

**Application Integration Architecture: Agile PLM
PIP for Oracle E-Business Suite**

Security Guide

Release 3.6

E88838-03

August 2018

Application Integration Architecture: Agile PLM PIP for Oracle E-Business Suite Security Guide, Release 3.6
E88838-03

Copyright © 2013, 2018, Oracle and/or its affiliates. All rights reserved.

Primary Author: Oracle Corporation

Contributing Author: Edlyn Sammanasu

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.

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.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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.

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.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	v
Audience.....	v
Documentation Accessibility	v
Related Documents	v
Conventions	v
 1 Document Scope	
Documentation Audience.....	1-1
Guide to this Document.....	1-1
 2 Understanding Security for Agile PIP for EBiz	
Agile PIP for EBiz Overview.....	2-1
Introduction to Security	2-2
Service-to-Service Security.....	2-3
Transport-Level Security.....	2-3
Message-Level Security.....	2-3
 3 Security Implementation for Agile PIP for EBiz	
Overview of PIP Security.....	3-1
PIP Security Policy	3-1
Interoperability with Agile Web Service Security	3-2
Interoperability with Ebiz	3-3
WSS Configurator	3-3
Starting the Web Services Security Configurator	3-4
Using the Web Services Security Configurator	3-4
Viewing the Current Web Services Security Policy	3-4
Updating to the Agile PLM 9.3.6/ Agile PLM 9.3.5/ Agile PLM 9.3.4 Security Policy	3-5
Restoring Web Services Security Policy.....	3-5
Using MDS to Switch Agile Protocol	3-5
Setting the SSL Environment.....	3-6

Preface

The integration between Agile PLM and Oracle E-Business Suite is designed to enable the product development process, as well as address the primary use cases around the synchronization of product content information between Agile Product Collaboration and Oracle Manufacturing.

Audience

This document is intended for administrators of the Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite: Design to Release.

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 that have purchased support 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

Oracle's Agile PLM PIP for Oracle E-Business Suite documentation set includes Adobe® Acrobat PDF files. The Oracle Technology Network (OTN) Web site <http://www.oracle.com/technetwork/documentation/agile-085940.html> contains the latest versions of the Agile PLM PDF files. You can view or download these manuals from the Web site, or you can ask your Agile administrator if there is an Agile PLM Documentation folder available on your network from which you can access the Agile PLM documentation (PDF) files.

Conventions

The following text conventions are used in this document:

- **AIA:** Application Integration Architecture
- **Agile (PLM):** Agile Product Lifecycle Management
- **EBiz:** E-Business Suite

- **Agile PIP for EBiz:** Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Document Scope

This document provides Oracle Agile PIP for EBiz administrators with the information needed to understand Agile PIP for EBiz security.

Documentation Audience

This document is written for IT users and Oracle Agile PIP for EBiz administrators who will be setting up Oracle Agile PIP for EBiz. It is assumed that those reading this documentation have a solid understanding of security concepts. The audience should also have basic knowledge of Oracle Agile PIP for EBiz.

Guide to this Document

This guide provides information needed to help you to understand Oracle AIA Agile PLM for Oracle EBS security.

The guide is organized as follows:

- ["Understanding Security for Agile PIP for EBiz"](#) on page 2-1 gives an overview of security fundamentals related to Agile PLM for EBiz.
- ["Security Implementation for Agile PIP for EBiz"](#) on page 3-1 provides the necessary details on how to implement security for Agile PIP for EBiz.

Understanding Security for Agile PIP for EBiz

This chapter describes the fundamentals of security related to Agile PIP for Ebiz.

