Oracle® OpenSSO

Release Notes

Release 11*g*R1. Version 11.1.1.3.0

E17846-03

June 2011

Provides latest release information including known issues and important late-breaking product news.

ORACLE®

Oracle OpenSSO Release Notes, Release 11*g*R1. Version 11.1.1.3.0

E17846-03

Copyright © 2010, 2011 Oracle and/or its affiliates. All rights reserved.

Primary Author: Gina Cariaga

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, 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 which 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.

Contents

Preface v

Audience v
Purpose of This Document v
Documentation Accessibility v
Related Documents vi
Conventions vi

1 Oracle OpenSSO Security Token Service

1.1 Oracle OpenSSO Security Token Service Supported Standards and Applications 1-1
1.2 Oracle OpenSSO Security Token Service Download Location 1-1
1.3 Oracle OpenSSO Security Token Service Issues and Workarounds 1-2
1.3.1 Internet Explorer 7 and 8 Browser Options Should be Changed to Configure OpenSSO STS 1-2
1.3.2 OpenSSO STS ssoadm do-batch Subcommand Throws a Null Pointer Exception 1-2
1.3.3 Activating OpenSSO STS in the WebLogic Server 10.3.3 Administration Console Throws Exceptions 1-2
1.3.4 OpenSSO STS opensso-client.zip File Contains an Unsupported WAR File 1-3
1.3.5 Custom Configurator Can Disable an Existing OpenSSO STS Configuration 1-3

2 Oracle OpenSSO Fedlet

2.1 Oracle OpenSSO Fedlet Supported Standards and Applications 2-1
2.2 Oracle OpenSSO Fedlet Download Location 2-1
2.3 Oracle OpenSSO Fedlet Issues and Workarounds 2-1
2.3.1 Oracle Identity Federation Identity Provider Returns Error Without Service Provider Signing Certificate 2-2
2.3.2 Java Oracle OpenSSO Fedlet Single Sign-On Fails on JBoss AS 5.0.x 2-2
2.3.3 ConfigureFedlet Program Has Incorrect Korean Translation 2-2
2.3.4 ConfigureFedlet Program Returns Message "Unrecognized command: -genKey" .. 2-3
2.4 Documentation Errata 2-3
2.4.1 Oracle OpenSSO Fedlet Java API Reference 2-3

Preface

Welcome to *Oracle OpenSSO Release Notes*. This document contains the release information for the Oracle OpenSSO Security Token Service (OpenSSO STS) and the Oracle OpenSSO Fedlet. It describes differences between these Oracle OpenSSO components and their documented functionality.

Oracle recommends you review its contents before installing or working with the product.

Audience

This document is intended for enterprise administrators and web services developers.

Purpose of This Document

These release notes supplement the core Oracle OpenSSO documentation set. The release notes provide information about known issues and workarounds for installing and using OpenSSO STS and the Oracle OpenSSO Fedlet.

This document is accurate at the time of publication. Oracle will update the release notes periodically after the software release. You can access the latest information and additions to these release notes on the Oracle Technology Network at:

`http://www.oracle.com/technology/documentation/`

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle OpenSSO documentation library:

- *Oracle OpenSSO Security Token Service Administrator's Guide*
- *Oracle OpenSSO Fedlet Interoperability Guide for Oracle Identity Federation*

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.
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

Oracle OpenSSO Security Token Service

The Oracle OpenSSO Security Token Service (OpenSSO STS) provides a secure way to handle identity propagation that is controllable by policy. As a trusted authority service, OpenSSO STS issues and validates security tokens. As a web services security provider, OpenSSO STS secures communication among web service clients and web service providers

This chapter contains the following topics:

- Section 1.1, "Oracle OpenSSO Security Token Service Supported Standards and Applications"
- Section 1.2, "Oracle OpenSSO Security Token Service Download Location"
- Section 1.3, "Oracle OpenSSO Security Token Service Issues and Workarounds"

For detailed installation and administration instructions, see the *Oracle OpenSSO Security Token Service Administrator's Guide* in this documentation library.

