

Oracle® Insurance Policy Administration

Configuration of SAML 1.1 Between OIPA and OIDC

Version 10.1.2.0

Document Part Number: E59346-01

December, 2014

Copyright © 2009, 2014, Oracle and/or its affiliates. All rights reserved.

Trademark Notice

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

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

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

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 USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software 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.

Where an Oracle offering includes third party content or software, we may be required to include related notices. For information on third party notices and the software and related documentation in connection with which they need to be included, please contact the attorney from the Development and Strategic Initiatives Legal Group that supports the development team for the Oracle offering. Contact information can be found on the Attorney Contact Chart.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. 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 in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Software License and Service Agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Table of Contents

INTRODUCTION.....	4
Customer Support	4
PREREQUISITES	5
CREATING A DOMAIN FOR THE APPLICATIONS	6
CREATING A USER IN THE DOMAIN'S	6
GENERATING AND REGISTERING SSL CERTIFICATES	7
Source Site.....	7
Destination Site	7
CONFIGURING KEYSTORES AND SSL.....	8
Source Site.....	8
Destination Site	9
SAML SOURCE SITE CONFIGURATION	10
Creating the SAML Credential Mapper	10
Configuring the Relying Party Properties	11
Configuring SAML 1.1 on the Source Site	11
SAML DESTINATION SITE CONFIGURATION	13
Creating a SAML Identity Asserter.....	13
Configuring the Asserting Party Properties.....	13
Configuring SAML 1.1 on the Destination Site.....	14
CONFIGURING OIPA AND OIDC	16
Configuring OIPA	16
Configuring OIDC.....	16
TESTING SINGLE SIGN-ON	17
Importing the Certificate to IE	17
Testing the Application.....	17
DEBUGGING THE APPLICATION	18

INTRODUCTION

Security Assertion Markup Language (SAML) is an XML standard used to exchange authentication and authorization data between web domains. Oracle Insurance Policy Administration (OIPA) and Oracle Insurance Data Capture (OIDC) use SAML to facilitate a Single Sign-On (SSO) service between the two applications. This document explains the process for configuring SAML 1.1 for use with these systems.

Customer Support

If you have any questions about the installation or use of our products, please visit the My Oracle Support website: <https://support.oracle.com>, or call (800) 223-1711.

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.

PREREQUISITES

The following prerequisites are needed before SAML 1.1 can be configured for use with OIPA and OIDC:

- Oracle WebLogic Server version 10.3.6
- OIDC Version 5.1.0.0
- OIPA version 10.1.0.0

CREATING A DOMAIN FOR THE APPLICATIONS

Create a domain in the source WebLogic server where OIPA will be deployed. The OIDC application will run in the destination WebLogic server. The following table contains example domain details that will be used for demonstration purposes throughout this document.

	IP Address	Application Name	Port	SSL Port
SAML Source: OIPA	OIPAHostIP	OIPA	OIPAPort	OIPASSLPort
SAML Destination: OIDC	OIDCHostIP	OIDC	OIDCPort	OIDCSSLPort

CREATING A USER IN THE DOMAIN'S

1. Create any OIPA Application user credentials same in the OIPA WebLogic domain at Home > Summary of Security Realms > myrealm > Users and Groups.

The following are example user credentials:

Domain	Realm	Username/Password
OIPA	myrealm	qatester1/qatester1
OIDC	myrealm	qatester1/qatester1

2. On the OIDC WebLogic domain, create a user with the same credentials and add it to the DCDataAdministrators and DEVTest groups.

GENERATING AND REGISTERING SSL CERTIFICATES

Source Site

1. Open a command prompt window.
2. Change the directory to WEBLOGIC_HOME\wlserver_10.3\server\lib.
3. Run the `keytool` command to generate a keystore called `oipakeystore.jks`, as is shown below. Be sure to enter the source server's IP address after `CN=`.

```
keytool -genkeypair -alias oipaalias -keyalg RSA -validity 365 -keysize 2048 -keystore  
oipakeystore.jks -dname "CN=10.184.226.231, OU=Oracle Financial Services, O=Oracle India,  
L=IDC, ST=Hyderabad, C=IN" -storepass oracle123 -keypass oipakeypass
```

4. Run the `keytool` command with the `-export` option to generate a certificate called `oipaalias.der`.

```
keytool -export -alias oipaalias -keystore oipakeystore.jks -rfc -file oipaalias.der -  
storepass oracle123 -keypass oipakeypass
```

5. Run the `keytool` command with the `-import` option to store the certificate in `oipatruststore`.

```
keytool -import -alias oipaalias -file oipaalias.der -keystore oipatruststore.jks -storepass  
oracle123 -keypass oipakeypass -noprompt
```

6. A confirmation message reading, "Certificate was added to keystore" should appear.

Destination Site

To create and register SSL certificates for the destination site, repeat steps 1–6 above, with one difference: Delete the certificate (`oipaalias.der`) that is created for the destination site and replace it with a copy of the certificate that was created for the source site. This will import the source site's WebLogic Server configuration.