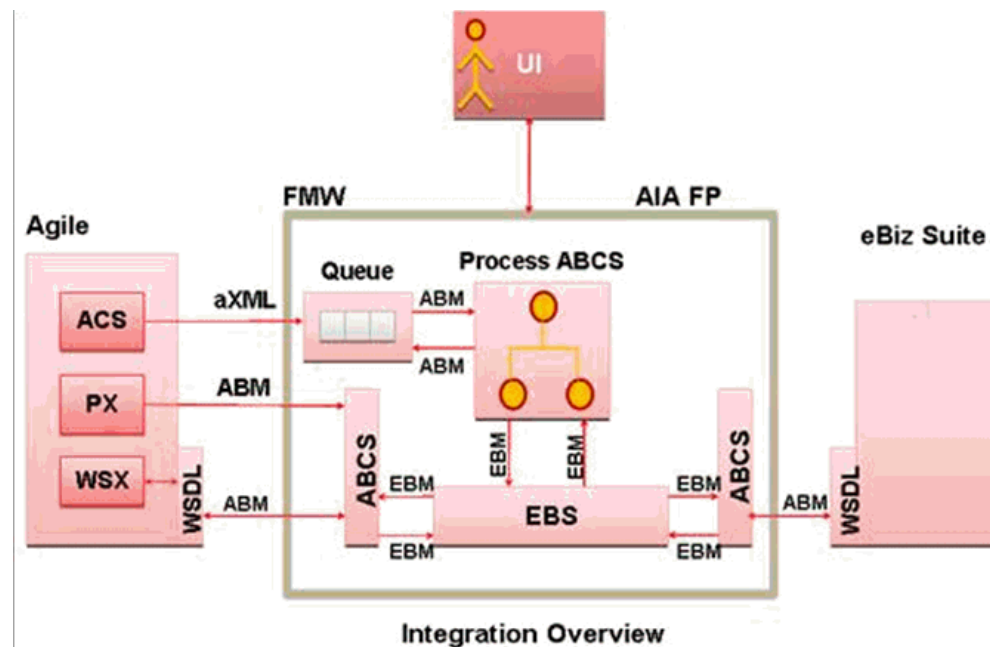
Agile PIP for EBiz Overview

The integration between Agile PLM and Oracle E-Business Suite is designed to enable the product development process and address the primary use cases around the synchronization of product content information between Agile Product Collaboration and Oracle Manufacturing. This allows for rapid implementation of Oracle's next-generation integrated enterprise PLM processes that help the customers reduce costs and any risks associated with typical third-party and custom integrations.

The Agile PLM pre-built integration for Oracle E-Business Suite includes the following functions:

- Manufacturing release of new product definition and product launch.
- Change management of previously launched products.
- Bidirectional synchronization of engineering change status and material attribute information from Oracle Manufacturing to Agile PLM.
- Monitoring and control of the change processing and validation queues.

[Figure 2-1](#) illustrates the Agile PLM to Oracle E-Business Suite integration architecture.

Figure 2–1 Agile PLM Business Process Flow

For more information, see the *Oracle Application Integration Architecture Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite: Design to Release Implementation Guide*.

Introduction to Security

Agile PIP for EBiz is based on the Foundation Pack. The Foundation Pack is a part of the AIA framework, so AIA security can be applied to Oracle Agile PIP for EBiz.

AIA provides support for all security-related functions including:

- Identification
- Authentication (verification of identity)
- Authorization (access controls)
- Privacy (encryption)
- Integrity (message signing)
- Non-repudiation
- Logging

The service-oriented architecture (SOA)-based integration approach allows for clear separation between the interface and the actual business logic. This provides the security architect with a number of choices in deploying security for SOA and web services.

For example, a SOAP web service interface, such as `ProcessEngineeringChangeOrderAgileReqABCS`, can be hosted as a proxy instead of the real endpoint that hosts the business logic implementation. The gateway proxies communication to and from the web service, and performs security functions on behalf of the service endpoint. The actual endpoint is virtualized. Even though the

client thinks it is talking directly to the service provider, it communicates through the proxy.

Service-to-Service Security

Because a typical interaction in the Oracle AIA framework is part of multiple discrete interactions involving a service requester, client-specific Application Business Connector Service (ABCS), Enterprise Business Service, server-specific ABCS and the service provider, choosing a security model plays a critical role.

Oracle AIA architecture enables you to choose one over the other at the implementation time for each of the transactions.

Adoption of the industry-standard WS-Security security model is possible, provided that all participating applications in the transactions provide inherent support.

Transport-Level Security

Existing technologies such as SSL can be used to secure the transport channel. SSL enables two applications to securely connect over a network and authenticate each other. It also enables you to encrypt the data exchanged between the applications. In Oracle's Web Services Security model, this transport security mechanism can be used to provide point-to-point security, data integrity, and data confidentiality.

See *Fusion Middleware Concepts and Technologies Guide for Oracle Application Integration Architecture Foundation Pack* for more information.

Message-Level Security

Oracle AIA places strong emphasis on message-level security. For a web service, XML encryption provides security for applications that require a secure exchange of data. While SSL was considered the standard way to secure data exchanges, it has limitations. For example, assume that a document visits several web services before hitting its eventual endpoint. By using XML encryption, the document can be encrypted while at rest or in transport. Encrypting only portions of a document instead of the whole document is also possible.

