. Start the WebLogic (managed) servers that executes the OHI Components application.
8. In the WebLogic Console, in the "Provider Specific" settings tab of the OHIAuthenticationProvider, set the SSLEnabled flag (restart of WebLogic server required).

9. Test the setup. If an additional OID instance was created and the original instance is no longer needed, the original OID Instance / Configuration set can be stopped using opmnctl. Optionally, it can be removed.

Configuring SSL for Coherence

OHI Components applications use an Oracle Coherence distributed cache that is shared between multiple cluster nodes. It is expected that all cluster nodes reside in the same security zone, i.e. the OHI application server and database zone. Coherence provides an SSL implementation that secures TCMP communication between cluster nodes that can be enabled if required. For information on how to configure SSL to secure Coherence TCMP traffic please visit the following URL: http://docs.oracle.com/cd/E24290_01/coh.371/e22841/toc.htm.

1. http://download.oracle.com/javase/6/docs/technotes/guides/security/jsse/J SSERefGuide.html
2. http://download.oracle.com/docs/cd/E17904_ 01/apirefs.1111/e13952/taskhelp/security/ConfigureKeystoresAndSSL.html

4 User Access

This chapter provides an overview of user access related topics.

4.1 User Provisioning

Before users can access OHI applications they have to be provisioned first, i.e. they have to be registered within the system. The User Provisioning web service is used for that purpose. It is documented in the User Access Implementation Guide.

OHI Components applications do not store password data.

Alternately, if OHI applications are configured for SSO, users may be auto-provisioned. See the documentation on configure SSO and auto-provisioning here (page) in the OHI Value Based Payments Installation Guide.

4.2 User Authentication

Before users can access the system they have to be authenticated by entering username and password credentials in the login page. OHI Components applications delegate the actual authentication request to an identity and access management system of choice. The authentication provider can be configured through the WebLogic console. A combination of multiple authentication providers is supported, for example to try credential store A first and credential store B second.
Failed login attempts can be logged in a specific security log.

OHI Components applications do not enforce any password policies, like setting a maximum number of failed login attempts before an account is locked. That is also delegated to an access management system.The OHI Components Operations Guide explains the configuration for that.

For additional information on authentication please see the following sources:

- The Installation Guide for a specific OHI Components application explains the configuration of authentication providers, e.g. for Oracle Internet Directory (OID).
- For more information on WebLogic Authentication Providers see http://docs.oracle.com/cd/E17904_01/web.1111/e13707/atn.htm.
- The OHI Components Operations Guide explains how the security log can be configured.

4.3 User Authorization

Access to data in OHI applications is restricted based on user authorizations. Access to all UI pages is protected: a page cannot be accessed unless a user is granted the proper privileges to do so.
Furthermore, more granular access to data in OHI may need to be restricted based on user authorizations for several reasons, like:

- privacy, e.g. secret addresses,
- sensitive medical information, e.g. regarding diagnoses and procedures for a member,

- user skill level, e.g. for adjudicating high-value claims

Access controls are maintained entirely in the application. Roles are fully configurable in the application but can be maintained in an external source (typically a directory server) so that these can be interfaced using the OHI Components Provisioning Service. For additional information on configuration of user access rights please consult the User Access Implementation Guide.

4.4 Cookies

An OHI Components application is accessed by users through a browser. Because OHI Components applications use session cookies to manage user sessions, cookies must be enabled in the browser. Consult the browser's documentation to configure the use of cookies.

The JSESSIONID session cookie contains the session ID generated for a user to manage data associated with the user's session. A unique session ID is generated when a user successfully logs into the OHI application. The session ID is generated by the JEE server and passed to a browser as a non-persistent cookie. The browser retains it for the duration of the session, and deletes it when the user logs out or the session times out. During a session, when a browser issues a request back to the application server, it sends the session cookie in the HTTP header of the request. Requests that do not contain valid session IDs are not processed by the server.