CONFIGURING KEYSTORES AND SSL

Source Site

1. Log in to the WebLogic Server Administration Console.
2. Navigate to the **Domain Structure** screen.
3. Select **Environment > Servers**.
4. Select AdminServer.
5. Navigate to the settings for AdminServer and click the **Keystores** tab.
6. On the Keystores tab, click the **Change** button and select **Custom Identity and Custom Trust** from the drop-down box.
7. Configure the settings for the keystore as shown below.

Custom Identity Keystore	WEBLOGIC_HOME\wlserver_10.3\server\lib\oipakeystore.jks
Custom Identity Keystore Type	jks
Custom Identity Keystore Passphrase	oracle123
Confirm Custom Identity Keystore Passphrase	oracle123
Custom Trust Keystore	WEBLOGIC_HOME\wlserver_10.3\server\lib\oipatruststore.jks
Custom Trust Keystore Type	jks
Custom Trust Keystore Passphrase	oracle123
Confirm Custom Trust Keystore Passphrase	oracle123

Note: Be sure to enter the full filepaths of your keystores.

8. Click **Save**.
9. Click on the **SSL** tab.
10. Configure the settings for the SSL key as shown below.

Private Key Alias	oipaalias
--------------------------	-----------

Private Key Passphrase	oipakeypass
Confirm Private Key Passphrase	oipakeypass

11. Click **Save**.

Destination Site

To configure SSL and keystores for the destination site, follow steps 1–11 above for the destination server.

SAML SOURCE SITE CONFIGURATION

Creating the SAML Credential Mapper

1. In the WebLogic Server Administration Console, navigate to the **Domain Structure** screen.
2. Select **Security Realms**.
3. Select **myrealm**, which is the default realm.
4. Click on the **Providers** tab.
5. Click on the **Credential Mappings** tab.
6. Check the “**SAMLCredentialMapper**” of Type **SAMLCredentialMapperV2** is exist or not, if not click **New**. The Create a New Credential Mapping Provider page will open.
7. In the **Name** field, enter “**SAMLCredentialMapper**”
8. In the **Type** drop-down box, select **SAMLCredentialMapperV2**.
9. Click **OK**.
10. Restart the server.
11. Once the server is restarted, select **Configuration > Provider Specific**.
12. Configure the settings for the Credential Mapper as shown below.

Issuer URI	http://www.oracle.com/oipaSAML
Name Qualifier	oracle.com
Default Time to Live	120
Default Time to Live Offset	0
Signing Key Alias	oipaalias
Signing Key Pass Phrase	oipakeypass
Confirm Signing Key Pass Phrase	oipakeypass

13. Click **Save**.

Important: The system time should be the same for the source and destination servers. If there is any difference between the two machines' system times, the offset can be mitigated by using the Default Time to Live and Default Time to Live Offset parameters.

Configuring the Relying Party Properties

1. In the WebLogic Server Administration Console, click on the **Management** tab.
2. Select **Relying Parties**.
3. Click **New**.
4. In the **Profile** drop-down box, select **Browser/POST**.
5. In the **Description** field, enter "oipaSAML."
6. Click **OK**.
7. Back on the Relying Parties screen, click on the newly created Relying Party.
8. Configure the settings for the Relying Party as shown below.

Enabled	Checked
Description	oipaSAML
Target URL	http://OIDCHostIP:OIDCPort/oidccontext/adfAuthentication
Assertion Consumer URL	https://OIDCHostIP:OIDCSSLPot/samlacs/acs
Assertion Consumer Parameters	APID=ap_00001
Sign Assertions	Checked
Include Keyinfo	Checked

Configuring SAML 1.1 on the Source Site

1. Navigate to the **Domain Structure** screen.
2. Select **Environment > Servers**.
3. Select **AdminServer**.
4. Select **Federation Services > SAML 1.1 Source Site**.
5. Configure the SAML Source Site settings as shown below.

Source Site Enabled	Checked
Source Site URL	http://OIPAHostIP:OIPAPort/PASJava

Signing Key Alias	oipaalias
Signing Key Passphrase	oipakeypass
Confirm Signing Key Passphrase	oipakeypass
Intersite Transfer URIs	/samlits_ba/its /samlits_ba/its/post /samlits_ba/its/artifact /samlits_cc/its /samlits_cc/its/post /samlits_cc/its/artifact
ITS Requires SSL	Checked
Assertion Retrieval URIs	/samlars/ars
ARS Requires SSL	Checked

6. Click **Save**.

SAML DESTINATION SITE CONFIGURATION

Creating a SAML Identity Asserter

1. Ensure that the certificate file (oipaalias.der) you generated previously in the source site server was copied into the directory WEBLOGIC_HOME\server\lib.