Oracle AIA leverages web service administration tools such as Oracle Web Services Manager (OWSM) in a non-intrusive manner to ensure the validity, as well as safety, of the XML messages exchanged between services. This methodology ensures that no enforcement of web services security is in silo mode. Integration architects and developers can focus on integration logic, and the security architects and administrators can focus on security and management. Having security policies enforced through a centralized tool enables the administrators to ensure that the corporate rules are applied, as well as to apply the policy changes centrally instead of applying them in each of the web services.

A typical web service security can have multiple policies attached that can:

- Decrypt the incoming XML message
- Extract the user's credentials
- Perform an authentication for this user
- Perform an authorization check for this user and this web service
- Write a log record of the preceding information
- Pass the message to the intended web service, if all steps are successful

Security Implementation for Agile PIP for EBiz

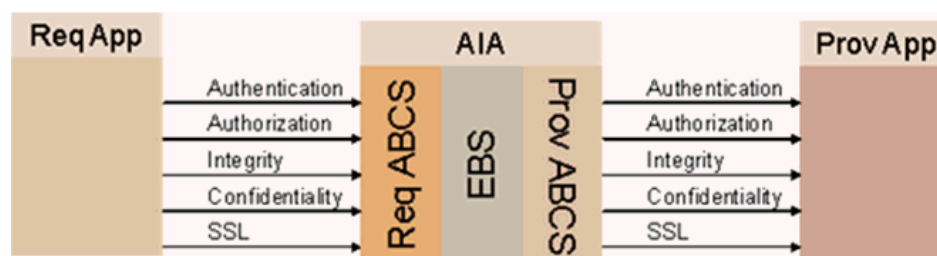
This chapter gives a general picture of PIP security, and describes how PIP security interacts with Agile and Ebiz Web Services.

Overview of PIP Security

The AIA framework provides the following methods to secure the service-to-service interaction:

- Identify clients through authentication.
- Secure messages through encryption.
- Avoid message tampering with digital signatures.
- Encrypt the channel through SSL.

Figure 3–1 High-level Security Architecture



Agile PIP for EBiz 3.6 is shipped with this security implemented, except SSL, which needs manual configuration. OWSM already helps PIP to implement the security methods, and OWSM provides multiple policies to protect web services. The following sections focus on which policies are used in Agile PIP for Ebiz, and how to operate with Agile/Ebiz security.

PIP Security Policy

Since PIP is based on the AIA framework, all AIA policies can be used by PIP. The following is a list of policies which are used in Agile PIP for EBiz:

- Global Service Policy applied:
 - oracle/aia_wss_saml_or_username_token_service_policy_OPT_ON - This is a cloned copy of oracle/wss_saml_or_username_token_service_policy with Local

Optimization set to ON. This is needed for local optimization to work when both client and service composites are co-located.

- Global Service Client Policy applied:
oracle/aia_wss10_saml_token_client_policy_OPT_ON
- Other Service Policies applied:
 - oracle/aia_wss_saml_or_username_or_http_token_service_policy_OPT_ON - This is a cloned copy of oracle/wss_saml_or_username_token_service_policy with Local Optimization set to ON and HTTP basic authentication added as an additional option. Clients such as ODI that do not have the infrastructure to use web services security can call this service using HTTP basic authentication.
 - oracle/no_authentication_service_policy - The oracle/no_authentication_service_policy policy is to those services that do not need authentication.
- Other Service Client Policies applied:
 - oracle/aia_wss_saml_or_username_or_http_token_service_policy_OPT_ON
 - oracle/aia_wss10_saml_token_client_policy_OPT_ON
 - oracle/wss_username_token_client_policy
 - oracle/wss_http_token_client_policy

Interoperability with Agile Web Service Security

Agile 9.3.4, 9.3.5 and 9.3.6 provide a tool to enable security for Web Services in running time. Refer to the *Agile Product Lifecycle Management Security Guide* and follow the steps to enable/disable the security for Agile PLM web services.