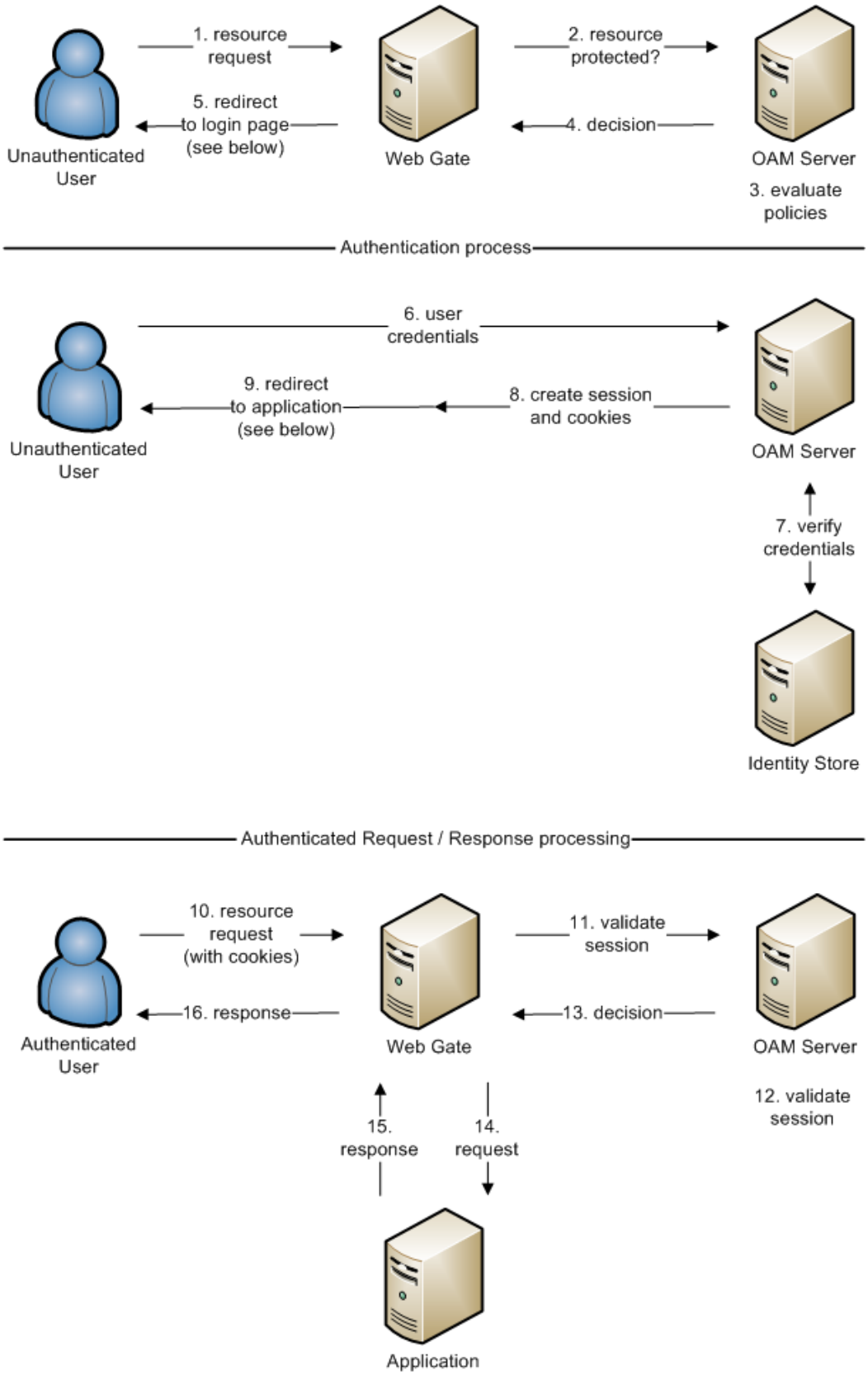
4.5 Single Sign-On (SSO)

OHI Components applications can participate in various SSO architectures. Example use cases are:

- Multiple OHI Components applications, each being executed in its own WebLogic domain, for which Oracle Access Manager (OAM) provides SSO capabilities.
- One or more OHI Components applications that are part of a larger set of business applications for which a third party identity management solution provides SSO capabilities.

