Oracle® Insurance Claims Adjudication for Health

Security Guide

Release 2.12.4.0.0

E23647-01

February 2013

ORACLE®

Oracle Insurance Claims Adjudication for Health Security Guide, Release 2.12.4.0.0

E23647-01

Contents

List of Figures

List of Tables

Preface

This guide helps to install, configure and manage Oracle Health Insurance (OHI) Applications in a secure manner.

Audience

This document is intended for IT Architects and System Administrators.

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.

Related Documents

For more information, see the following documents:

- *The Installation Guide for the specific Health Insurance Application*
- *Securing a Production Environment for Oracle WebLogic Server 10.3.4*(http://docs.oracle.com/cd/E17904_01/web.1111/e13705/toc.htm)
- *Securing Oracle WebLogic Server* (http://docs.oracle.com/cd/E17904_01/web.1111/e13707/toc.htm)
- *Oracle Database 11.2 Security Guides* (http://www.oracle.com/pls/db111/portal.portal_db?selected=25)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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) 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.

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.

3

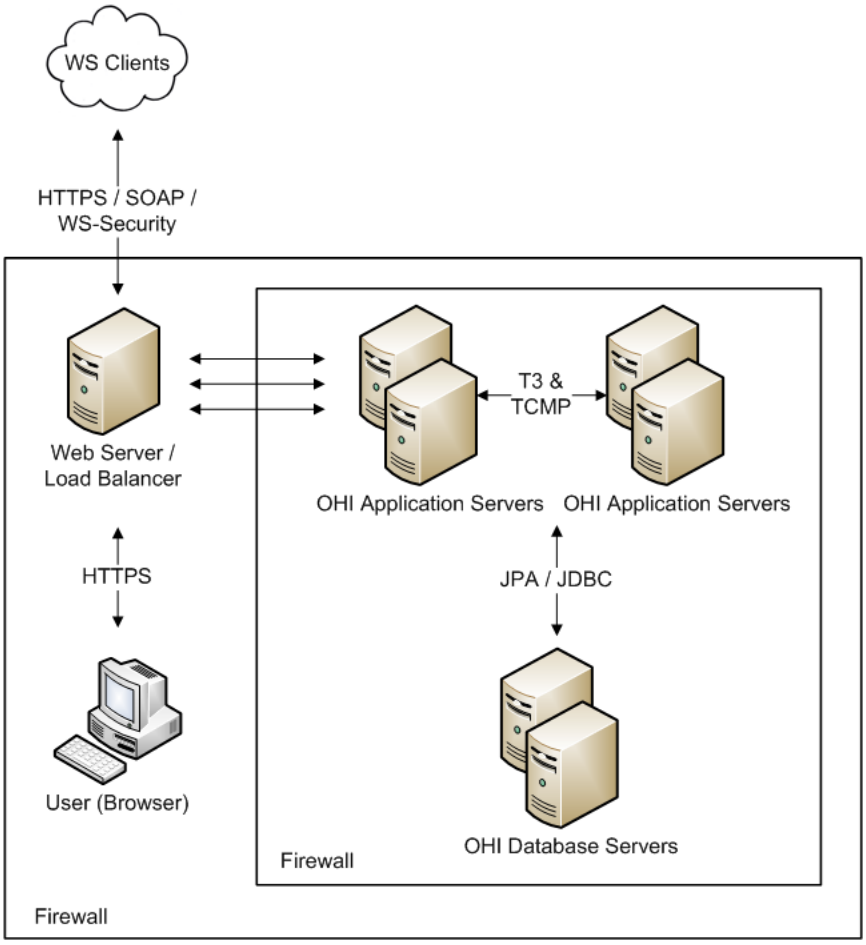
System Deployment

3.1 Network Security in an OHI Environment

When deploying OHI 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.

Figure 3–1 Network security in an OHI environment



A typical OHI 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.

Please make sure 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.

3.1.1 Accessing the User Interface outside the Firewall

OHI 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.

3.1.2 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 WS-Security policies to enforce authentication and to guarantee integrity and confidentiality of messages.

3.1.3 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.

Caution: Oracle recommends that all OHI 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.

3.1.3.1 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
- http://download.oracle.com/docs/cd/E17904_01/apirefs.1111/e13952/taskhelp/security/ConfigureKeystoresAndSSL.html

3.1.3.2 Configuring SSL for Authentication: using LDAPS

OHI 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 and Oracle Internet Directory (OID). OID supports three SSL Modes that are listed in the following table.