When interacting with an Agile web service that is enabled for WS-security, you must add a security header in the SOAP header with all the information needed for security functions. Based on the security of the Agile service, you must add information for any combination of authentication, encryption and integrity. The following table lists the certified policies:

Table 3–1 Certified Policies

Composite Name	Service Name	Certified Policies
ProcessEngineeringChangeOrderAgileReqABCImpl	ChangeABSService TableService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
ProcessItemListInitialLoadAgileABF	BusinessObjectService ItemABSService TableService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
SyncBillOfMaterialsConfigurationListAgileProvABCImpl	ConfiguratorTerminationService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy

Table 3–1 (Cont.) Certified Policies

Composite Name	Service Name	Certified Policies
UpdateEngineeringChangeOrderListAgileProvABCImpl	ChangeABSService ChangeStatusService MergeABSService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
UpdateItemBalanceListAgileProvABCImpl	ItemABSService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
UpdateItemListAgileProvABCImpl	ItemABSService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
ValidateEngineeringChangeOrderListAgileReqABCImpl	ChangeABSService TableService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy

Note: The out-of-box policy for Agile web services is oracle/wss_http_token_client_policy. If you are running Agile PLM in a non-Web Services Security environment, the Web Services Security Configurator does not need to be run. For more detailed steps, refer to the *Oracle AIA Agile PLM for Oracle EBS: Design to Release Install Guide*.

Interoperability with Ebiz

When interacting with an EBiz web service that is enabled for WS-security, you must add a security header in the SOAP header with all the information needed for security functions. Based on the security of the EBiz service, you must add information for any combination of authentication, encryption and integrity. The following table lists the certified policies:

Table 3–2 Certified Policies

Composite Name	Service Name	Certified Policies
GenerateItemNumberService	GenerateItemNumberService	oracle/wss_username_token_client_policy

Note: The out-of-box policy for EBiz web services is oracle/wss_username_token_client_policy.

WSS Configurator

The Web Services Security (WSS) Configurator integrates the Design to Release: Agile - EBS pre-built integration with the Agile PLM 9.3.6/Agile PLM 9.3.5/Agile PLM 9.3.4 security environment. If you are running Agile PLM in a non-WSS environment, the Web Services Security Configurator does not need to be run.

Starting the Web Services Security Configurator

After you install the Agile PLM PIP, the Web Services Security Configurator files are located in the \$SERVICES_LOCATION/pips/AgileToEbiz/Tool directory.

Make sure that the WebLogic Server is started and that the WebLogic console is accessible before running the configurator tool.

To start the Web Services Security Configurator:

1. Open a Command Prompt window.
2. Make sure the JAVA_HOME and WLS_HOME environment variables point to the correct locations.
3. Change to the \$SERVICES_LOCATION/pips/AgileToEbiz/Tool directory.
4. Open the wssconfig-d2rpip file and update the value of the wlstlocation variable, based on the example path in the file.
5. Run the wssconfig-d2rpip script.

Using the Web Services Security Configurator

When the Web Services Security Configurator initializes, you have the option to review your current security policy, to support the Agile PLM 9.3.6/Agile PLM 9.3.5/Agile PLM 9.3.4 security policy, or to restore the security policy to the default policy (oracle/wss_http_token_client_policy).

For more information on the Agile PLM 9.3.6 /Agile PLM 9.3.5 /Agile PLM 9.3.4 security policy, see the Agile Product Lifecycle Management Security Guide.

```
*****
*      Agile PLM D2R PIP Web Services Security Configurator      *
*****

[1] : View current web services security policy
[2] : Set WS Security Policy to 'oracle/wss_username_token_over_ssl_client_policy'
[3] : Restore WS Security Policy to default 'oracle/wss_http_token_client_policy'

Please enter the option to proceed:
1
```

Viewing the Current Web Services Security Policy

To view the current web services security policy:

1. Enter 1 at the prompt.
2. Enter your SOA server URL, username, and password at the designated prompts.

Note: If you are running a standalone server, the SOA server URL should be the URL of the Admin Server. If you are running a cluster environment, the SOA server URL should be the URL of one of the Managed SOA servers.

3. Press Enter

The current web services security policy displays and the configurator tool closes. If you need to update or rollback your security policy, you must restart the tool.