Oracle internally runs multiple OHI Components applications and verifies the SSO capabilities using OAM and the Oracle WebGate. In an SSO architecture the WebGate functions as a kind of firewall / proxy that protects resources based on URI patterns. It collaborates with OAM for authenticating users and establishing user sessions.

The following graphic provides a high-level overview for that architecture. It shows the components involved in authenticating a user and handling a request.



Overview of the process:

1. The user sends a request for accessing an OHI Components application.
2. The WebGate forwards the request to OAM for policy evaluation.
3. OAM:

- Checks for the existence of an SSO cookie.
- Checks policies to determine if the resource protected and if so, how?

4. OAM logs and returns decisions.
5. WebGate responds as follows:
   - Unprotected resources are served to the user.
   - For a protected Resource the request is redirected to a SSO login page. Authentication processing begins.
6. The user enters credentials and these are submitted to OAM.
7. OAM verifies the credentials, for example by delegating the authentication request to an Oracle Directory server.
8. OAM starts the session and creates cookies for that, e.g. an OAMAuthnCookie.
9. Now that the user is authenticated, the user's request is redirected to the application.
10. It again passes the WebGate.
11. The WebGate forwards the request to OAM for policy evaluation.
12. OAM evaluates policies and validates the session based on the cookies.
13. OAM logs and returns decisions.
14. The request is passed on to the OHI Components application.
15. The application processes the request and returns a response.
16. The response is returned to the user's client.

Setting up all the components that are involved and wiring these together is a complex process that should be handled by experienced resources. Oracle Consulting services can assist with that.

OHI Components applications SSO properties

As OHI Components applications do not store user credentials, authentication requests are delegated to external authentication providers. For example, for an OHI Components application that is executed in a WebLogic domain a WebLogic Authentication Provider can be configured to handle user authentication against an external identity store. If an OHI Components application participates in an SSO architecture then the application relies on external components, like Oracle Access Manager and Oracle WebGate, to authenticate users. In that case the application must be configured such that it no longer authenticates users.

The Installation Guide for OHI Components applications specifies the properties that must be set in order for an OHI Components applications to take part in an SSO architecture.

5 Web Services Security

This chapter explains how OHI Components applications web services are secured and which security configuration options are available.

5.1 Web Services Security Overview

For any web service, it is important to guarantee integrity and confidentiality of messages and to ensure the identity of a client that is accessing OHI web services. This can be achieved by implementing different types of security measures.

Security Type	Description
Transport-level security	Secures the connection between the client application and a web service with Secure Sockets Layer (SSL).
Message-level security	Includes all the security benefits of SSL, but with additional flexibility and features. Message-level security is end-to-end, which means that a message is secure even when the transmission involves one or more intermediaries. The message itself is digitally signed and encrypted, rather than just the connection.
Access control security	Specifies which roles are allowed to access web services (answers the question "who can do what?").

By default OHI Components applications web services verify that the request is executed by an authenticated user. Transport-level security is not enabled by default; it should be put in place, at least to cover the communication between the client that initiates the request and the firewall / load balancer that handles the traffic. Load balancers often provide efficient support mechanisms for transport-level decryption and encryption which is to be preferred over having a WebLogic domain handling transport-level decryption and encryption.

Before these are used, make sure that the OHI Components applications web services are properly secured in accordance with your organization’s security requirements and standards.

Minimal Required Security for OHI Components Applications Web Services

The minimal security measures for OHI web services should comprise the following:

- Encrypt any message using SSL in order to assure message confidentiality. Note that OHI web services may receive or send messages that contain protected health information. Even within the intranet or internal network the messages that are exchanged should be encrypted.
- At the network level, e.g. in a switch or router, configure that OHI Components applications web services can only be accessed through the load balancer or web server that is set up to regulate any access to OHI. OHI Components applications web services should not be accessible from any other device within the organization. Additional security measures to allow or prevent message traffic from certain clients within the organization may be configured in the load balancer or web server.