1.1 Oracle OpenSSO Security Token Service Supported Standards and Applications

For information about the platforms and product versions supported by the Oracle OpenSSO Security Token Service, see the appropriate certification matrix:

`http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html`

1.2 Oracle OpenSSO Security Token Service Download Location

The Oracle OpenSSO Security Token Service is available to download from the Oracle Fusion Middleware 11gR1 Software Downloads page:

`http://www.oracle.com/technology/software/products/middleware/htdocs/fmw_11_download.html`

1.3 Oracle OpenSSO Security Token Service Issues and Workarounds

This section describes the following issues and workarounds for the Oracle OpenSSO Security Token Service:

- Section 1.3.1, "Internet Explorer 7 and 8 Browser Options Should be Changed to Configure OpenSSO STS"
- Section 1.3.2, "OpenSSO STS ssoadm do-batch Subcommand Throws a Null Pointer Exception"
- Section 1.3.3, "Activating OpenSSO STS in the WebLogic Server 10.3.3 Administration Console Throws Exceptions"
- Section 1.3.4, "OpenSSO STS opensso-client.zip File Contains an Unsupported WAR File"
- Section 1.3.5, "Custom Configurator Can Disable an Existing OpenSSO STS Configuration"

1.3.1 Internet Explorer 7 and 8 Browser Options Should be Changed to Configure OpenSSO STS

Before you configure OpenSSO STS, set the Internet Options settings for Internet Explorer 7 or Internet Explorer 8 as follows:

- Permit the execution of JavaScript (Enable Active scripting).
- Add the OpenSSO STS site to be configured to the Trusted sites zone.

1.3.2 OpenSSO STS ssoadm do-batch Subcommand Throws a Null Pointer Exception

Included per bug 6940462.

The `ssoadm do-batch` subcommand throws a Null Pointer Exception (NPE) related to logging before the command completes.

1.3.3 Activating OpenSSO STS in the WebLogic Server 10.3.3 Administration Console Throws Exceptions

Included per bug 6964741.

After deploying OpenSSO STS (`openssosts.war`) in Oracle WebLogic Server 10.3.3 in production mode and starting the OpenSSO STS web application, exceptions are thrown in the console where the WebLogic Server domain was started.

After starting OpenSSO STS, it remains started and exceptions are not thrown again until OpenSSO STS is stopped and then restarted.

The workaround is to copy the `saaj-impl.jar` file from the OpenSSO STS `opensso-client-jdk15.war` file to the WebLogic Server 10.3.3 configuration `endorsed` directory, as follows:

1. Stop the WebLogic Server 10.3.3 domain.
2. If necessary, unzip the OpenSSO STS ZIP file.
3. Create a temporary directory and unzip the `openssosts-zip-path/opensso/samples/opensso-client.zip` file in that directory, where `openssosts-zip-path` is where you unzipped the OpenSSO STS ZIP file. For example:

   ```
   cd openssosts-zip-path/samples
   ```

```
mkdir ziptmp
cd ziptmp
unzip ../opensso-client.zip
```

4. Create a temporary directory and extract the `saaj-impl.jar` file from `opensso-client-jdk15.war`. For example:

```
cd openssosts-zip-path/opensso/samples/ziptmp/war
mkdir wartmp
cd wartmp
jar xvf ../opensso-client-jdk15.war WEB-INF/lib/saaj-impl.jar
```

5. Create a new directory named `endorsed` under the `WEBLOGIC_JAVA_HOME/jre/lib directory` (if `endorsed` does not exist), where `WEBLOGIC_JAVA_HOME` is the JDK that WebLogic Server is configured to use.
6. Copy the `saaj-impl.jar` file to the `WEBLOGIC_JAVA_HOME/jre/lib/endorsed` directory.
7. Start the WebLogic Server domain.

1.3.4 OpenSSO STS opensso-client.zip File Contains an Unsupported WAR File

Included per bug 6964168.