Updating to the Agile PLM 9.3.6/Agile PLM 9.3.5/Agile PLM 9.3.4 Security Policy

Enter option 2 on the Web Services Security Configurator to update your security policy to the Agile PLM 9.3.6/Agile PLM 9.3.5/Agile PLM 9.3.4 policy (oracle/wss_username_token_over_ssl_client_policy). After enter the required information, the updated policy is attached and the endpoint address is updated for the related web services.

```
Session started for modification.
The policy subject is selected for modification.
Policy reference "oracle/wss_username_token_over_ssl_client_policy" added.
The policy set for subject "/WLS/soa_domain/soa-infra/default/ValidateEngineeringChangeOrderListAgileReqABCSImpl#1.0
[SCA-Reference(ChangeABSServiceChangeABS)]" was saved successfully.

Session started for modification.
The policy subject is selected for modification.
Policy reference "oracle/wss_username_token_over_ssl_client_policy" added.
The policy set for subject "/WLS/soa_domain/soa-infra/default/ValidateEngineeringChangeOrderListAgileReqABCSImpl#1.0
[SCA-Reference(TableService#Table)]" was saved successfully.

*****
* Web Services security policy is attached for AgilePLM PIP calls to Agile *
* PLM 9 Web Services. You can view the configuration by logging in to EH and *
* clicking SOA->soa-infra->default->> Composite and selecting Policies tab *
*****
```

You can validate the updated policy with Oracle Enterprise Manager.

Restoring Web Services Security Policy

If there is a need to restore the default web services security policy (oracle/wss_http_token_client_policy), enter option 3 on the Web Services Security Configurator. After entering the required information, the default policy is attached and the endpoint address is updated for the related web services.

```
Session started for modification.
The policy subject is selected for modification.
Policy reference "oracle/wss_http_token_client_policy" added.
The policy set for subject "/WLS/soa_domain/soa-infra/default/ValidateEngineeringChangeOrderListAgileReqABCSImpl#1.0
[SCA-Reference(TableService#Table)]" was saved successfully.

I

7/7 ValidateEngineeringChangeOrderListAgileReqABCSImpl Composite Restore Done
All Restore Action Done
```

Using MDS to Switch Agile Protocol

To use MDS to Switch the Agile Protocol:

1. Download the Configuration File from MDS.
2. Update \$DOMAIN_LOCATION/soa/aia/MDSUtils/DownloadMetadataFileDP.xml content:

```
<?xml version="1.0" standalone="yes"?>
<DeploymentPlan>
<Configurations>
<DownloadMetadataFile downloadLocation="{env.DOMAIN_ LOCATION}/soa/aia/bin/"
fileToDownload = "/soa/configuration/default/AIAConfigurationProperties.xml"
wlserver="fp" />
</Configurations>
</DeploymentPlan>
```

```
source <DOMAIN_LOCATION>/soa/aia/bin/aiaenv.sh
```

- ```
ant -f $SOA_HOME/aiafp/Install/AID/AIAInstallDriver.xml
-DPropertiesFile=$DOMAIN_LOCATION/soa/aia/bin/AIAInstallProperties.xml
-DDeploymentPlan=$DOMAIN_LOCATION/soa/aia/MDSUtils/DownloadMetaDataFileDP.xml
```
3. Update AIAConfigurationProperties.xml and AIAInstallProperties.xml in \$DOMAIN\_LOCATION/soa/aia/bin.
    - If you are updating to the Agile PLM 9.3.6/Agile PLM 9.3.5/Agile PLM 9.3.4 security policy with web service security configurator:
      - In /properties/participatingapplicatons/agile of AIAInstallProperties.xml, update port to https port and update protocol to https.
      - In AIAConfigurationProperties.xml, replace all Agile URLs from http to https. Fourteen (14) locations should be replaced.
    - If you are restoring the web service security policy with Web Service Security Configurator:
      - In /properties/participatingapplicatons/agile of AIAInstallProperties.xml, update port to http port and update protocol to http.
      - In AIAConfigurationProperties.xml, replace all Agile URLs from https to http. Fourteen (14) locations should be replaced.
  4. Upload into MDS.
  5. Update \$DOMAIN\_LOCATION/soa/aia/MDSUtils/UpdateMetaDataFileDP.xml content:

```
<?xml version="1.0" standalone="yes"?>
<DeploymentPlan>
<Configurations>
<UpdateMetadataFile wlserver="fp" mdslocation="apps/AIAMetaData/config">
<fileset dir="${env.DOMAIN_LOCATION}/soa/aia/bin">
<include name="AIAInstallProperties.xml" />
</fileset>
</UpdateMetadataFile>
<UpdateMetadataFile wlserver="fp" mdslocation="/soa/configuration/default">
<fileset dir="${env.DOMAIN_LOCATION}/soa/aia/bin">
<include name="AIAConfigurationProperties.xml" />
</fileset>
</UpdateMetadataFile>
</Configurations>
</DeploymentPlan>

source <DOMAIN_LOCATION>/soa/aia/bin/aiaenv.sh
cd $DOMAIN_LOCATION/soa/aia/MDSUtils/
ant -f $SOA_HOME/aiafp/Install/AID/AIAInstallDriver.xml
-DPropertiesFile=$DOMAIN_LOCATION/soa/aia/bin/AIAInstallProperties.xml
-DDeploymentPlan=$DOMAIN_LOCATION/soa/aia/MDSUtils/UpdateMetaDataFileDP.xml
```