5.2 Options for securing OHI Components web services

By default OHI Components applications web services verify that the request is executed by an authenticated user. If that is not the case then the server will not process the request and an HTTP 401 – Not Authorized response is returned.

This is implemented for SOAP and RESTful services in a different manner:

- SOAP services: OHI Components applications only verify that the request is executed by an authenticated principal. OHI Components applications do not assume neither enforce the use of a specific authentication mechanism. It is the responsibility of the customer to make sure that the authentication is properly handled.
- RESTful services: the RESTful services in OHI Components applications' HTTP API make use of Basic Authentication as the default authentication mechanism. Failing to pass an “Authorization” HTTP header or passing in Base64-encoded credentials that did not pass authentication will result in the server challenging the client for username & password credentials.

Authentication for web services can be enforced in many different ways. The following paragraphs describe some options.

Applying SOAP WS-Security Policies

OHI Components applications support the WS-Security 1.1 standard, also know as WSS. WSS policies can be applied (or attached to the OHI Components SOAP services) in two different ways:

- Through Oracle WebLogic WSS policies.
- Through the use of Oracle Web Services Manager (OWSM), a separately licensed product.

Oracle WSM must always be enabled on the WebLogic domain in which OHI Components applications are executed. Note that OWSM should only be licensed if the OWSM WSS policies are applied. OWSM can be selected upon domain creation, or added to a domain by extending it at a later stage.
In order to enable OWSM in a domain, an MDS schema must be installed using Oracle's Repository Creation Utility (RCU). MDS means Oracle Metadata Services, and provides a repository for Fusion Middleware components, such as Oracle ADF and OWSM. It is important that the RCU version matches the WebLogic version that is
used for executing an OHI Components application. The correct version of the RCU is mentioned in the WebLogic documentation. For example, for WebLogic 10.3.6 with the 11.1.1.7 ADF runtime version the RCU can be determined from the Oracle® Fusion Middleware Download, Installation, and Configuration ReadMe
11g Release 1 (11.1.1.7.0)[1].

For additional information on using WSS policies please consult the following resources:

- For WebLogic web services policies, see guide Securing WebLogic Web Services for Oracle WebLogic Server[2].
- For OWSM web services policies, see guide Security and Administrator's Guide for Web Services[3].

Using the Oracle API Gateway (OAG)

Where WSS policies are enforced at the WebLogic domain, API gateways like OAG, offer a more centralized form of protection between. The gateway is positioned at the boundary of untrusted and trusted zones and as such provides DMZ-class security at the service perimeter

of service oriented environments. OAG can be used to implement OAuth for OHI Components applications' HTTP API for example.

Disabling the default Web Services security settings

It is possible to disable the default OHI Components applications web services security by setting property ‘ohi.ws.require.authentication’ to false in the application's properties file. In order for these changes to take effect, the application needs to be restarted.

Merely disabling authentication leaves the web services unsecured. This should only be done if web services are properly secured in a different way.

1. http://docs.oracle.com/cd/E23104_01/download_readme_ps6/download_readme_ps6.htm
2. http://docs.oracle.com/cd/E17904_01/web.1111/e13713/toc.htm
3. http://docs.oracle.com/cd/E17904_01/web.1111/b32511/toc.htm

6 HIPAA Compliance

This chapter covers HIPAA and HITECH compliance for OHI Components applications.

6.1 Oracle and HIPAA

The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) requires Covered Entities to implement processes and safeguards designed to protect the privacy and security of electronic protected health information (ePHI or simply PHI).
HIPAA has evolved through subsequent legislation:

- The Privacy Rule was added in December 2000. It gives patients rights over their health information and sets rules for how information is used, shared, accessed and protected. Moreover, the rule explicitly lists ePHI identifiers like name and social security number.
- The Security Rule was added in February 2003.
- The HITECH Act that was passed in February 2009 which dictates how the privacy and security of health information must be managed by Covered Entities and Business Associates (or BAs).
- The Omnibus Rule that is effective as of September 2013. Among other things, it extended the definition of a BA to parties that create, receive, maintain and transmit PHI on behalf of a Covered Entity.