The `openssosts.zip` contains the `opensso-client.zip`, which has samples and corresponding WAR files. The `opensso-client-jdk15.war` file is not supported, because the minimum supported JDK for OpenSSO STS is JDK 1.6.0_18.

The workaround is to not deploy the `openssoclient-jdk15.war` file. This WAR file, however, contains the `saaj-impl.jar` file, which is used in the workaround for Section 1.3.3, "Activating OpenSSO STS in the WebLogic Server 10.3.3 Administration Console Throws Exceptions."

1.3.5 Custom Configurator Can Disable an Existing OpenSSO STS Configuration

After using `stsconfig.jsp` to create a successful OpenSSO STS configuration, to avoid an internal accidental configuration overwrite or change of the OpenSSO STS configuration, it is recommended that you perform one of the following procedures.

Without a Load Balancer. If you have not deployed OpenSSO STS behind a load balancer, perform the following steps before deploying the `openssosts.war` file:

1. Create a temporary staging area:

```
mkdir /tmp/staging
```

2. Go to the staging area:

```
cd /tmp/staging
```

3. Expand the `openssosts.war` file:

```
jar xvf WAR-FILE-HOME/openssosts.war
```

4. Go to the config directory:

```
cd config
```

5. Remove the `options.htm` file:

```
rm options.htm
```

6. Go up one directory:

   ```
   cd ..
   ```

7. Create `openssosts.war` from the staging area:

   ```
   jar cf /tmp/openssosts.war *
   ```

8. Redeploy the `/tmp/openssosts.warfile` on the same web container instance on which OpenSSO STS was originally deployed and configured.
9. Remove the staging area directory:

   ```
   rm -rf /tmp/staging
   ```

With a Load Balancer. If OpenSSO STS is fronted by a load balancer, protect `DEPLOY_URI/config/options.htm` from the load balancer.

2

Oracle OpenSSO Fedlet

The Oracle OpenSSO Fedlet (Fedlet) is a lightweight service provider (SP) implementation that can be integrated with a Java or .NET application, enabling the application to communicate with an identity provider (IdP) such as an Oracle Identity Federation identity provider using the SAML 2.0 protocol.

This chapter includes the following topics for the Oracle OpenSSO Fedlet:

- Section 2.1, "Oracle OpenSSO Fedlet Supported Standards and Applications"
- Section 2.2, "Oracle OpenSSO Fedlet Download Location"
- Section 2.3, "Oracle OpenSSO Fedlet Issues and Workarounds"
- Section 2.4, "Documentation Errata"

For detailed information, see the *Oracle OpenSSO Fedlet Interoperability Guide for Oracle Identity Federation* in this documentation library.

2.1 Oracle OpenSSO Fedlet Supported Standards and Applications

For information about the platforms and product versions supported by the Oracle OpenSSO Fedlet, see the appropriate certification matrix:

`http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html`

2.2 Oracle OpenSSO Fedlet Download Location

The Oracle OpenSSO Fedlet is available to download from the Oracle Fusion Middleware 11gR1 Software Downloads page:

`http://www.oracle.com/technology/software/products/middleware/htdocs/fmw_11_download.html`

For some deployments, rather than downloading the Oracle OpenSSO Fedlet, a service provider administrator can get a previously configured Oracle OpenSSO Fedlet package from the identity provider administrator.

2.3 Oracle OpenSSO Fedlet Issues and Workarounds

This section describes the following issues and workarounds for the Oracle OpenSSO Fedlet:

- Section 2.3.1, "Oracle Identity Federation Identity Provider Returns Error Without Service Provider Signing Certificate"

- Section 2.3.2, "Java Oracle OpenSSO Fedlet Single Sign-On Fails on JBoss AS 5.0.x"
- Section 2.3.3, "ConfigureFedlet Program Has Incorrect Korean Translation"
- Section 2.3.4, "ConfigureFedlet Program Returns Message "Unrecognized command: -genKey""

2.3.1 Oracle Identity Federation Identity Provider Returns Error Without Service Provider Signing Certificate

Included per bug 9952201.