## Setting the SSL Environment

### Setting the SSL Environment

After updating the security policy, you must set the SSL environment between Agile PLM 9.3.6/Agile PLM 9.3.5/Agile PLM 9.3.4 and the Design to Release: Agile - EBS pre-built Integration. For more information on installing Agile PLM 9.3.6/Agile PLM

9.3.5/Agile PLM 9.3.4, see Agile Product Lifecycle Management Application Installation Guide, Release 9.3.6/Release 9.3.5/Release 9.3.4.

Here's an example of how to set the SSL environment between Agile PLM 9.3.6 and the Design to Release PIP with self-signed certificates.

### To set the SSL environment for Agile PLM:

1. Create a directory named agile-keystore936 on the machine where the WebLogic files are located.
2. Change to the newly created directory and run the following command to create the agile-keystore.jks file:
 

```
keytool -genkey -keyalg RSA -alias ssl -keystore agile-keystore.jks -keysize 2048 -storepass <password>
```
3. Enter the following information for the key generation command:
 

```
CN=<Weblogic_hostname>, OU=<organizationUnit>, O=<organizationName>, L=<localityName>, ST=<stateName>, C=<countryName>
```
4. Run the following command to create and export the SSL certificate, agile-ssl-cert:
 

```
<password> -alias ssl
```

```
keytool -export -file agile-ssl-cert.cer keystore agile-keystore.jks -storepass <password> -alias ssl
```
5. Run the following command to import the SSL certificate and create the Trust store:
 

```
keytool -import -file agile-ssl-cert.cer keystore agile-trust-store.jks -storepass<password>
```
6. In a web browser, go to [http://<Weblogic\\_hostname:portnumber>/console](http://<Weblogic_hostname:portnumber>/console) to open the WebLogic Console.
7. In the left pane of the Console, select Environment>Servers, then click the Server name on the right pane.
8. From ServerName>Configuration>General, check SSL Listen Port Enabled. The default port is 7002.
9. Select Configuration>Keystores, choose Custom Identity and Custom Trust.
10. In the Identity section, define the following attributes for the identity keystore:
  - Custom Identity Keystore: (Windows example)  
C:\agile-keystore-936\agile-keystore.jks
  - Custom Identity Keystore Type: JKS
  - Custom Identity Keystore Passphrase: <password>
11. In the Trust section, define the following properties for the trust keystore:
  - Custom Trust Keystore: (Windows example)  
C:\agile-keystore-936\agile-trust-store.jks
  - Custom Trust Keystore Type: JKS
  - Custom Trust Keystore Passphrase: <password>
12. Activate the changes in the WebLogic Console.
13. Connect to the Agile PLM system.

After you have configured SSL on the Agile PLM system, you must make the Integration Server trust the Agile Server.

**To make the Integration server trust the Agile Server:**

1. Open a command prompt window and change to the %MW\_HOME%\wlserver\server\lib directory.
2. Copy the agile-ssl-cert.cer file from the Agile PLM server to the Integration server.
3. Run the following command to import agile-ssl-cert.cer in the Integration server's key store using the DemoTrust keystore:  

```
keytool -import -file agile-ssl-cert.cer -alias a9-ssl-cert -keystore
DemoTrust.jks
-storepass DemoTrustKeyStorePassPhrase
```
4. In a web browser, go to [http://<Weblogic\\_hostname:portnumber>/console](http://<Weblogic_hostname:portnumber>/console) to open the WebLogic Console.
5. In the left pane of the Console, select Environment>Servers, then click the Server name on the right pane.
6. Select Configuration>Keystores, choose Custom Identity and Custom Trust.
7. In the Trust section, define the following properties for the trust keystore:
  - Custom Trust Keystore: %MW\_Home%\wlserver\server\lib\DemoTrust.jks
  - Custom Trust Keystore Type: JKS
  - Custom Trust Keystore Passphrase: DemoTrustKeyStorePassPhrase
8. Save Changes.