By definition of the Omnibus Rule Oracle is considered a BA when Oracle performs functions on behalf of a a Covered Entity that involve access to PHI. That is even the case when no specific customer Business Associate Agreement (or BAA) is in place.
To address the requirements coming from this, Oracle implemented:

- standard BAAs with its suppliers as well as standard BAAs for use by Oracle's customers that enables them to fulfill their requirements.
- processes that address compliance with the administrative, physical and technical requirements of the Security Rule.
- annual audit that are conducted by a third party to assess Oracle's level of compliance. This includes cloud services and consulting engagements.

6.2 HIPAA by Design

HIPAA and HITECH require covered entities to

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

The Privacy rule is more functional in nature and will be an integral part of the design of the application/service as this is exposed to the user community. The Security Rule is a series of administrative, technical, and physical security safeguards and related policies and procedures designed to require covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. Both rules impact the development

process but it is the Security rule that has proved more intractable as there are requirements to not only follow the rule but to show that the rule is being followed.

Covered entities are required to comply with every Security Rule, however, the Security Rule categorizes certain standards as "addressable," while others are "required."

- Required - These implementation specifications must be implemented.
- Addressable - The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is **reasonable and appropriate** for that covered entity. If it is not, the Security Rule allows the covered entity to **adopt an alternative measure that achieves the purpose of the standard**, if the alternative measure is reasonable and appropriate.

There are a number of Administrative Standards and Technical Standards that have a direct impact on the development process. Examples of these are listed in the following table. The last column contains examples that illustrate how the OHI Components applications development process or architecture (including the Oracle technology stack) handles the rule. Alternatively, it identifies how customers implementing OHI Components applications should deal with the rule.

Rule	Implementation	Oracle & OHI Solution
ADMINISTRATIVE - Security Management Process - 164.308 (a)(1) Risk analysis (Required)	Assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the covered entity or business associate.	Oracle Global Product Security review for every major release of an OHI Components application. Specific security audits for Oracle Cloud deployments.
TECHNICAL - Security Management Process 164.312(a) -Mixed	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). (2) Implementation specifications: (i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity. (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. (iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information	By default, OHI Components applications only accept requests from authenticated, identifiable users. OHI Components applications provide role based authorization to associate roles with users. The WebLogic runtime environment implements account inactivity / session timeout. Users have to re-authenticate in order to continue working. Any web traffic should be encrypted using TLS/SSL, at least from client to load balancer / DMZ (more on this elsewhere in this guide). For data at rest the Oracle database offers the Transparent Data Encryption feature.

TECHNICAL - Audit Controls 164.312 (b) (Required)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	OHI Components applications record access, even read-only access, to PHI data. For example: • OHI Claims logs which users have viewed specific claims • OHI Alternative Reimbursement logs which users have viewed data for specific members
TECHNICAL - Integrity 164.308 (a)(3) (Required)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Users who have access to the ePHI should be minimized. For that, customers should apply the Principle of Least Privilege (see elsewhere in this guide) and the Principle of Minimum level of access. OHI Components applications require that users are explicitly provisioned to access an application (through the provisioning service). Moreover, users should not be granted access to system functions (and associated data) that they do not need for their work.
TECHNICAL - Transmission Security 164.312 (e) (Mixed)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. (2) Implementation specifications: (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Customers should use TLS/SSL to effectively protect data in transit. Consider the use of Oracle Advanced Security SQLnet encryption between the mid-tiers and the database if required.

6.3 HIPAA and OHI Development and Consulting resources

OHI Development and Consulting resources interact with customers in various ways. Customers make use of OHI systems through Cloud based offerings or using on-premise installed systems. OHI staff may be required to access OHI environments for support or maintenance purposes. Oracle staff utilizes dedicated systems and environments specifically designed to retain PHI. For example, any data stored on Oracle consulting laptops is encrypted; Oracle Support systems are regularly audited for compliance.

All Oracle employees are required to take the Information Protection Awareness training upon employment and every two years thereafter.
Oracle employees with access to ePHI environments are required to take annual HIPAA trainings. Training is provided through Oracle University and completion is tracked.