Note:	Copying this certificate file to this location will replace the certificate previously generated for the destination site server.
--------------	---

2. Log in to the WebLogic Server Administration Console for the destination site server.
3. Navigate to the **Domain Structure** screen.
4. Select **Security Realms > myrealm**.
5. Select **Providers > Authentication**.
6. Click **New**. The Create New Authentication Provider page will open.
7. In the **Name** field, enter "SAMLIdentityAsserter."
8. In the **Type** drop-down box, select **SAMLIdentityAsserterV2**.
9. Click **OK**.
10. Restart the server.
11. Once the server is restarted, select SAMLIdentityAsserter and click on **Management > Certificates**.
12. Click **New**.
13. In the **Alias** field, enter "oipaalias."
14. In the **Path** field, enter the filepath of the certificate that was copied in from the source site server.
15. Click **Finish**. If the certificate registration was completed without issue, the message "The certificate has been successfully registered" will display.

Configuring the Asserting Party Properties

1. Back on the **Management** tab, click on **Asserting Parties**.
2. Click **New**.
3. In the **Profile** drop-down box, select **Browser/POST**.
4. In the **Description** field, enter "oipaSAML."
5. Click **OK**.

6. Back on the Asserting Parties screen, click on the newly created asserting party.
7. Configure the asserting party's settings as shown below.

Enabled	Checked
Description	oipaSAML
Target URL	http://OIPAHostIP:OIPAPort/PASJava
POST Signing Certificate Alias	oipaalias
Source Site Certificate URIs	/oidc/web/adfAuthentication
Source Site ITS URL	https://OIPAHostIP:OIPASSLPort/samlits_ ba/its
Source Site ITS Parameters	RPID=rp_00001
Issuer URI	http://www.oracle.com/oipaSAML
Signature Required	Checked
Assertion Signing Certificate Alias	oipaalias

8. Click **Save**.

Configuring SAML 1.1 on the Destination Site

1. Navigate to the **Domain Structure** screen.
2. Select **Environment > Servers**.
3. Select **AdminServer**.
4. Select **Federation Services > SAML 1.1 Destination Site**.
5. Configure the SAML Destination Site settings as shown below.

Destination Site Enabled	Checked
Assertion Consumer URIs	/samlacs/acs
ACS Requires SSL	Checked
SSL Client Identity Alias	oipaalias
SSL Client Identity Pass Phrase	oipakeypass

Confirm SSL Client Identity Pass Phrase	oipakeypass
POST Recipient Check Enabled	Checked
POST One-Use Check Enabled	Checked
Used Assertion Cache Properties	APID=ap_00001

6. Click **Save**.

CONFIGURING OIPA AND OIDC

Configuring OIPA

In OIPA's PAS.properties file, make the following changes:

- Set `oidcApp.url` to <http://OIDCHostIP:OIDCPort/DCW51/adfAuthentication?embed=true>.
- Set `oidcApp.isAuthorized` to `false`.

Configuring OIDC

In the `web.xml` file of `OIDCPresentation`, make the following changes in the `<login-config>` section:

- Give the `<auth-method>` element a value of `CLIENT_CERT, FORM`.
- Give the `<realm-name>` element a value of `myrealm`.

TESTING SINGLE SIGN-ON

Importing the Certificate to IE

1. In Windows Explorer, navigate to WEBLOGIC_HOME\wserver_10.3\server\lib.
2. Double-click on oipaalias.der and click **Install Certificate**.
3. Click **Next**.
4. Select **Place All Certificates in the Following Store** and click **Browse**.
5. Select **Trusted Root Certification Authorities** and click **OK**.
6. Click **Next**.
7. Click **Finish**.
8. A security warning will display. Click **Yes**. If the import was completed without issue, the message "The import was successful" will display.

Testing the Application

1. Point a web browser to the OIPA login page (<http://10.184.226.231:7007/PASJava/Login/Login.iface>).
2. Enter "qatester1" for both the Client Number and Personal Id and click **Login**.
3. Navigate to **Case > Case Entry**.
4. Accept any security certificate warnings that display. The OIDC home page will open in the Case Entry Detail window.

DEBUGGING THE APPLICATION

1. In the WebLogic Server Administration Console, navigate to the **Domain Structure** screen.
2. Select **Environment > Servers**.
3. Select **AdminServer**.
4. Click on the **Debug** tab.
5. Expand **WebLogic > Security > SAML**.
6. Click the checkbox to enable SAML debugging. The log file for the server will be made available for both the source and destination domains.