If the Oracle OpenSSO Fedlet service provider metadata (`sp.xml` file) does not include a signing certificate, a version 11.1.1.2.0 and earlier Oracle Identity Federation identity provider returns an error at run time when it receives a SAML 2.0 AuthN request.

The workaround is to add a signing certificate to the Oracle OpenSSO Fedlet service provider metadata before you load the metadata into the Oracle Identity Federation identity provider.

The absence of a signing certificate in the Oracle OpenSSO Fedlet service provider metadata indicates that the Fedlet will not be sending signed requests. Therefore, you can add any arbitrary certificate to the metadata for this workaround, since the certificate will never be used at run time for signature verification.

2.3.2 Java Oracle OpenSSO Fedlet Single Sign-On Fails on JBoss AS 5.0.x

Included per bug 9965450.

If you deploy the Java Oracle OpenSSO Fedlet on JBoss Application Server 5.0.x, `index.jsp` does not display and the Java Fedlet single sign-on (SSO) fails with an IllegalStateException.

The workaround is to add the following Java options for JBoss AS 5.0.x:

1. Stop the JBoss AS 5.0.x web container.
2. Add the following Java options in the JBoss AS 5.0.x `run.conf` file:

```
-Djavax.xml.soap.MetaFactory=com.sun.xml.messaging.saaj.soap.SAAJMetaFactoryImpl
-Djavax.xml.soap.MessageFactory=com.sun.xml.messaging.saaj.soap.ver1_1.SOAPMessageFactory1_1Impl
-Djavax.xml.soap.SOAPConnectionFactory=com.sun.xml.messaging.saaj.client.p2p.HttpSOAPConnectionFactory
-Djavax.xml.soap.SOAPFactory=com.sun.xml.messaging.saaj.soap.ver1_1.SOAPFactory1_1Impl
```

3. Start the JBoss AS 5.0.x web container.

2.3.3 ConfigureFedlet Program Has Incorrect Korean Translation

Included per bug 9946834.

The Korean translation of the Java Oracle OpenSSO Fedlet `ConfigureFedlet` program has an incorrect translation of the following prompt:

```
Enter the directory with path where Oracle-OpenSSO-Fedlet.zip is extracted to:
```

The workaround is to specify the directory where you extracted the `Oracle-OpenSSO-Fedlet.zip` file.

2.3.4 ConfigureFedlet Program Returns Message "Unrecognized command: -genKey"

Included per bug 12408673.

This error message is displayed when you use the ConfigureFedlet Program to configure the Fedlet and both of the following are true:

- You are using a newer JDK such as Java version 1.6.0_22.
- You answered "Yes" to this question: "Do you want to generate keystore and key pair for the Fedlet?"

The program fails with the following error:

```
ERROR>Unrecognized command: -genKey
OUTPUT>Usage:  keytool [COMMAND] [-- COMMAND]...
OUTPUT>Manage private keys and public certificates.
OUTPUT>Cannot generate keystore.
```

Use one of the following workarounds:

- Use an older version of JDK such as Java version 1.6.0_21.
- Use a newer version of JDK, but answer "No" to the question: "Do you want to generate keystore and key pair for the Fedlet?"

  Then after the Configure Fedlet program is done, follow the steps in this documentation to generate the keystore and a signing/encryption certificate for the Fedlet: http://download.oracle.com/docs/cd/E17842_01/doc.1111/e17847/configjavasp.htm#BABEGHCE

2.4 Documentation Errata

This section describes documentation errata for the Oracle OpenSSO Fedlet.

2.4.1 Oracle OpenSSO Fedlet Java API Reference

The Oracle OpenSSO Fedlet Java API reference is available in the *Oracle OpenSSO 8.0 Update 2 Java API Reference*:

http://download.oracle.com/docs/cd/E19681-01/821-2131/index.html

---

Note: The Oracle OpenSSO Fedlet does not support the `getPolicyDecisionForFedlet` method.