Table 3–1 Supported SSL Authentication Methods

SSL Authentication Method	Description	Supported by OHI Applications?
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 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 OHI 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 Application.

- Export the Self-Signed root certificate from the Self-Signed Wallet using the Fusion Middleware Enterprise Manager.
- Make a backup of the JVM's cacerts file.
- 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 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.

3.1.3.3 Configuring SSL for Coherence

OHI uses 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 URLs:

- http://docs.oracle.com/cd/E24290_01/coh.371/e22841/toc.htm

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.

> **Note:** OHI applications do not store password data.

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 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.

> **Note:** OHI does 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 Operations Guide explains the configuration for that.

For additional information on authentication please visit the following sources:

- The OHI Installation Guide explains the configuration of an authentication provider 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 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 provisioning service.

For additional information on configuration of user access right please read the User Access Implementation Guide.

4.4 Cookies

An OHI application is accessed by users through a browser. Because OHI uses 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.

5

Web Services Security

Out-of-the-box, OHI web services are not secured. This chapter explains how OHI web services can be used in a secure manner.

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.

Table 5–1 Web Services Security

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 SOAP message is secure even when the transmission involves one or more intermediaries. The SOAP 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 web services are not secured.The remaining paragraphs in this chapter outline different options to secure OHI web services.

WARNING: Before these are used, make sure that OHI web services are properly secured in accordance with your organization's security requirements and standards.

5.2 Minimal Required Security for OHI 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 these should be encrypted.
- At the network level, e.g. in a switch or router, configure that OHI web services can only be accessed through the load balancer or web server that is set up to

regulate any access to OHI. OHI 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.

5.3 Applying WS-Security Policies

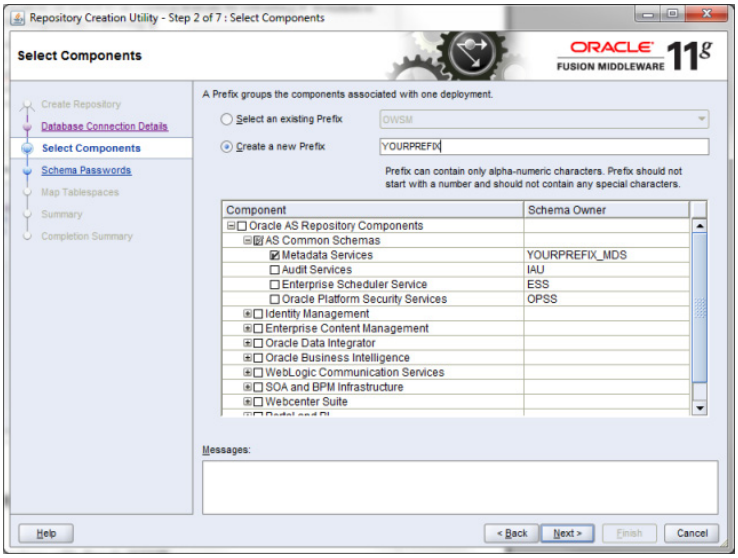
OHI applications support the WS-Security 1.1 standard, also know as WSS. WSS policies can be applied (or attached to the OHI web services) in two different ways:

- Through Oracle WebLogic WSS policies.
- Through the use of Oracle Web Services Manager (WSM).

Oracle WSM must always be enabled on the WebLogic domain in which OHI 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. Installation of OWSM comprises the following steps:

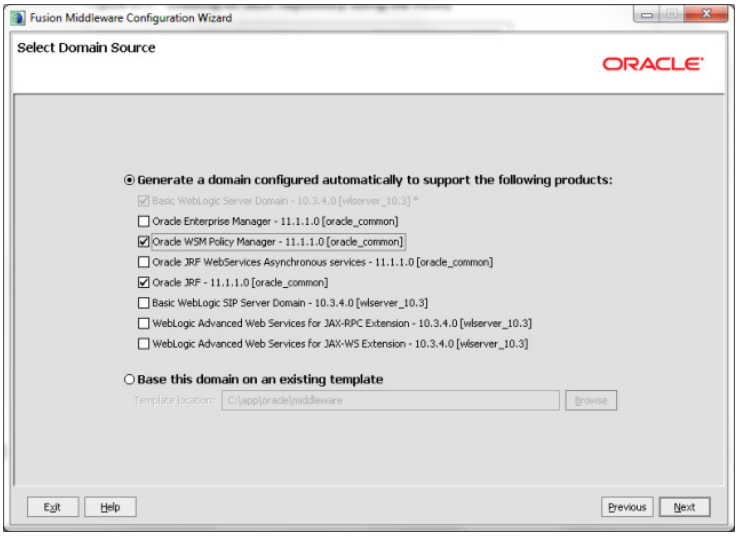
1. First, in order to enable OWSM in a domain, an MDS schema must be installed using Oracle Repository Creation Utility (RCU). MDS means Oracle Metadata Services, and provides a repository for Fusion Middleware components, such as OWSM. It is important that the RCU version matches the WebLogic version that is used for executing an OHI application. The OHI Installation Guide for a specific release mentions the required RCU version. In the RCU, select the Metadata Services as shown in the following figure:

Figure 5–1 Creating an MDS Repository using the RCU



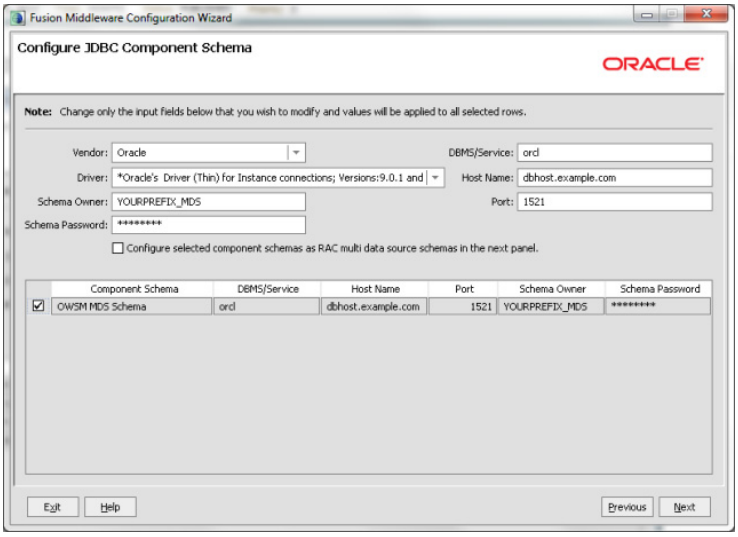
2. Next, when installing the domain using the Fusion Middleware installer, on the "Select Domain Source" screen select the checkbox "Oracle WSM Policy Manager 11.1.1.0 (oracle_common)":

Figure 5–2 Creating a Domain with OWSM



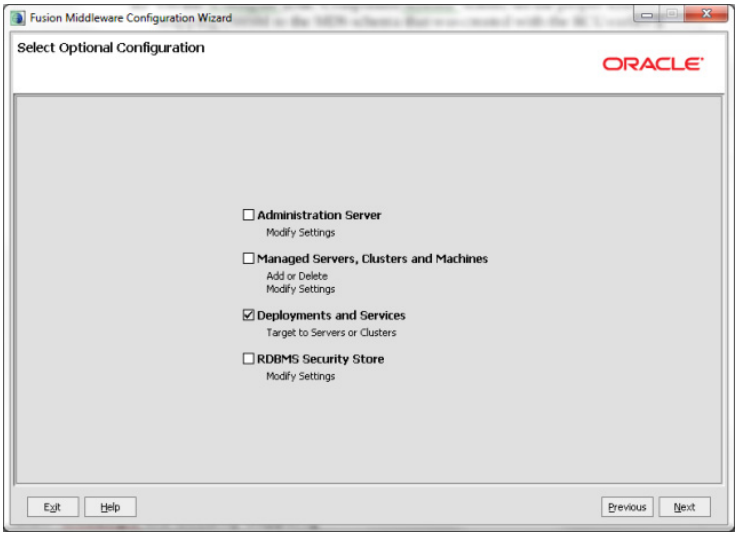
3. On the "Configure JDBC Component Schema" screen, set the proper schema for mapping OWSM to the MDS schema that was created with the RCU earlier:

Figure 5–3 Selecting the MDS Schema



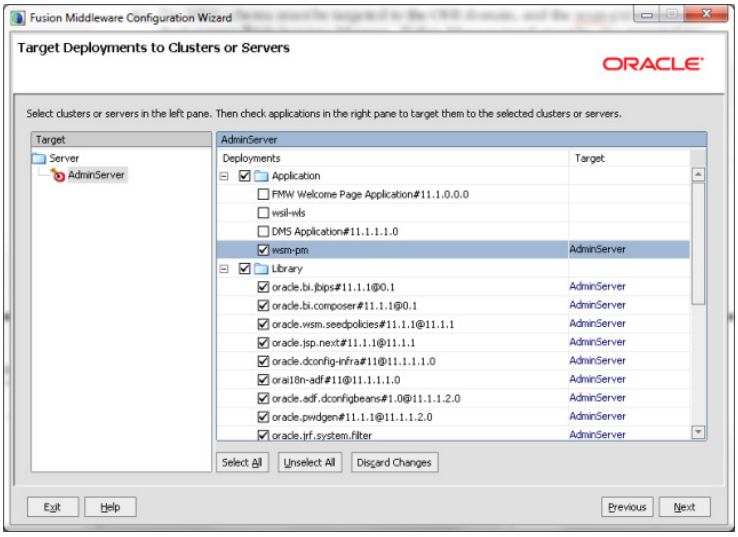
4. The MDS schema must be targeted to the OHI domain, and the wsm-pm deployment (Web Services Manger – Policy Management) must be also targeted to it. This can be done on the Deployments and Services tab. On the "Select Optional Configuration" screen, check the box "Deployments and Services":

Figure 5–4 Selecting the 'Deployment and Services' Option



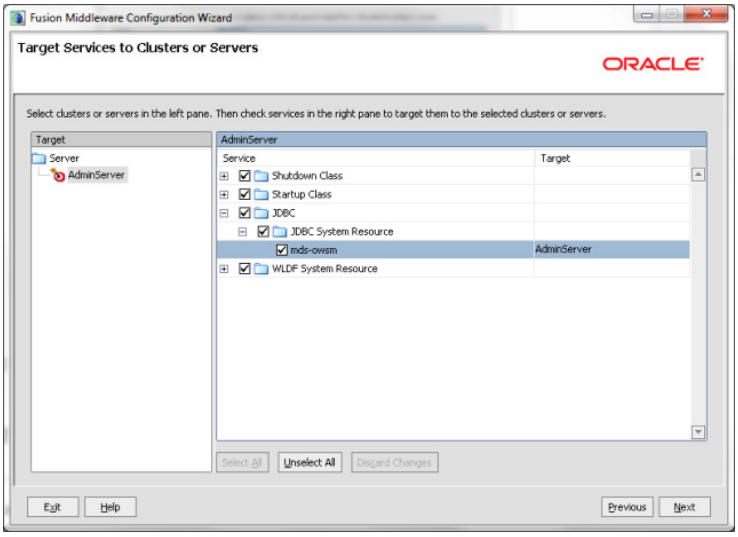
5. On the "Target Deployments to Clusters or Servers" screen, the deployment called "wsm-pm" must be targeted to the Admin Server (and any managed server that runs OHI).:

Figure 5–5 Targeting the wsm-pm deployment



6. On the "Target Services to Clusters or Servers" screen, the JDBC data source mds-owsm must be targeted to the Admin Server (and any managed server that runs OHI).:

Figure 5–6 Targeting the JDBC deployment for MDS



7. Finish creating the domain and installing the OHI application to be able to apply WebLogic or OWSM WS-Security policies to OHI web services. To validate that the policies are available for applying to OHI web services:
   - Open the OHI deployment in the WebLogic console
   - Select one of the web services
   - In the Settings page for the web service open the Configuration tab and the WS-Policy tab below
   - Determine if the policy should be applied to the service endpoint or to a specific operation
   - Finally, determine what kind of policy will be used, either a WebLogic policy or an OWSM policy (OWSM licenses required):

Figure 5–7 Determine the type of Policy

For additional information on using WSS policies please visit the following URLs:

- For WebLogic web services policies, see guide Securing WebLogic Web Services for Oracle WebLogic Server (http://docs.oracle.com/cd/E17904_01/web.1111/e13713/toc.htm).
- For OWSM web services policies, see guide Security and Administrator's Guide for Web Services (http://docs.oracle.com/cd/E17904_01/web.1111/b32511/toc.htm)